SLTPS-PAC Meeting 1-25-17

[Multiple conversations; off-mic]

MARK BRADLEY: OK, ladies and gentlemen. Shall we start?

F: Go ahead.

BRADLEY: OK. I thank everyone for coming. This is our first one of 2017, I think the 12th one total. This is my first, so I'm going to be working off a heavily scripted text, so if I sound wooden it's because I am today. Hopefully, I'll improve over time as I get more familiar with what this is. I mean, I helped do some of the drafting of the executive order that created this but never having been in the pilot seat here, so we'll go slowly and methodically today. And let me tell you just a little bit about myself. This is my fourth federal job. I came over here from the Department of Justice National Security Division where I worked on a variety of issues including the Foreign Intelligence Surveillance Act to intelligence community guidelines to all sorts of boards and panels and that. Before that, I was Pat Moynihan's legislative director on the hill. I took a segue for eight years being a criminal defense lawyer here in our city, just to tip your smiles, and I was in the CIA back in the '80s working on Pakistan after the

Russians invaded. So this seems like kind of, I guess, a capstone to my career, sitting here. Anyway, I'm delighted to be here, and this is an important committee, and I've been told it's a very collegial one, which is absolutely essential to be able to get this work done. So, without further ado, let me start with my script.

This is a public meeting, as you all know, subject to the Federal Advisory Committee Act. The minutes of the SLTPS-PAC meeting are available to the public. This meeting is being audio-recorded. The microphones around the table have enough cord to be repositioned in front of anyone who wants to speak. A floor microphone is located to the side of the room for audience members to use. Anyone who is making a presentation but not sitting at the table can use the podium at the front of the room to give your briefing. Please identify yourself when speaking so we have an accurate record of your comments. This is particularly important, because maybe of our members are participating by telephone conference. We want them to know who we are when we are speaking and what we need to know when -- we need to know who they are when they are speaking. All right, so just some administrative things, membership changes. Last year, two SLTPS (inaudible) members ended

their service on the committee, Kevin Donovan of Johnson & Johnson, who completed his fourth-year term, and Lindsey Johnson of Tennessee Fusion Center, who had new responsibilities that precluded her from continuing with the committee. Several very qualified members were nominated for the positions. From among them, the previous acting chair, Bill Cira, selected Agnes Ranier Kirk. Agnes is the Washington State chief information security officer. Angus indicated she would participate via teleconference. Welcome, Agnes.

AGNES KIRK: Thank you.

BRADLEY: Yeah, wake me up.

M: (inaudible), you can adjust the volume maybe unless she's not --

BRADLEY: All right. Next is Jessica Davenport. Jessica is a senior management analyst supervisor with the Florida Department of Law Enforcement at the Florida Fusion Center. Jessica indicated she would participate via teleconference. Jessica, are you there?

JESSICA DAVENPORT: I'm here, and thank you. I look forward to working with you all.

BRADLEY: Lovely. Agnes and Jessica, we are pleased to have you on the committee and look forward to your contributions, so don't be shy about speaking up. There are also changes on

the federal side. Lou Widawski, the member from the Department of Transportation, is retiring at the end of the month. Joan Harris, the DOT alternate, indicated she -- that a new member of the committee would be identified when the replacement of Mr. Widawski is selected.

M: Yes, and we have someone here. I haven't had the pleasure to meet you, but we'll go around.

ROBERT VINCIGUERRA: I'm Robert Vinciguerra, DOT. I'm sitting in for Lou today.

BRADLEY: OK.

ROBERT: Because [Keith Seikel?] was appointed -- wasn't appointed -- is taking over temporarily once Lou is gone until we can get a director appointed. So until that time, either Joan or myself will be coming to the meetings.

BRADLEY: OK, lovely. Michael Layton will no longer be able to serve on the SLTPS-PAC because he has a new assignment at the NRC. He advised that Darryl Parsons, the NRC alternate, will continue to represent the NRC on the committee until a replacement for Mr. Layton is named. All right. Let's go around the room and introduce who's at the table. Do you want to?

GREG PANNONI: Hi, good morning, Greg Pannoni, ISOO and the designated federal official for the meeting.

TIP WIGHT: Tip Wight, I'm the vice chair and acting in the capacity of special assistant to the president of the National Fusion Center Association for the purposes of this meeting.

HARRY COOPER: Harry Cooper, CIA.

RICHARD LICHT: Richard Licht. I'm with the Multistate Information Sharing and Analysis Center.

RUSS PORTER: Good morning. I'm Russ Porter. I'm here representing the ODNI. Normally, Rick Hohman from our security side of the apparatus sits here, but they couldn't make it today, so they asked me to come in. I have 30 years of prior experience in state and local law enforcement and intelligence.

BRADLEY: Great.

KEITH MINARD: Keith Minard, Defense Security Service.

JOSH EDERHEIMER: Josh Ederheimer, DOJ Office of Tribal Justice coming from the DC Police Department before I came to DOJ.

LYDIA LOCKLEAR: Lydia Locklear, Office of Tribal Justice, (inaudible).

PATRICK VISCUSO: Pat Viscuso. I'm at ISOO, and I'm the associate director for CUI.

VINCIGUERRA: Robert Vinciguerra, Department of Transportation.

ELAINE CUMMINS: Elaine Cummins, FBI.

LEO MASCIANA: Leo Masciana, State Department.

BEN RICHARDSON: Ben Richardson, DOD.

CHARLIE ROGERS: Charlie Rogers, DHS. I manage state and local security programs.

BRADLEY: Anybody who is with us on teleconference identify themselves, please.

MARK PEKRUL: Mark Pekrul, Department of Energy.

BRADLEY: Hi, Mark.

MARK SCHOUTEN: Mark Schouten, Homeland Security and Emergency Management Director for the state of Iowa.

BRADLEY: Welcome.

GLENN BENSLEY: Hey, Mark. Glenn Bensley, Department of Justice.

BRADLEY: Hey, Glenn.

BENSLEY: Congratulations on your new position.

BRADLEY: Thanks, man.

DORI KOREN: Good morning, folks. This is Dori Koren. I'm a sergeant with the Las Vegas Metropolitan Police Department assigned to the Southern Nevada Counterterrorism Center.

JEFF FRIEDLAND: Good morning. Jeff Friedland, representing state and local tribal and territorial.

DARRYL PARSONS: This is Darryl Parsons with Nuclear Regulatory.

DEWEY WEBB: Dewey Webb with the National Native American Law Enforcement Association.

BRADLEY: Sounds like that's --

KIRK: And, again, this is Agnes Kirk with the state of Washington.

M: Jessica (inaudible). I guess we don't have Joe Lambert.

BRADLEY: It doesn't sound like it, no. OK, thank you so very much. All right. We all have folders. In there are copies of the meeting agenda, the slides for the presentations we're going to have today and the minutes of the last meeting. All right. I'm going to turn it over to Greg Pannoni here to talk about old business.

PANNONI: OK. Thank you, Mr. Chair.

BRADLEY: You're welcome.

PANNONI: And welcome, as well, formally to the committee.

BRADLEY: Thanks.

PANNONI: So I did want to say this is a continuing thing. We know that, due to budgetary limitations, we have to continue to offer this teleconference capability, because we just simply don't have the funds to pay for travel for those that are out of the area. And on that point, I want to recognize Rich Licht, who came here from New York to attend in person. Thank you, Rich. With the action items, we had three from the last meeting, and they're all interrelated, so I'm going to ask my colleague, Vice Chair Charlie Rogers, to participate, but I'll start with the

first one. These concern -- as I said, they're interrelated. They concern access to classified information, eligibility for access, and access to information systems, so they're all sort of interrelated in that sense. The first one -- excuse me -- concerned JWICS access for Fusion Center personnel and other state, local, and tribal personnel without the requirement of being detailed to a federal agency. I did want to point out that if you look closely at the executive order for the program it does set the threshold for both access to classified information and for information systems that process or store classified information.

So, as you probably know, the access is set at the secret level. That's the basic threshold, and then there's a more stringent threshold essentially on a case-by-case basis with sponsoring agency approval for a higher access above secret, so top secret, sensitive compartmented information, special access program information, and it's similar for the information system requirement. And then, for the -- and the physical custody works the same way. If there is to be physical custody above the secret level, the order speaks to having a DHS person or another federal government executive agency person full-time to manage the operations

and controls of the Fusion Center. So, with that said, I think you can see that, you know, technically a person does not have to be detailed to a federal agency in order to gain access to JWICS, but, granted, it's a high threshold. There are stringent -- much more stringent controls to access JWICS. Unfortunately, we've had some transition with our DNI representation, so, in all candidness, I haven't had the opportunity to really have a good, length discussion with respect to JWICS access, which ultimately is under their authority. So we still want to pursue that, because this whole program, state-level tribal private sector, is about consistent sharing -- excuse me -- consistent safeguarding and to enhance the sharing of classified information. So I share the concern and understanding that there is, at least in certain instances, a need for access to higher levels above secret, which -- it has happened in some in some instances, as Charlie Rogers has indicated. So I'll -- unless the DNI would like to -- our colleague from the DNI would like to make any comments on this -- I'm not trying to put you on the spot -- I'll ask Charlie to continue.

ROGERS: Yeah, there are two other elements that came up that DHS had to go back and research, and there was concern about the length of time that -- inactivity on HSDN, which

is our secret-level system, how quickly would someone's account be deactivated. Actually, I didn't know the answer to that, and we thought it was around 20 days. It turned out that it's 30 days, and there was a desire to increase it, but it seems like it's not an issue in the sense that, if you are state and local using HSDN and you don't use it for 30 days, you can get it reactivated for another 60 days, so up to 90 days. It just requires that the individual set up a password or a code word or something with the help desk.

M: Challenge questions, challenge questions.

BRADLEY: Challenge questions.

ROGERS: So it's really quite a length period that you have, a grace period. It does require, during the initiation process to get access to the system, that you create this -- I don't know what the right word is -- code word, password.

M: Challenge questions.

ROGERS: Challenge questions, yeah. So I think it's kind of a nonissue, and then I also went ahead and asked what it was for our internal SCI system, and it's similar. It's the same length of time. So I think some people may have been canceled out at 30 because they weren't aware of the challenge question, so I think that's been answered. And

the other question was -- and I had to go back and look into it -- our intelligence and analysis directorate sponsors a select number of people for SCI access, and they've recently formalized how they nominate folks. They don't actually clear them. My office clears them, but they're the vetting activity within DHS for SCI, and they formalized some processes and some forms. So I went back to them, and the concern was, are these forms and processes going to survive the transition to the next administration. So I went back, reviewed the memos and the forms that governed how they nominate, and I asked them specifically, "Is this formalized?" They said, "It's absolutely formalized," and there was concern that it be formalized. And then, I went back to our implementing directive to look at the exact language, and the implementing directive, which was approved by this committee and which is national policy, basically sets the criteria for SCI access for state, local, tribal, private sector. And the I&A nominating forms mirror the policy exactly, and I think the basic thing was that it's a case-by-case decision that's evaluated on the individual -- there's a requirement that the individual identify a SCIF or a location that they can access it, because state facilities basically can't have SCI under their own management. They can have -- New York

City and Chicago have SCIFs, but they're managed by DHS. And the other one was that they commit to a duration of about 18 months. I don't -- the implementing directive "a sufficient duration," you know, to justify the expense, but I&A has set it at 18 months. So, to summarize it, it's articulated in policy. It's in our national policy, and in the I&A policy they told me it is in place and is not going to go away.

M: And, if I may add, there are some words in there about a "demonstrated and foreseeable need."

ROGERS: Yeah. Well, there's quite a bit of words in the implementing directive about the demonstrated need and the categories of personnel, and there's a wide range of personnel who can get SCI access, and the fact that they have a connection to Homeland Security and a federal counterterrorism mission and that they have the ability to influence and provide expertise to the process. So we --

SCHOUTEN: Charlie, Mark Schouten from Iowa. I don't know if you can hear me. I'm wondering, can you distinguish JWICS from your standard HSDN? Are those, the processes for obtaining access to each of those, similar or different?

ROGERS: Well, I'm not an expert on this. I mean, JWICS is an SCI-level system managed by the intelligence community. HSDN is a secret-level system that DHS manages and that

other federal agencies participate in. The requirements for access to the systems are based upon your clearance level for part of it and whether you have the SCI or special compartmented information access. So they're two separate systems with two separate requirements for access. One is an intelligence community system. One is a collateral DHS system.

WIGHT: This is Tip Wight. If I could clarify, though, to your question, for state and local personnel as of right now, and that's the action item we have open, the only way to get a JWICS account is to be detailed to a federal agency. At least, that's what I'm told, and that's one of the action items we're still trying to follow up on. So, for state and local personnel, unless you're, say, assigned to a joint terrorism task force or something like that, there's no way to get a JWICS account at present, so we're trying to work our way through that.

SCHOUTEN: You know, from an Iowa standpoint, as homeland security advisor, we're not so concerned about JWICS. We would like direct connection to HSDN, which I assume, then, Charlie, would be through you and perhaps easier to get than JWICS.

ROGERS: Well, it's easy. It's not exactly through me. One, HSDN requires a secure facility to be built to house the

network or the system, so it's -- and then, there's a cost, a monthly cost, just to manage it. There's a personnel cost to manage that alarmed room, so there's a whole security overlay that goes with it. These systems are basically endorsed and nominated by the intelligence and analysis directorate and DHS, not by the office of security. They, you know -- because there's a fairly significant budget and a fairly significant security footprint, they limit the number of locations that get it. For the most part, they're going directly to fusion centers, and then the expectation is that people could work with and cooperate with fusion centers to gain access to the network within the fusion center. So getting access to the network is not that difficult. I think it's a matter of negotiating with I&A, having the appropriate clearance, negotiating with the fusion center, but getting -- if you wanted one at your location, now we're talking about a very significant outlay, but those decisions are not made by my office. We --

SCHOUTEN: Yeah. Charlie, we have that. We've got an MOU with the National Guard to use their SCIF. We're having a little bit of difficulty getting our critical infrastructure -- our lifeline critical infrastructure person who is working cyber access to HSDN on a regular

basis, so we're looking at alternatives in the interest of sharing information and sharing it better. I think, as Tip said at the last meeting, cyber puts all of those information sharing in a different light, and we just have to make sure that information is getting out.

WIGHT: Yeah. This is Tip. I couldn't agree more, and that's -- unfortunately, that's one of the reasons for my push for the TS/SCI access for fusion centers, is because much of that cyber information is at the TS level. We can have a discussion of whether it needs to be or not, but unfortunately it is, so that's part of it, but certainly for your issues at the secret level as well. And I take it you guys aren't collocated with the Iowa Fusion Center?

SCHOUTEN: No, we're not, and so we talked with our intelligence -- DHS intelligence officer two days ago, and I think we perhaps enlightened him that, among states, not all states have their homeland security advisor under the DPS, or Department of Public Safety, which also controls the Fusion Center. Sometimes, the Fusion Center -- quite often, Fusion Centers are outside of the homeland security advisor's office, so there isn't that automatic linkage that I think maybe DHS is assuming is happening. The connection, the information sharing isn't perhaps as good as it could be or as it would be if the connection were

direct. Not all states are created the same. Not all states are organized the same, so I think there's maybe -- I don't know -- 15 states where the homeland security advisor is not connected directly with the fusion centers. So we're putting all our eggs into that basket, into that organizational structure. I'm not sure we're sharing information as well at the level of some states.

ROGERS: There's definitely diversity in the way in which states are configured, and, you know, I mean, we could have a guest speaker from I&A, I guess, come and talk to it, but it's really not a -- it's an internal DHS activity and the Intelligence and Analysis Directorate that they are prioritizing, wherever they can, where these resources are going. It's -- I'm not a budget person. I can't tell you the cost, but it's fairly significant to construct, manage, and operate a room that houses HSDN, and the monthly costs. So, for the most part, they're identified in fusion centers.

WIGHT: And you know, just -- this is Tip Wight again -- the was DC solved it, because the fusion center originally started in the police department, and then the homeland security advisor is not collocated with that, works out of the Emergency Management Agency, they actually relocated the fusion center to the Emergency Management Agency, so it

was collocated with the HSA. So, you know, different entities will probably have different solutions for it based on the leadership.

SCHOUTEN: I think you're right, Tip.

M: That may not be a bad suggestion to have next time --

M: Yeah, sure.

BRADLEY: -- an intelligence and analysis person come brief us on the process.

ROGERS: For their field ops, yeah.

M: OK.

BRADLEY: All right. Now, we'll turn -- this is Mark Bradley, the chair -- we'll not turn to new business. Charlie, you're not off the hook. I'll introduce you again, and you'll provide an update on the SLTPS security program implementation.

ROGERS: Yeah, this is Charlie Rogers. I do this at every meeting, so I'm reluctant to go through, in granular detail, every aspect of the program, so I'll give you a broad overview of what we're doing, and then, if there are questions about the program, I'll certainly answer them. But, basically, the state and local, tribal, private sector security program, a big emphasis is on fusion centers. It's on state, local, tribal, where they are housing classified information, primarily fusion centers. So the

program has different aspects to ensure that we're providing the support we need to provide, that the classified information at those locations is protected sufficiently, and that we're doing oversight to ensure that it's occurring. So we have a security compliance review program. We do about 15 a year. One year, we did 19. One year, we did 11. We implemented that program in late 2012. I think it was in September of 2012, and since then we've done 76 compliance reviews with fusion centers, and we expect to do 15 this year. So it's a pretty robust program. We also go out and -- you know, I&A goes out for assistance visits. I&A is our Intelligence and Analysis directorate. We also go out on special visits for other occasions. So the numbers are that last year we did 15. We expect to do 15 this year. We've done a total of 76.

Another aspect of the program is that, under the implementing directive, fusion centers are required to appoint security liaisons who are individuals onsite who have responsibility for managing the classified and managing the secure room at their location, so we have an ongoing training program to ensure that the security liaisons are kept at an appropriate level of expertise to carry out their duties. So we have a webinar program that

we've established. We do about 10 of those a year, and that includes about two hours of training and provides an opportunity to go over the policy and procedures, answer questions. So, most recently, in '15 we did 10 webinars, trained 81 security liaisons, and last year we also did 10 webinars and trained 80 security liaisons. So it's not perfect training. It's not web-based training. When we do go out on compliance -- it is web-based training. It's not in-person training. But when we do go out on compliance reviews, we also do training during that time period. And the other training program we have, which is funded through the Intelligence and Analysis activity, is quarterly training events, and that's where we bring in newly appointed security liaisons for about two and a half days of training at DHS headquarters. The Office of Security, I&A, and other offices within DHS participate in that training, so it's very -- in '16, we actually didn't have any of those events. I think it was a funding issue. But in '17 already, we've had one, and we've had four people come in. They actually came in on Election Day, and we trained those four folks.

We talked a little bit about personnel security, and, just to put it out there, currently DHS has approximately 2,100

private-sector clearances under EO 13549. These are subject matter experts that have been identified, and they have secret clearances. We have another 5,000 state and local personnel who are cleared through the program. We've also -- and this is since the inception of DHS -- we've also inactivated about 2,200 clearances, so we've got about 7,500 people with clearances. We also have deactivated an additional 2,500 clearances through separation or when they're no longer eligible and they no longer work for the company or no longer work in the infrastructure that the company represents, and they're debriefed.

PANNONI: Hey, Charlie. It's Greg Pannoni. Just to get an idea, do you know approximately how many SCI accesses you have?

ROGERS: Yeah, I have that number here. We -- the combined number of state, local, and private sector SCIs -- let me make sure I read this right -- is 370, and that's both the private sector folks --

PANNONI: And state and local.

ROGERS: -- state and local.

WIGHT: And just one note on that -- it's Tip Wight -- that isn't necessarily all the state, local, tribal, or private sector personnel that are cleared to SCI level. That's

only through DHS. There are personnel like myself who are cleared through FBI, so there are other sources, but --

ROGERS: Right. And under the executive order, it delegated to the agencies to clear whoever they felt they needed to, so it wasn't -- DHS is not solely responsible for all state and local clearances, but you're right. The FBI frequently clears a -- they also have, I think, a clear turnover and debriefing process when you're in the program or out of the program. So what else did I want to tell you about the program? So any other questions about clearances?

SCHOUTEN: Charlie, Mark Schouten again, just to further fill out the record, in a state like Iowa our security liaison is part of homeland security and emergency management, not part of the fusion center. And the person that does the liaison work is a former NSA employee who, for some reason, moved back from DC to Iowa, I think to raise a family, and he is our security liaison. We work with our PSA to do the private sector clearances, and particularly now, with cyber, we are reaching out to the lifeline critical infrastructure folks and talking with our PSA, trying to get more clearances for them. And I'm inclined to agree with Tip on this, too, that maybe the secret among some of them probably is not enough. I think we have one utility rep who is part of the Kansas Fusion Center. I believe he

has the top secret SCI, and I think, from the cyber standpoint, if you're really going to be getting into the attack analysis, SCI is probably necessary.

ROGERS: Yeah, you're right. The PSAs do nominate a lot of private sector -- we have two nominating activities in DHS. One is with the intelligence and analysis director, and one was with MPPD, who has the private sector infrastructure protection mission. So there are two nominating elements that feed into the office of security, and they vet and validate the requirements for us.

SCHOUTEN: And so, Charlie, from my standpoint, what do I do, living out here in the state of Iowa? But I think our office has taken the approach that we should increase the number of folks with clearances but do so judiciously, particularly among the, you know, 300 to 400 municipal utilities we have in the state, one or two who would represent that sector or the gas systems or the water and wastewater reclamation systems. They have organized groups. We're talking to them, saying we'd like one or two people that we are going to nominate with the PSA to get a clearance, because we think merely giving them a nondisclosure agreement at the time of an incident is probably not going to be adequate. If we want to prepare them, I think we need to give them some threat information,

and all of this has changed after Ukraine. I mean, before Ukraine, we weren't nearly as sharply focused on lifeline critical infrastructure as we are now, and, having the knowledge that an attack like this is possible, we'd like to bring these folks into the fold, perhaps give them more information about the nature of the risk. But to do so, we really need -- they need to be cleared at, at least, the secret level to make it worth their time to hear the briefing.

ROGERS: Well, you could contact me. I'm not the person with the answer, but I could try to connect you to the critical infrastructure people in DHS, and they're really the ones that you would need to establish a relationship with in order to facilitate any sponsoring of clearances. So the clearances would have to have a nexus to a DHS mission. I'd say that's pretty much a precondition, but that's what the critical infrastructure people are involved in. They're involved in infrastructure and cyber, so, you know, I can give you my email.

SCHOUTEN: And I think we're consistent with what they're doing. I mean, like I said, the private sector folks, the PSA is handling it. We have maybe four or five in process. We won't end up with more than six. We don't want to burden the system, but we think -- and the PSA agrees -- that we

will be adding a lot of value to the state by having select members or representatives of critical lifeline industries with clearances so they can hear the nature of the risk.

ROGERS: Yeah. That makes sense.

BRADLEY: That all makes sense.

ROGERS: Yeah, if you want my email address, I guess the simplest one is charles.rogers -- R-O-G-E-R-S -- @DHS.gov.

SCHOUTEN: Excellent. Excellent. I think we're OK, Charlie.

ROGERS: And I'll -- I can try --

SCHOUTEN: I think we're good. We'll see how these clearances are processed, but I think we have an idea of how we think we should be doing it, and the federal DHS plays a critical role, and the information sharing is paramount. So I think it's, so far, working really well, and I think we're taking steps to add a ton of value to what we do.

ROGERS: OK, sounds good.

BRADLEY: Thank you, Charlie. This is the chair again, Mark Bradley. I'm now going to note that Greg Pannoni will be joining Charlie for the next presentation. They'll provide an update on the status of an initiative that sets for the National Industrial Security Program procedures for sharing and safeguarding classified information with certain private sector and other non-federal entities. They

discussed this at our last meeting, so this is kind of, I guess, an update.

PANNONI: An update.

BRADLEY: Yeah. OK, gentlemen?

PANNONI: All right. I'll start with this -- Greg Pannoni, again. So, as the chair mentioned last meeting, Charlie provided extensive, substantial information about this program. And if you look at the minutes, pages four through six comprehensively document the discussion, so I want to pick up from that point rather than rehash all the things that got us to that point of this classified critical infrastructure protection program under the NISP, the National Industrial Security Program. So, to advance the story, the president signed the implementation procedures on December 28th, 2016, and that's the beginning of implementation. There's a considerable amount of work, responsibility, mostly on the DHS side, the DHS secretary, but also working with DOD, slash DSS, but DOD is really the representative for DSS, as we know. So that process is just getting started. The procedures are designed to streamline the process for sharing and safeguarding critical infrastructure, classified critical infrastructure protection program information. And you know, as you may know from before, the vetting, reporting, and oversight

mechanisms under this program are less stringent than they are under the traditional NISP program, and that was done deliberately to get involvement from both parties, and, you know, we're operating under these cooperative research and development agreements, CRADAs, so it does fall under the NISP because of that. A CRADA is an agreement. It's a contract. So that's part of what got us to where we are, so I'm going to turn it over to you unless there are any -- maybe we want to wait for questions until Charlie updates.

ROGERS: I'll keep it short, but I'll give a little bit of an overview, too, of the hybrid. I mean, it's -- we were brought to the table to develop an alternative program by the National Security Council. They directed DHS and DOD to get together and to come up with an alternative program to facilitate classified information sharing with cyber, cyber-related, with the private sector. And there are people in this room who were involved. Kathy Branch and Keith Minard and Greg were involved in writing this, and it was a long process of negotiation and writing to come up with an alternative process that was -- both lessened the burden on companies and at the same time retained some of what was determined to be essential safeguarding requirements of any classified information sharing with the private sector. So the White House did sign it. It has a

long name. We refer to it as the hybrid. We're kind of lazy about that, but the long name is Additional National Industrial Security Program Procedures for Sharing and Safeguarding Classified Information with the Private Sector Infrastructure Entities. And some of the key elements that are waived for this program are that the private sector companies who will eventually get access to classified information would not be required to get a facilities clearance, would not be able to bid on a classified contract, would not be permitted to store classified at their location. But once they met all the requirements of the program, they could get security clearances that would enable this classified information sharing. The things that are required for this program to...

M: Sorry about that.

BRADLEY: Sorry about the interruption.

ROGERS: The things that are required to be in place for this information, this classified information sharing to take place, some are relatively simple, like creating security agreements between DHS and the company, and some are complex, which is establishing a foreign ownership, control, and influence, information collection, and evaluation process. And the complexity of this process is not completely under-- even the complexity of it is not

completely understood by me. The more we begin to scratch the surface, the more we require that we need to really -- it's going to be a challenge to stand up a full capability in DHS. So, having said that, the hybrid was signed on December 28th. We had internal meetings on December 29th in DHS. We went down to DSS, the Defense Security Service, on December 13th. We are working directly with them to help us understand what is involved in establishing this capability in DHS. We have one MOU signed with -- MOA signed with them. We have a person detailed down there full-time to begin to acquire that. There are an additional three other people in DHS who have been assigned to intermittently meet with people at DHS, collect documents. There are ongoing conversations on this. We have plans to meet with the NRC, because they have a program that we think we could -- anything we can learn, anything we can copy, steal, duplicate, anything that will help us move forward, we're urgently doing that right now. I failed to mention that, in order to implement this program, DHS had to become a cognizant security agency under the National Industrial Security Program, and that was actually facilitated by EO 13691 in February 2015. So we became a CSA a year -- about two years ago, but we've been just sitting around, waiting for the hybrid to be officially approved, because that was

the sole purpose of us becoming a CSA. And I think, even before I open it to questions, Keith, is there anything you want to add about this?

MINARD: No. It's Keith Minard, Defense Security Service. We brought DHS on board to help (inaudible) through the process. It's going to be a long process to understand FOCI analysis and mitigation. There's a lot of procedures, like Charlie said, that are required to be put in place, such as information collection approvals from the companies or entities they're going to be serving, and also, a key point, as he mentioned, working with the NRC. The NRC has some FOCI and mitigation processes that might be more like what DHS needs to do, so we're making sure that we get them with the right communities along the way to start understanding the processes as we go along.

M: Charlie, why don't you just give them an understanding of the approximate size, where we are today and where we project to be in a few years? I know you don't have hard numbers, but you and I have discussed this before --

ROGERS: Yeah, yeah. There are --

M: -- as far as how many entities under the CRADAs.

ROGERS: There are about 165 companies who have signed these cooperative agreements with DHS with the expectation that they will eventually be able to enter into the program, and

certainly there's a backed-up momentum or backed-up expectation. You know, these companies urgently want to get in the program. We've all been waiting for a couple of years for its approval, but we couldn't build a program without being a CSA, without having the hybrid sign. So, having said that, there are, I think, about 265. Maybe I've got that -- maybe it's 165. Anyway, there's approximately 200 companies -- let me put it that way -- that are in the background, but the program office in DHS has about a dozen that they urgently would like. So the plan is, one, we have to build the capability and as quickly as possible, as quickly as possible, which -- we haven't determined when that will be -- that we at least begin to get some of these companies in the pipeline. And the number is about a dozen that they would like to get in the pipeline, but we can't just put them in the pipeline until we are able to appropriately vet them and appropriately do all the requirements that are necessary for the hybrid, and we're moving as quickly as we can to do that. We have money in the '18 budget, both money and requests for personnel, to supplement this program, but we don't have -- you know, we're taking it out of [Hyde?] right now, and we're getting assistance from our partners in other cognizant security agencies. But, you know, we'll

be able to give an update at the next meeting of where we are. Right now, we're just urgently trying to understand all the things that need to be accomplished in order to implement it, and the most urgent thing we're trying to do right now is understand the information collection process, the forms and the FOCI evaluation. There will eventually be an oversight program associated with it, but that's not the most urgent thing we need to build now, so all of our people are being applied to the front end. And once we get that structure in place, then we can pivot back and build our oversight processes, and we have -- I think that's basically where we are right now.

PANNONI: Yeah, that's good. And one other thing, just once we get there, it's important to know that this is very much insular, these facility clearances or entity eligibility determinations. We're pivoting to that nationally in terms of the name of what we call facility clearances. We restrict it just to this program, so there's no reciprocity where they can take the fact that they're granted this entity eligibility and start bidding on contracts that involve classified information. They would have to enter the traditional NISP process in order to do that.

ROGERS: Yeah, and the real purpose of the program is to facilitate classified cyber information sharing. There are

-- the plan is to enable DHS and other federal agencies to share threat and risk information and to mitigate risk with companies by having classified information sharing, and that’s the goal. They wouldn't -- as we said, they wouldn’t store, but they could have six, eight, 10, 12 people cleared so that they could get the information they need to protect their networks and to feed back expertise to the federal community. Where we are now is trying to get there. We’ve got the approvals.

BRADLEY: That’s a good first start. Great. Good. (inaudible), right? This is the chair again, Mark Bradley. At this time, I’m going to introduce Tip Wright -- Wight, SLTPS Entity Vice Chair, who will make a presentation on the National Network of Fusion Centers. Colonel Retired Lee “Tip” Wight is currently the director of the DC Metropolitan Police Department’s real-time crime center. It’s quite busy as of late.

WIGHT: We just had our Super Bowl.

BRADLEY: Yeah. He was a director of DC’s fusion center from 2013 to 2016 and also served as the vice president of the National Fusion Center Association from 2014 to 2016. His briefing, entitled “Fusion Centers and National Strategy, National Asset, Local Resource,” will describe state, local, tribal, and territorial fusion centers and the

National Fusion Center Network. It will detail the national strategy for the national -- a lot of "nationals" here -- for the National Network of Fusion Centers, which was raised in -- issued in 2014 by the National Fusion Center Association. The presentation will also describe the federal framework to support the national strategy and will provide several examples of the many initiatives already underway and completed by federal, state, and local partners to strengthen the national network. Tip?

WIGHT: All right. Thank you, Mr. Chair. And I apologize to those folks, especially Russ Porter. I'll wake you up at about slide 24. I know you've heard portions of this, if not all of it, multiple times, and my colleagues in Florida and Iowa, I know you may be beating your head against the wall since we've discussed this so much. But I was asked at the last meeting to provide a briefing on this strategy, and, as I continue to work in this realm, it amazes me to the degree that people don't understand what a fusion center is, that the network, in fact, exists among all 78 of these, and how to leverage these resources, and, in fact, are unaware that there is a strategy now. And the intent of that, really, is to kind of standardize the delivery, I think, of this capability to both state, local, tribal, territorial, and, I should add, private sector as

well as allowing our federal government partners to leverage that as well. So that's the purpose of the briefing. I apologize; for those of you on the phone, I could not get the video, so hopefully the briefing, I assume, was sent out. And the slides aren't numbered, so I'll do my best to keep you up with where I am.

I'll turn to the second slide and just -- actually, before I do that, let me -- words matter. And I realize, as I sit here, it says "local resource." My intent with that is not just local entities. That really encompasses the whole umbrella of state, local, tribal, territorial, private sector. Anything below the federal level is my intent with the term "local" there, so put quotes around that, and don't anyone take offense. I wasn't trying to be exclusive in that. So, now, turning to slide two, again, there's a lot of misconceptions as to what a fusion center actually is. It's amazing how many times I either hear it mis-described -- and, you know, there's a lot of myths out there. It is what it is, but, just to clarify, these are not federally owned or controlled. That's the biggest thing. Everyone seems to think DHS owns these things. They are not. They are very much owned by the state, local, tribal, or territorial entity that controls these.

They do regional intelligence and information sharing. You know, the challenge with these -- although some of the things such as the national strategy and the FEMA grant program, the requirements under DHS I&A for reporting and evaluation have standardized them to some degree, they're still -- each one is unique, and I often get, "Why are they -- you know, why is each one of the 78 different, and, you know, why are there 18,000-plus police departments in America?" it's because each jurisdiction wants to tailor that service to their local needs. So I don't think -- you know, coming out of the military, when I first got into the fusion center world, "Gosh, they're not all the same? There's not standard doctrine or, 'This is how you build a fusion center'?" Well, no, there's a reason for that. It actually makes sense the more you look at it, and I would say they're probably, these days, more similar than they are different, but they are each unique, so that's important to understand, that some will have an investigative role, such as the Boston Regional Intelligence Center. They were out on the scenes of the Boston Marathon bombing, gathering evidence and helping support that investigation immediately after. Those such as my former center, the WRTAC in DC, were not. We had no investigative capability, and we're under the rubric of an

emergency management agency. But they all are multi-agency and have, you know – again, the composition in each will be very unique. We, in DC, had about 50 partner agencies that had a variety of different kinds of relationships, from having a full-time liaison officer detailed to us to virtual connectivity that we talked to every couple of weeks at a staff meeting at the end of a phone line. And, again, that varies across the national network, and what they are focused on will, again, depend on the jurisdiction. In DC, we were all threats and all hazards, and there's a doctrinal point there. You'll hear the term "all crimes," "all threats," "all hazards." What's the difference? Isn't a crime a threat and a hazard? Well, in the doctrinal world of this, the threat is a manmade thing out there, and a hazard is something naturally occurring, such as a hurricane or an earthquake. So when you hear that term -- and, of course, when someone professes to be all-crime, such as we did at the WRTAC, I realized that I didn't have an analyst, you know, for every possible crime that's out there. I didn't have a single analyst that focused on each of those crimes, but, guess what, within the network, the national network, you've got over 900 trained analysts out there. Generally, you can reach out and touch someone and find that asset if you need it. So,

while we didn’t have a human smuggling expert in the fusion center in DC, I could certainly reach out to our southern border fusion centers and definitely find an expert in that when the need arose. So that’s kind of understanding what they are.

Now, the other key, I think, to this brief and to understand fusion centers is understanding what they’re not. And like we said, they’re certainly not federally owned. We’ve been clear on that. They also don’t duplicate the mission of joint terrorism task forces, and I often get, “What’s the difference between a fusion center and a JTTF?” Well, first off, a JTTF is owned by a federal agency, right, and it has a single mission, counterterrorism, whereas in the fusion center you’re looking at all threats and all hazards. And most fusion centers -- some are just law enforcement and homeland security. Again, that depends. But, for example, you know, in DC we were certainly worried about terrorism, but we’re also worried about pandemic influenza and possibly Ebola, you know, public health threats, so keeping in mind that it’s not a single mission focus, whereas the joint terrorism task force certainly is, same thing with a HIDTA, a high-intensity drug trafficking area, again, a single

focus, and regional information sharing centers, again, a different mission and are not necessarily state, local entities.

So, with that being said, you know, there are, such as -- some fusion centers have very much a real-time crime center focus. You know, in DC, it's separate. The police department has a real-time crime center, which I'm now running, but the fusion center mission continues, and, again, those real-time crime centers tend to be focused just on that law enforcement mission whereas your fusion center has that broader -- and the real-time crime center has a very tactical mission focus. And again, while we may be collocated with an emergency management agency -- and, at least count, I believe five or six of the 78 were managed by emergency -- fusion centers were managed by emergency management agencies, they're certainly not just an emergency management program. Those are separate and managed by other agencies. And, like we said, they're certainly not all the same as, I think, you've gotten from the flavor of this.

The history is varied, and there's been a lot of documents written, as we turn to the next slide. You know, a lot of

people think that fusion centers started with 9/11. They certainly got a lot of focus after that from the 9/11 Commission, but I think Russ was around at the beginning where these things started. And the reason many of them are in law enforcement agencies is because that's where they started. The idea was intelligence-led policing, trying to get ahead of the crime blots, and, you know, let's interdict or prevent before it occurs versus picking up the pieces afterwards. And then, of course, after 9/11 we realized that, "Oh, gosh," we might be sharing information horizontally among agencies but not necessarily vertically as well as we can with our federal partners and getting that intelligence information down to that state and local level. And a variety of reports and guidelines for how we're going to share information have come out, various Congressional documents and investigations into them, some perhaps not as well-informed as they could be in terms of some that have been discredited. But in 2013, I believe, Majority Leader King did a good assessment of fusion centers and the House Homeland Security Committee and ended up putting out and saying, "Well, that's great. Actually, these fusion centers have come a long way, are performing well, but there is no strategy for them. What are you going to do? How are you knitting this all

together?” And hence, Fusion Center Association began working on this strategy in 2014. I was actually one of the authors of it.

Turning to the next slide, we produced this thing in 2014 in response to that, and if you want a copy of it it’s available out there on the National Fusion Center Association website. That’s NFCAUSA.org. It’s right there on the front. You can download a copy and reference that whenever you’d like. That next slide shows what’s in it, and I’m going to talk to it as we go, but understanding, turning to the next slide, this wasn’t something the NFCA developed in isolation. We worked with partners at the National Governors Association, Major County Sheriffs Association, Major City Policy Chiefs Association, ICP, HIDTA, and other agencies including Fire Service and Emergency Management, so it wasn’t something that three or four of us locked ourselves in a room and wrote. This has had broad circulation and support as we developed it.

Turning to the next slide, the intent of this, the idea is really to define the strategy of the national network, identify a path forward, and really talk about some of the effectiveness and demonstrate, really, what an asset this

national network is, and that's kind of the big picture here. As we talk on slide seven, key components of it, the mission of the national -- the whole purpose of this is to use these unique and leverage these unique capabilities that are out there. I mean, like I said, they're -- and this is where I get on my bandwagon briefly. When you have the talent and the capabilities that are there such as -- you know, like I said, we have over 900 trained analysts, and many of these are former, you know, federal intelligence community personnel that have either retired or decided they wanted to work closer to the mission at the state and local level. And to be able to leverage that skill set, they're trained to the same standards as, you know, federal analysts, and to be able to use that talent, which is why I talk about -- you know, when we talk about TS/SCI clearances, it still to this day makes no sense that when someone takes off their federal hat with that same training and goes to work for a state and local agency, the next day they're only cleared to a secret level. You know, that's mindboggling to me and just doesn't seem like we're leveraging those capabilities. So that's kind of the purpose of talking about this, the strategy in terms of receiving, analyzing, disseminating, gathering threat information and intelligence in support of those state,

local, tribal, territorial, and private sectors as well as federal efforts to protect the homeland. That's really the bottom line. It almost doesn't matter from what. It's just to help protect the homeland.

Turn to the next slide, key components. The vision is that, really, this national network has become and continues to be a multidisciplinary, all-crimes, all-threats, all-hazard, information-sharing network and really, foot-stomp on the next piece, protecting the nation's security while safeguarding the privacy, civil rights, and civil liberties of our citizens, and that is something that is really key. One of those myths about fusion centers that's out there is, "Oh, these are the local spy centers," you know, and nothing could be further from the truth. We all have privacy, civil rights, civil liberties policies. All comply with 25 C.F.R. Part 23 and continual training in ensuring that we are protecting those privacies, civil rights, and civil liberties, which goes to those values that we talk to on the next slide in terms of the respect, the integrity, and professionalism.

Turn it to the next slide, defining the national network, and this is in the strategy. This slide captures it, but

if somebody goes, “What is the network that’s actually defined in the strategy?” and, really, those key bullets, it’s a decentralized, distributed, self-organizing national asset, and I think that’s key to understand, “self-organizing,” right? There is no federal directive that all these entities participate together, but we do, and it functions quite well. And as we talked about, who consists of these? There are 78 of them, and recognizing that there are three in federal territories. The US Virgin Islands, Puerto Rico, and Guam have them as well, the ones you see on the map. The function of that network, on the next slide, really, the bottom line -- and we talked about it -- there are a lot of words in the strategy on it, but really what we’re trying to do is just trying to help keep people safe by producing intelligence and sharing information. That’s fundamentally what the network does, and helping enable collaboration across jurisdictions for a variety of reasons.

There are four goals, turning to the next slide, of the national strategy. Number one -- and, again, we put it as the first goal because that’s critically important to ensure we’re maintaining, and I guess, yeah, it’s a [build?] slide -- but protecting the information, privacy,

civil rights, and civil liberties, that’s key in everything we do. The next bullet is really talking about expanding the network of each fusion center. So, you know, while I had -- at the WRTAC, I had 50 partner agencies. Gosh, if you think of how many agencies are in DC, you know -- and, again, there’s no requirement that agencies share information with fusion centers, something I continually thought. But, boy, there’s so much out there, so really trying to expand the breadth and depth of each fusion center’s individual network is the focus of goal two, so some initiatives to support that.

And then, goal three talks about really strengthening and continuing to strengthen that national network. So goal one, privacy, civil rights, civil liberties; goal two, build that network for each individual center; goal three is, really, to enhance the overall national network. And then, goal four is, really, that vertical piece of connecting with our federal partners and strengthening the information sharing efforts that go along with that. I’ll walk through, on the next few slides, just some kind of specifics of the goals, and I really have kind of hit a lot of these, so I'm going to skim through these pretty fast, and we’ll get to some of the specific initiatives and talk

about that to give you a little more detail, some of the meat of the mission (inaudible) just words on slides.

So on the next slide, goal one, some of the key -- each goal has objectives underneath it and a breakdown and just talking about each of the initiatives. There are 37 initiatives that support this whole strategy, so each of those initiatives is walked back and nested under the objectives, which is why you'll see that broken out. But I already talked about the important of upholding that public confidence, and, then, each of the objectives talks to a separate aspect of that. Turning to goal two, again, we talked about the individual network, and, again, I just highlighted a couple of key objectives here because I can't remember -- it's been a bit since we worked on this, but I think there are probably six or seven objectives in this one. So you see just talking about opportunities for better outreach and engagement with state, local, territorial, private sector, ensuring that we've got visibility for local homeland security priorities in the fusion center, and talking about improving information-sharing within each of the areas of responsibility of these fusion centers.

Goal three, we're talking about the whole, overall network again and how can we leverage that, and some key objectives, centers of analytic excellence. You know, it's great if one fusion center is really strong and has some great tradecraft, if you will, but how can we make sure that we spread that out to the other 77? How is that available? Just because one center has a lot of funding or got lucky with some great analysts, how can we make that available to the network? And I'll talk a little bit more about that. And then, you know, gosh, if we're going to strengthen this network -- unfortunately, because each agency is unique and each has unique contracting practices and procurement practices and, frankly, funding availability, some, the systems that each fusion centers, end of being different, and they're not all interoperable or interconnected. So that is certainly a challenge when you're leveraging and when we talk about sharing information or having analysts from one center come to support another one. If the folks from Maryland walk into my center, you know, former fusion center, they could probably, you know -- once we get them swipe card access, they could probably answer the door and, you know, answer telephones. But to log in, they wouldn't have any ability to log in and use our systems and really leverage that

talent that we have, so how do we develop that kind of capability and interoperability? And that really ties to objective four. You know, if you do become overwhelmed and you need help from elsewhere, you know, we've got to train. We've got to practice. We've got to have those systems that we can use.

And then, go forward, talking about leveraging that partnership between and information-sharing between the federal partners and our network, talking about how do we collaborate, some key objectives on that, the formalized production of joint products. That has come a long way. Many of these initiatives are already completed in the federal framework, so I'll show you that. Certainly, in DC, we're doing -- routinely putting out joint products. In fact, the WRTAC just did one for the inauguration, a joint threat assessment for the inauguration with DHS, FBI, NCTC. And then, you know, again, there's a lot of talent out there. It's a separate mission, but how do we work with -- since most of the fusion centers have a counterterrorism mission, how do we work with the joint terrorism task forces and leverage that information back and forth?

So turn it to slide 37. I'll talk about these 37 initiatives. And, again, this is just nine of the 37 that are out there, but, again, talking to -- and, again, these all go back and nest under the goals and individual objectives. But talking about standardizing training, I mentioned I had at the WRTAC 50-something liaison officers. Well, is there a standard training program? How do they know what to do as a liaison officer? What's their role? Where do they get that? So developing a standard training program for DHS has helped out, and, when I say "DHS," I&A has helped us out a lot with that. We were doing some individual -- creating some training that was being standardized across the network. You know, going straight down, common technology services, you know, while we can't specify what a jurisdiction will buy -- because, again, there are different procurement rules and requirements -- what we can do is put kind of, if you will, a rating system or best practices and a kind of list that some of the systems are out there that work better, serve better needs than others. You know, we've talked -- like social media and research, almost every day I get a contract coming in and telling me they've got a great new system that we ought buy. OK, of all these systems, what really has worked the best, and what are some options that might be common among

some of the fusion centers? We're also talking about maybe, at the NFCA level, holding some licenses that can be used for some of these systems by the individual centers. Again, you get into different laws and what some states can do for privacy and realizing that some folks can do things that other folks can't. So there's a balance there, but that's kind of the gist of that.

Certainly, the Department of Corrections and correctional facilities, different rules apply on collection of information. There's a ton of intelligence there. Leveraging that and kind of making that process improve there is something that we strive to do. And again, just hitting a couple of these others, as you can see, improving cyber strategies -- certainly, at the time this was written, that was a huge growth area. I know our colleagues from Iowa are certainly all over this and looking to enhance that as well. It's still a growth area, but now the awareness, I would say -- probably all of the 78 know that this is an issue out there and are dedicating resources in the cyber area. It's kind of -- again, because capturing cyber analysts is expensive and it's hard to get really good ones, because the private sector can certainly outbid us, you know, how do we not rebuild the

wheel in all 78 fusion centers? How can we share and leverage that talent across the board. You know, standard comprehensive fusion center intelligence requirements of note, one thing to understand about fusion centers, we don't have tasking authority. So, unlike a federal intelligence agency where I can actually task collection, I can't do that at the state and local level. I always called it [ASKANT?]. I can pick up the phone and ask you if you can share your intelligence with us, but in terms of -- having collection requirements and standing intelligence requirements and refining those and keeping them current is the objective there. We talked about cross-training analysts between fusion centers and the role that we had in an exchange program with the Maryland center. So we'd actually send analysts to spend a week at the Maryland center, and they would send analysts to ours, so, again, they could do more and be of use in a crisis besides, you know, serve coffee and answer the phone. So they could -- they actually had logins and passwords and understood the systems and the products and our processes, and, again, trying to do that in a broader context within regions, because likely, if the DC center is overwhelmed, Maryland probably is, too, so maybe we'd need to reach up to, say, Connecticut or something for help depending on that. So

that needs to continue to expand, and then I've got a separate slide. I'll talk to some of the centers of analytic excellence on that.

Again, turning to the next slide, as I mentioned, there is a federal framework that complements the national strategy, and there were 40 projects identified with that. I list -- you'd think, "Well, if 37 are completed and three are in progress, it ought to be easy to come up with how finished you are." Some of those three that are in progress are, like, half-complete or two-thirds complete. So, rather than getting into fractions, because some of them -- or develop an MOU, the MOU has been developed, but it's awaiting final signature and things like that. So that's kind of -- it's almost complete, frankly, with some of those. The federal goals, there are four goals that kind of mirror the goals of the national strategy, and their first goal is, again, continuing to safeguard information while protecting privacy, civil rights, and civil liberties.

Their second goal is kind of standardizing that partnership between the federal government and fusion centers, and then goal three is really expanding the engagement along the

same lines, so, once we standardize how we do it, then expanding that engagement, really enhancing the core capabilities to improve the situational awareness in those centers. And then, kind of talking along the same line as one of the national strategy goals, really leveraging that national -- ensure that the federal agencies are able to leverage all that talent and information that's out there in the state, local, tribal network, because there is a lot of information at the state and local level that federal agencies don't have. Some of those projects -- and, again, Charlie just gave us a great rundown on some of those key projects that were in the federal framework to support the strategy, getting -- enabling TS/SCI clearances for state, local, tribal, territorial analysts, I will say, while it's probably not yet as smooth as it could be, it works. I had -- in DC, I had at least six TS/SCI clearances granted, and I don't know, again, across the national network what other -- how many other agencies have done that, but the process is there. It did work, and we're just looking to refine it, and we can talk about that as some of the action items as we continue to do it, but it is there, and it does work.

The other thing, there's a fusion center assessment program annually that was done by DHS, and I will tell you that was

cumbersome. There were over 300 questions. That was a month-long program, and you had to collect just reams of data. I ended up having to dedicate one person full-time, year-round, to collecting data just to support that assessment. And, you know, General Taylor, who's the departed I&A head, realized and got much feedback that that was just overly burdensome on fusion centers, so we revised it down. I think we got it down to about 10 metrics with kind of five key ones that the fusion centers had to collect the data on, and the other five that DHS collected the data from existing data that was already out there, such as our products that we post on the homeland security information network and others. So it really reduced the requirement while still managing to show the effectiveness of the network and tell the fusion center story and explain why federal money is being used to support these centers in most cases.

And then, another one is to really define where fusion centers fit in that cyber mission space. As you know, DHS has the requirement for that cyber defense mission nationally, so figuring out where to fit the fusion centers in, and talking about some of those common technology requirements, you know, common analytic training standards,

and really refining and improving those analytic training centers. We started talking about, you know, the talent that's out there. And then, there's an initiative to develop a national mission cell, which is to imbed a DHS analyst, not a reports officer but an actual analyst from DHS I&A, and an FBI analyst into a fusion center and products on site that address national mission priorities, generally counterterrorism.

M: Can we hold any questions until the end?

WIGHT: If you don't mind, let me run through this. I'll probably answer -- hopefully I'll answer most of these, but then I'll be happy to go back and cover anything you'd like to on that. Just on the -- you know, turning to the next slide, 21, I could go on for hours on this, the amount of collaboration that's out there, the success stories that have occurred because of fusion centers. You know, I'm not going to walk through each of these. I've got some slides. Just suffice it to say that the awareness -- and I am a big fan. Originally, I know [HSIN?] took a lot of hits for whatever reason, but, you know, in any developmental system I am a fan of HSIN. It works. The situational awareness from the sit room that's out there, you know, we were -- the nation was seeing what was going on in DC because we were posting the information in the sit room, both the

police department and the fusion center. Similarly, there is an awareness room -- it's called [CINAware?] -- for sharing cyber security information and, you know, threats to law enforcement, all that information that's happening. And you know, a lot of these things, especially in the cyber world, it's not a local issue. This is somebody maybe in a local area, but they're attacking, frankly, internationally or nationally as well. So, often, issues that occur in one area such as ransomware or you name it will pop up elsewhere, so having that ability to instantly share information about an attack and provide that information through the CINAware network is a great thing.

And, you know, turning to the next slide, we talk about Alabama and Chicago collaborating, just an example. You know, somebody in Alabama is looking at social media and got concerned about some postings that were on there, and they called their local fusion center. They did the see-something, say-something and notified the Alabama fusion center. And as they dug into this, it turns out that the individual was traveling up to Chicago where he stated he was going to kill some folks up there, and it was actually law enforcement numbers. And they passed the information to the Chicago fusion center, who actually tracked this

individual down, located him, and, sure enough, he had a basement full of weapons and his own shooting range in his basement where he was training for the attack and planning to go do it. The subject was arrested. You know, so that kind of collaboration, and that occurs daily across the national network. It's often -- what's the value of the national network? When you take a look at some of these success stories and realize what things have been prevented, it's amazing how much value there is. And, you know, I'm not going to go into and talk San Bernardino, but suffice it to say that the Northern California center was supporting a network of partners there that you see on that slide with information during that event. And frankly, here in DC, we were up to the minute, blow by blow, knew what was happening in San Bernardino, and, again, not from -- call this, in quotes, "cyber rubbernecking." We're not just interested observers, but we're trying to determine -- the first question that my senior leaders would always ask from one of these, quote, spectacular events is, you know, number one, is there any nexus to DC? Number two, is it part of a broader plan, and, number three, is it coming our way? So having that awareness of, you know, "This is an isolated event in this location," or maybe not, that kind of thing, or, gosh, there is information that -- say, in

the Ohio State incident -- the individual traveled to DC days prior to that. “Huh, OK.” That’s great information for us, and we can support the investigation with that.

Just touching really quickly on the centers of analytic excellence, the idea here is to share tradecraft. We talked about how some fusion centers are blessed with some great skills in a certain area, but other centers may not have that access. The idea here is to be able to share that and put the -- this isn’t necessarily to do their work for them, although you can certainly reach out and touch those centers if you need them, but the idea is to explain how they built up that capability, here’s how we craft those products, here’s how we trained our analysts, and put that information out there for the other 78 centers to access, or 77. One of those -- again, another great initiative, turning to the next slide -- is that fusion center cyber pilot. And going on to the next slide, what they really produce is a toolkit that really -- we call it a cyber security program in a box, which is out of the box, and there’s -- again, if you need access to this information and where do I get this toolkit, it’s all -- you leverage that on the DHS HSIN. It’s all right there as well as through the National Fusion Center Association

website and talks about -- you know, because again, as many fusion centers are getting into the cyber realm, “Well, gosh, we don’t even know what to put down for a job description. How do we develop a requirement to hire one of these? What are we looking for, and then what are some of the skill sets? How do we get them trained? What’s the career path, certifications?” And again, all of this other information is available to them there, and that’s been very effective.

There’s also a cyber intelligence network. That’s another one of these initiatives that’s out there, and, again, I’m not going to spend a lot of time on that for now. Just understand that, turning to the next slide, there are six regions each. There’s a coordinator and a deputy in there. There’s that SIN portal on HSIN where you’ve got over 300 cyber professionals sharing information. And, as I talked about, there’s that real-time situation awareness room, SINAware, that’s on HSIN where, again, that’s all available. Also, turning to the final slide, if you’re out there on the phone and you want to know where your contact is and how to reach them, that’s available there. And, again, you can get that on HSIN or through the Fusion Center Association. With that, I will stop talking at

least briefly and take any questions. I know there's at least a couple out there and any from the phone as well.

BRADLEY: Well done. Questions, please.

LICHT: Just a quick question about -- this is Rich Licht -- your 37 initiatives and key projects. There's no funding stream for that, right? That's largely self-funded.

WIGHT: Yes.

LICHT: Federal agencies -- it doesn't -- there's nobody that sponsors that effort.

WIGHT: No, other than -- understand that fusion centers themselves, 76 of the 78 receive some form of federal grant funding. You know, some receive a lot, like DC. We were 100% grant-funded, and some such as Louisiana and Alaska receive none. And then, other states, there's varying -- although it's a relatively small portion of most of the others, so that, while there is grant funding, there was none specifically earmarked for these 37 initiatives. Although, depending on what they are, some fusion centers may well have applied for a specific federal grant to support it, but, with the strategy, it was -- there wasn't associated funding earmarked out.

LICHT: There's no DHS standardization of technology through (inaudible) or anything like that for -- potentially for that. Has that ever been explored?

WIGHT: I'm not sure I understand the question. Standardizing, that is one of the initiatives DHS and [PM ICE?] is working to kind of provide, some of the standard technology services and recommendations that are out there. But, again, part of the challenge is different rules and different, you know, funding availability, but there are -- and that's through HSIN -- there are analytic tools that are available. That's one of the initiatives that are there that have -- some of these tools are made available on HSIN that anybody can use.

LICHT: A good answer to a bad question.

WIGHT: Any other questions?

EDERHEIMER: (inaudible). This is Josh Ederheimer from the DOJ Office of Tribal Justice. I know that some of the tribes' tribal police departments I know -- Tohono O'odham on the southern border and the Saint Regis Mohawk on the northern border, but are you getting tribal law enforcement participating? Is there interest or resistance, or how is that going? I know it's working out pretty well in New Mexico and Arizona, but I'm not sure about other places.

WIGHT: Yeah. You know, again, there is participation in the national network. Certainly, Arizona is -- I know they have tribal representatives that are, you know, a formal part of their center. There is participation in varying

degrees. It's much like the national network. It's individual. It's localized. There's no standard level of participation. I don't, you know, know the number, currently, across the network. I could probably find out, but it just varies by region, and, again, there's no directive that anybody has to participate. It's a voluntary, you know, self-organizing network, so it's where the individual jurisdictions see the value in participating or are aware of it, you know. And again, that's one of the things I did as a fusion center director, was constantly conduct outreach briefings to go, "Hey, your local fusion center is here. Here is what we can offer you. Please partner with us and share information with us." But I can't force anyone to do that, and it's that way with the tribal entities. Some participate and see it as a great value added. Others, for whatever reason, don't, but we do -- the network does get tribal information.

EDERHEIMER: Thank you.

WIGHT: Mm-hmm. Any other questions? All right, Mr. Chairman. I've either bored them to death and numbed them, or they have the information and no questions. Ah-ha!

M: So it ends in '17, so you're working on the next version or --

WIGHT: You know, that's -- I was just talking with the executive director of the [NSCA?] about that, and kind of everyone, with the administration change, had taken a bit of a breather while we got through the election and the new administration. But he said his first priority is to assess where we are on this and then, obviously, see where we need to go for the next, so that will be an action item coming out. Yeah?

CUMMINS: I have to say I really enjoyed this. I was engaged at the policy level. Russ and I worked -- I think we met over the fusion center guidelines as we were working to write that first version, but with policy, you know, you get stuff in place, and you have to move on and do some other policy. But I really, really enjoyed your briefing.

WIGHT: Great. Thank you.

BRADLEY: Another high note, Tip. Thank you. This is the chair again. I'm now going to introduce Dr. Patrick Viscuso, the associate director of controlled unclassified information of ISOO, who will provide an update on the status of the implementation of the CUI program. Pat?

VISCUSO: Well, thanks very much. It's a real pleasure to be here. In fact, we have worked with state and locals in the past, and I recognized some names on the phone and here, and I'd like to work more closely in the future. We do

need the valuable input of this community in order to form guidance that makes some sense when it comes to the handling of this type of information, which is highly valued by this community. And I'd like to begin this presentation -- there are some people here that are new to CUI, so I ask those who are very familiar with it to bear with me, but, at the same time, I do want to bring people up to speed. Let's hold questions for the very end, because I'd like to be able to give the presentation as an organic whole, and then we can have an opportunity to discuss.

So I'd like to begin by actually describing the -- if we could go to the next slide, which is slide two, I'd like to describe the current problem in the executive branch. We have -- for information that's unclassified, that law, regulation, and government-wide policy tells the executive branch to control or protect, we have within the executive branch over 100 different systems for protecting this information, and it's reflected in over 100 different markings. And, often, there isn't even agreement on what the information is that we want to protect, and certainly there is no agreement on how to protect it. That is not a good situation, and it can lead to a lot of problems in

information sharing. And where information does take place, it can lead -- due to the fact that many of these agency policies are not freely available, it can lead to either under-protection, putting the information at risk, or overprotection, again, restricting the information in terms of its sharing and its flow. Now, if this is the problem within the executive branch, one can only imagine what there may be going on when this information is shared with nonfederal partners, law enforcement, state law enforcement, and others.

If we could go to the next slide, in order to address this problem, civil administrations have attempted to come up with solutions. There were solutions under the Bush administration, and there was a solution that was developed under the previous administration, and that solution had a very large participation in its development. The whole executive branch, really, the major partners in the executive branch, major partners in the state and local, tribal, private sector community, many were participating in the development of that executive order, which really expanded under the Republican regime into public administration. The problem was localized to terrorism information. It was a recognition that this problem had a

wider expanse, and the executive order addressed all of the information that requires protection within the executive branch that's shared with state and local, tribal, private sector. It addressed it in general.

So what did it do, this executive order? It established, in place of over 100 different systems, one system. It established the CUI program. It designated the National Archives as the executive agent, and the Information Security Oversight Office has now -- was delegated the responsibilities as the executive agent, and it did something extremely important. It established the criteria of what needed to be protected, and that's captured in that third bullet, what the law, the federal regulation, and the government-wide policy said to protect, establish an information [type?] in that law, regulation, government-wide policy, and said, "Protect this." Now, the problem -- and this is why we have over 100 different systems in the executive branch right now for doing this -- is that, often, the law, regulation, and government-wide policy didn't tell you how to protect it, so well-meaning agencies developed their own policies on what that meant. And, consequently, you have the problem we have now. You have the marking [FOUO?], and a number of agencies mean

different things by “FOUO” and have varying sanctions for what happens when you, in an unauthorized manner, release FOUO. So there’s a problem. Well, the CUI system is meant to fix this problem, so we have, now, one scope of information, one criterion for that scope of information, and we, as executive agent, were charged with the responsibility of establishing a registry. Next slide, please, that’s slide four.

The executive order wanted to make clear to the entire executive branch, to all of our partners what needed to be protected. So the idea was to establish an online public registry of all the categories and subcategories of controlled unclassified information that everyone was required to protect. And so, we had a data call out to the entire executive branch and asked them, “What do you protect now on the basis of law, regulation, and government-wide policy? How do you mark it? What are your policies?” And we received over 2,200 submissions, which we evaluated based on the criteria in the executive order. We sifted through them, and we came up with 23 categories, 84 subcategories, and we linked each one of those categories and subcategories to the law, regulation, and government-wide policy that established them, that said, “Protect this

type of information." And we also listed the sanctions that were associated with each one of those categories and subcategories, a very important point if you were establishing one system for the entire executive branch.

Our next task, and that was -- if we go to slide five, after establishing what needed to be protected -- and we completed, by the way, that registry in December of 2011. After establishing what needed to be protected, then we had to come to some sort of agreement as an executive branch on how to protect it, what that unitary standardized system would look like, and we captured that through five years of work in the 32 Code of Federal Regulations, Part 2002. We developed it through three years of informal coordination, which included input from state, local, tribal, private sector, but we had others, too, in addition to the key agencies of the executive branch that would be affected by this regulation, 28 major agencies that constituted most of the federal budget. We based the -- we had a council. We based its composition on the Chief Financial Officers Council, and we consulted with them three years. We asked them a key question: how do you protect this information right now? How do you safeguard it? How do you share it? How do you destroy it? How do you control it? How do you

mark it? How is it protected in the physical and electronic environments? Because we incorporated -- we wanted to incorporate the electronic requirements because most of this information exists within the electronic environment. And we were instructed by the president and the executive order to be consistent with the FISMA, with NIST guidelines and standards and OMB policy, not to create a parallel electronic set of requirements but to be consistent with those that already exist for protecting information that the law, regulation, government-wide policy requires protection of.

And so, we came to an agreement. We went forward with the OMB process, public rulemaking. After three years of informal coordination, we did two years of formal OMB public rulema-- OMB-managed public rulemaking, and the result was the 32 CFR 2002, which underwent public comment, including many comments from state, local, tribal, private sector community, but, in addition, many from industry and academic. We held numerous meetings during the public comment period, also during the formal-informal development, and I can say we received between 1,800 and 2,000 comments and proposals that we considered in crafting the 32 CFR 2002 to establish a baseline for protection.

Now, there are some things, I think, that this group is very interested in, and, if I had to kind of sift through, there are many things that I think this group would be very interested in. I'd have to just -- it was hard to pick one, due to the limits of time, but I'm going to pick one, and that is the cyber-security requirements, because, if I know anything about state, local, tribal, private sector, this is a big-ticket item. This costs a lot of money. How does a tribe upgrade its security, its IT system, in order to receive government information? And we considered this very carefully, and I'm going to describe how we approached this problem.

So, if we could go to slide six, let us return to the purpose of this program. What was the purpose of the program? Many things, ultimately, to make sure the information could be shared, but undergirding that was its common protection, its common marking, and the common definition of what that information actually is. But part of that is uniformity and consistency in the definition of protection, and we were told to do this consistent with the OMB policies, the FISMA, the NIST standards and guidance, so we did, and we prescribed a safeguarding standard. That

safeguarding standard is no less than moderate confidentiality. Confidentiality relates to safeguarding. That is what we were talking about, safeguarding. And when we say no less than confiden-- no less than moderate confidentiality, the term “moderate” is a key one. If the law tells us to protect something, it means to go beyond how we normally treat anything. In other words, if the minimum that we treat any system within the executive branch is low, when the law says, “Protect it,” it probably means something more than low, hence moderate. And most government agencies do have a moderate baseline for the protection of information that the law says to protect, particularly privacy information. Privacy information is protected at a minimum of moderate.

And so, we prescribed in the federal rule no less than moderate as a standard for all the information that the law, federal regulation, government-wide policy said, “Protect.” It’s up on the registry. However, that poses a very important problem for the state, local, tribal, private sector, and also for contractors to the government. If we could turn to slide seven, simply by receiving federal information to do something for an authorized purpose -- and we recognized in the federal rule, based on

our input from this community, that there are purposes, legal purposes, that have to be recognized. And when we talked about lawful government purpose, which is the standard by which this information will now be shared, we defined it in a particular way, and I'd like to read it, because I think it's important to this community: "Lawful government purpose is any activity, mission, function, operation, or endeavor that the US government authorizes or recognizes as within the scope of its legal authorities or the legal authorities of nonexecutive branch entities such as state and local law enforcement." So there's a clear recognition of the needs of this community to share the information for lawful purposes within the scope of its legal authorities.

But, again, if you are sharing this information for that reason, to fulfill a lawful government purpose, does this mean when you receive the information that you now are required to build a federal information system? If any of you are familiar with the requirements for building a federal information system, I would refer you -- if you're not, I would refer you to an interesting document. It is called the NIST Special Publication 800-53. It is about 500 or 600 pages long. It contains controls organized

according to families. This is basically a blueprint of how to build a federal information system. It is divided according to low, moderate, and high controls, and if you have something at moderate it assumes you have built all the controls that are at the low. It's very complex stuff. It is based on a lot of sources including congressional legislation. Some of the congressional requirements are not related precisely to security but are related to other concerns. There are requirements that get down to the point of whether you should set your computer to Greenwich Mean Time or not.

So it was thought, "How do we solve this problem?" Well, the first thing we have to do is go to the FISMA and really distinguish, according to the FISMA, what is a federal information system and what is a nonfederal information system. A federal information system is one that is operated by someone on behalf of the government. It is operated by a contractor, for example, on behalf of the government. It can be an email system, a payroll system. It can be an IT system that's built by a contractor. That's a federal information system. A nonfederal information system is one in which, for example, someone has received information incidental, for a contractor, to

providing a service or product to the government that's not processing. It can also be a tribal organization that has received the information for one of its lawful government -- for a lawful government purpose. They are not operating an information system on behalf of the government. Simply by receiving the information you're not operating a federal information system.

We recognized this. We teamed up with the NIST and developed this publication called the NIST Special Publication 800-171. We went through the entire catalogue of controls, the 853, and eliminated those controls that weren't related to safeguarding, that had nothing -- that were specific to federal concerns in addition, some of the ones I talked about before that were enacted by Congress that have, really, nothing to do with safeguarding but have to do with some political concerns, for example. And what we ended up with was not a set of controls but a requirements document, an objectives document organized according to 14 families that related to the definition of what good information security was in terms of safeguarding and set out objectives that could be met in a variety of ways, and we built flexibility into the document. The latest revision is December, December 22nd of this year, in

which we set out the requirement that the nonfederal entity that would be following this document would have a security plan that could set out where it was in terms of beating the objectives of this -- of good information security, so they could say, “We’re 40% there,” in that document and then set out a plan by which they could mete out the other 60%.

Why is that important? Because the government partner then could make a risk management judgment on sharing the information. These are -- so I’d like to leave you with two important points: it’s an objectives document, a requirements document that sets out goals for the nonfederal entity so they can get to them in a variety of ways, and it allows them to build into it a security plan that captures where they are right now and where they want to go. In both instances, there’s plenty of flexibility for a judgment to be made by a government entity in terms of whether to share the information or not. They can determine whether they’ve actually met those goals and how, and whether that’s sufficient for them to share the information.

Now, just a hint of where we're going to go with this with the contractor world, the next slide, slide eight, our intention is -- again, one of the intentions of the program is standardization, and what we intend to do is to propose this year a federal acquisition regulation rule that will be incorporated into procurements that are -- by the executive branch. Now, what would be some of the considerations in addition to levying the requirements of the program for protection of this information on nonfederal partners? Some of the considerations that we will be addressing will include how to identify the information sufficiently on the government side so that everyone knows what needs to be protected and, at the same time, highlight anything that's not standard in law that would -- that the nonfederal partner must follow in order to adequately protect the information and not break the law. We also will have a way in which we will capture information necessary for oversight, at least for contractors. We're dealing with an immense population. We will make use of current government systems to do this, to track who is holding CUI among the contractor world. Currently, in the system, the SAM, which is the System for Acquisition Management, which is the standard system that all contractors must register in. There are currently, in

terms of registrants, 350,000 registrants. These are contractors, grantees, and licensees. If only two-thirds of them hold CUI, you're talking about a population of 200,000. What we intend to do is levy that system in order to track who has CUI today so that some decisions can be made about who needs -- you obviously can't look it all over, so who needs to be examined more particularly for oversight questions.

If I could progress a little bit more, slide nine -- so that's what we're doing with the contractor world. I'd like to talk about the implementation of the program for the executive branch. With OMB, we negotiated, and with the CUI advisory council, 28 of the largest agencies in the government that control most of the federal budget, we negotiated deadlines according to which this program will be implemented. The deadlines are captured in a notice that's online, our CUI Notice 2016-01, that set out some basic things that seem very common sense, development of policy first by agencies. These are very large organizations, so they must develop their internal policy to be consistent with the CUI program. Then, they have to train their employees. At the same time, they have to look over their systems, because some of them are not at

moderate confidentiality. Some of them are at low, and I'm sure everyone in this room knows the problem of data breaches in the executive branch. So what is called for is an inventory of those systems and then a plan by which those systems will be brought to moderate confidentiality.

The physical security requirements of protecting this information are not burdensome. If it's in paper form, physical form, it's one physical barrier, and we have that explain in our rule, what that means. So we anticipate a kind of soft interim operating capability at year one that will mainly deal with the physical, and the division and development of policy and training. And then, by year two, optimistically, we're talking about the full implementation of the program. We have built into this timeline flexibility. In actuality, we think, although these are very aggressive timelines, that, actually, we're shortened when we went to OMB with our initial ones. We think that, in actuality, if we are flexible with these timelines it will take longer for agencies to develop their policy, to train all their employees, to inventory their systems. We think a more optimistic view is five to six years to implement this program in the executive branch.

Slide ten, so these are the main elements that we usually address with agencies in terms of implementation, and I think they have some relevancy for this community. I think everyone that is involved in information security and management must know that, in order to do it effectively, you have to have policy. You have to have someone that manages the program. You have to have training. You have to address physical safeguard systems. You have to have some provision for reporting incidents. You have to inspect yourself, and we know that state, local, tribal entities and agencies will be modifying their agreements and contracts to reflect the new program. When will this occur? When the agencies themselves have begun to implement the program in a meaningful way internally, then they will modify their agreements, because it would make sense if they're going to, for example, use the CUI markings, which are online. Then, they would have to be using them themselves, first, before they began to require others outside of their agency to use them.

If we go to slide 11, I have outlined here the main elements of the registry. There are some things here that I could discuss in some detail. I'd be more than happy to take some time to do this, but I think I am limited right

now in doing so. I will say a couple of just things that might be wondered about in terms of legacy information. Particularly for state and locals, if you deal with a major database that's online that has thousands upon thousands of PDFs, it's probably running through your mind, "How in the world will they -- if it's going to go under a new system of marking, how will they remark all of those?" And so, we've built flexibility into this rule based on input that we got from the agencies and from state and local that we can do these things in a much more creative manner. We can put a flash screen up and alert people that the information is CUI without having to remark every PDF. Legacy information in general, agencies have a great deal of flexibility in determining whether it should be remarked or not. The general rule of thumb is that if you're reusing the information, putting it into a new document, you should remark it.

Slide 12 has some very valuable things that I would point to your attention. I could have gone on for much more. This briefing normally lasts an hour and a half because we're trying to give people an orientation to the program, but we have several virtual briefings that anyone can attend. We have one tomorrow from 10:00 to 12:00. We have

one on February 14th, one on February 22nd. The times are listed here, and we have a large in-person briefing scheduled for January 27th, this Friday, at the William McGowan Theater in this building, the basement. Anyone can attend this. You will get the same information at all of these briefings, but, in particular, we are inviting nonfederal partners to the February 14th and February 22nd briefings. The content is the same. The questions are the same. This program is meant to be shared, and the guidance on it is meant to be open. That is, I guess -- I hope I did not take too much time, but if we have some questions I can briefly answer them. Otherwise, I do invite you to attend any of these briefings. I think they can be very informative.

M: Is this (inaudible)?

VISCUSO: Yes, it was. Yeah, and I kept -- I had that in mind with the people on the line, because I kept trying to refer to the page numbers. And we do -- we have a number of other briefings that I can provide electronically. We are -- we have a plan to put up a video of one of the larger briefings right off our website. That should be going up very soon. It's going to be based on the -- it's actually being videoed on Friday when we do the big briefing. That briefing, we've invited contractors, state, local, and all

the smaller agencies in the government and entities that have not had an opportunity for exposure at this point. Yes?

M: And how are you providing notice to the nonfederal partners about the February 14th and 22nd presentations (inaudible)?

VISCUSO: I'd like to -- this is where I need your advice.

M: I'd be happy to help.

VISCUSO: I would be delighted. And if there's anyone listening in on this phone call that has any ideas how we may obtain greater input from this community, at the end of the briefing on slide 13 I list my contact information as well as both of my leads for implementation and oversight. But feel free to, please, contact me directly. I am eager to hear any input and insights that you have and to, most of all, understand your needs and concerns so that in future policy guidance we can address them.

M: Thank you.

BRADLEY: Any more questions for Dr. Viscuso? All right. We're now going to turn -- this is the chair, by the way. We're now going to turn to the open forum discussion, which is kind of a bit of a free-for-all, I take it, so anything that's on your minds. And we especially encourage our new members to speak up, any problems that you're having or anything you'd like to have a wider discussion about.

Please feel free to speak up now, but, anyway, we open the floor, so take advantage of it. No? I know some of you very well. I know how you like to talk. I'm a bit surprised, but nevertheless -- yeah?

Wight: Well, I've got one. I didn't know if some folks on the phone might want to jump in, but just to be clear on the TS/SCI access for state and local, the next steps on that. Just understand that we'll probably never get the policy, at least soon, to where -- you know, I understand at the TS/SCI level it's got to be a federally-managed facility to have the physical machines in it that can process that. And I got New York City and Chicago, and there's some funding in (inaudible) some of the other major cities down the road. That's great. But to help, you know, Iowa and places where that may not be as easy, the real challenge there is just getting the analysts the ability to have -- once they get the clearance -- to get a JWICS account. So then, they can go into that sponsoring SCIF and, at least, log onto the machine and share information and actually process the TS/SCI, because right now the clearance will get you in where you can attend a meeting and read a document, but you can't process it.

M: Understand. Right.

Wight: Right. So that's the real challenge, being able to do it without being detailed to a federal, you know, program.

M: Sure. I got you. Yeah.

Wight: Of course, the defini-- maybe it's as simple as changing the definition of what "detailed" means. You know, if that means I go over there once every two weeks and that counts as being detailed, fine, but it kind of -- yeah, I don't know. It's just -- you know, there's a lot of pushback in that.

Rogers: Executive Order 13549, you know, it talks about the operating level being "secret," and then you can get TS/SCI at the discretion of the agency. It also says access to classified systems are in accordance with agency policy, so we have to go back to the agencies that are managing the TS/SCI networks in order to understand what exactly their policy is. And that's the key, because the executive order doesn't say --

M: No, it doesn't.

Rogers: -- that doesn't direct the agencies. It says they still govern their system and policies.

M: (inaudible) left that way.

Wight: And one follow-on to that, just in terms of getting the access itself, we have to have a SCIF owner sign off on, you know, the access and that they will do the [read-

ins?]. When that initially came out through DHS, it said, "It can't be DHS," which, you know, didn't kind of make a lot of sense. We were fortunate here. We were able to find another federal agency, but in a lot of cases, for our partners out there across the nation, the DHS facility may be one of the only, you know --

Rogers: Yeah, I wasn't aware of that. That's in the I&A document.

Wight: So it may have just been the newness of it and the interpretation, but for us it made a lot of sense to be able to go, "Well, OK, DHS, I&A, how about sponsoring it?" "No, no, it can't be us." So I'm not sure if that was a miscommunication or something is actually written down.

Pannoni: It sounds like it. If they accredited the SCIF, if DHS accredited the SCIF, they should be able --

Wight: Yeah. I know. One would think, but it just -- like I said, I don't know what that was, but we were told it had to be an other-than-DHS facility, so that's something that we may be working on.

Rogers: Yeah, I could ask about that. I'm not --

Wight: It may just have been a simple miscommunication or the newness of the policy, but that is something that I know we ran into, and other agencies may have that problem.

BRADLEY: Anything else? Before we wind up, let me just remind you of our next meeting. The next SLTPS-PAC meeting will be held on Wednesday, July 26th, 2017, 10:00 a.m. to 12:00 noon here, in the National Archives, so please mark your calendars. We conclude. Thank you so much for coming. I think this was worthwhile, and, again, this is an incredibly important board, it seems to be, after, especially, hearing these briefings. So, anyway, thanks again for coming, and we are adjourned.

M: Thank you.

M: Thanks.

END OF AUDIO FILE