State, Local, Tribal, and Private Sector Policy Advisory Committee (SLTPS-PAC) Meeting

Moderator: ISOO
January 29, 2020
9:56 am ET

Mark Bradley: All right, let me start again. Welcome. I am Mark A. Bradley, Director of ISOO and also the Chair of this committee.

This is the first one of 2020 and the 17th overall. This is a public meeting subject to the FACA, the Federal Advisory Committee Act. The Minutes will be available to the public.

A couple of ground rules is that when you speak please identify yourselves first before you say anything because again, we're preparing a transcript for the public. And it is a lot easier for us to reconstruct what was said by actually having a name and a title to go with what the quotes were. Otherwise we have to guess and I think we're pretty accurate but pretty is not good enough so let's try to do it 100%.

Anyone who's making a presentation who doesn't sit here, I guess just have a couple. Can go up to the front of the room here and use the little podium we have.

If you're on the phone, please mute your cell phone, right, before you…

Greg Pannoni: Yes.

Mark Bradley: …talk. We've had trouble before with echoes and all sorts of strange audio things.

We've had some membership changes since we last met. I'm pleased to introduce four new SLTPS members. Eric Tysarczyk, Director for Preparedness New Jersey Office of Homeland Security and Preparedness who's on the phone I believe.

Eric Tysarczyk: I am. Thank you.

Mark Bradley: And you're welcome. Tiffany Olson Kleemann, General Manager Distil Networks, Arlington, Virginia, who's here I believe Tiffany.

We have Meghann Teubner, Director of Counterterrorism Intelligence Analysis NYPD attending, right. I figured that was you.

Mary Michelle Schechter, Director, Division of Community and Maternal Child Health Nassau County Department of Health New York who's on the phone I believe. Oh I guess we'll find out a little later.

We're going to get back to you all in a bit and we'll have you actually tell us a little bit about yourselves. Not now though but we will.

I'm pleased to report that the SLTPS our members selected Marc Sachs as their Vice Chair and I approved his selection. Marc's been active with us since 2018 so again congratulations. You're welcome. No or mine too.

A couple of vacancies, we have one on the SLTPS entity membership vacancy. We have (Dory Korn), a Detective and Supervisory Task Force Officer of Las Vegas Police Department has completed his term. So we're one short now on your side. So I'm going to ask you all to please submit some nominations for us.

Just for sake of geographic diversity it would be nice to have somebody west of Mississippi River. I'm not hard over on that but we'd like to have the country represented itself. I know that due to budget constraints we can't pay for the person to come which I understand that there's a hardship.

But still just in terms of being able to look at the entire country it would be useful again to have somebody west of the Mississippi River.

Okay on the federal side we have a new member from the Department of Transportation. Welcome to Dr. Sidonie Dunham. I guess on the phone too I suppose, right?

Greg Pannoni: Right.

Mark Bradley: Yes, okay. And we have vacancies now in three agencies. We have to fill. Two are fairly recent, the NRC and the Federal Bureau of Investigation so we'll be looking for new appointments from them.

And we also have one from the Department of Defense.

Greg Pannoni: Right.

Mark Bradley: So we need to have those filled. Federal members, it's been a year now since we've seen your Financial Disclosure Forms. So we're going to have to ask that they be submitted. Again I'm not asking for new forms. Just submit the ones you normally submit for your own agencies. That's good enough for us.

Reason why we're asking for that, the bylaws require them, I don't see them. Our General Counsel (Nora) does. So again just kind of a pro forma thing to make sure there are no conflicts of interest.

All right, with that let's go around the table and introduce ourselves. Greg, I'll go to you…

Greg Pannoni: Sure.

Mark Bradley: …first. Yes.

Greg Pannoni: Thank you. Good morning. I'm Greg Pannoni. I'm Associate Director ISOO and the designated Federal Officer for the meeting.

Marc Sachs: Good morning. Marc Sachs, the Vice Chair of the – on the SLTPS side and I am the Chief Security Officer at Pattern Computer, a startup out of Seattle.

Meghann Teubner: Good morning. Meghann Teubner. I'm the Director of Counterterrorism Intelligence Analysis with the New York City Police Department.

Tiffany Kleemann: Tiffany Kleemann, Senior Vice President now at Imperva Corporation, just Distil Networks just got acquired, my company. So thank you.

Mark Bradley: Congratulations.

Tiffany Kleemann: (Unintelligible).

Patrick Hogan: I'm Patrick Hogan, USDI. I fill in for DoD till we designate a member.

Earl Camp: So Earl Camp, FBI, filling until FBI designates a member.

Martin Earring: Good morning, Martin Earring, staff assistant, Office of Tribal Justice and the Department of Justice.

Valerie Kerben: Good morning, Valerie Kerben, I'm the DNI Representative, Senior Security Advisor.

Leo Masciana: Leo Masciana, State Department, Diplomatic Security.

Rich McComb: Good morning, Rick McComb. I'm the DHS Chief Security Officer.

Charlie Rogers: I'm Charlie Rogers, the Vice Chair of the DHS Representative.

Mark Bradley: All right, let's go to the phone, anybody on the phone want to introduce themselves?

Glenn Bensley: Yes, Glenn Bensley, Assistant Director, Security Staff, U.S. Department of Justice.

Eric Tysarczyk: Hi. Eric Tysarczyk, Director of Preparedness, New Jersey's Office of Homeland Security.

Darryl Parsons: Darryl Parsons, Nuclear Regulatory Commission.

Jessica Davenport: Jessica Davenport.

Marc Brooks: Marc.

Jessica Davenport: Florida Fusion Center.

Marc Brooks: Good morning, Marc Brooks, U.S. Department of Energy.

Adam Walker: Hey good morning. This is Adam Walker at DHS Office of Intelligence and Analysis, State and Local Partner Engagement.

Tom Woolworth: Good morning, I'm – my name is Tom Woolworth. And I am the past President of the National Native American Law Enforcement Association.

Mark Bradley: Anyone else on the phone.

Patrick McCurdy: This is Patrick McCurdy. I'm with the Defense Counterintelligence and Security Agency filling in for (Lynn Weber) and (Emily Enterline).

(Trisha Franicar): This is (Trisha Franicar), also from the Defense Counterintelligence and Security Agency. I'm sitting in for the Executive Program Manager of Policy and Procedures.

Mark Bradley: Okay anyone else. All right, thank you, I am going to turn it over now…

Greg Pannoni: Don't you want to introduce these folks here?

Mark Bradley: Oh I'm sorry, yes. Don't want to get behind us.

Darrell Jackson: Oh.

Mark Bradley: Yes, yes. No.

Darrell Jackson: My name is Darrell Jackson. I'm with Compliance, Standard and Training Division at DHS.

Mark Bradley: Right.

Steve Buckley: Steve Buckley with I&A Security Management (Press).

Nicole Stone: Good morning, Nicole Stone, I'm (unintelligible).

Mark Bradley: Okay thank you. All right, now I'll turn it over to Greg Pannoni, my Deputy.

Greg Pannoni: All right.

Mark Bradley: And designated Federal Officer.

Greg Pannoni: Thank you.

Mark Bradley: Some of our old business.

Greg Pannoni: Thank you. Thank you. Thank you, Mr. Chair. So first the Minutes from the last meeting that we had in July should be in your packages in case you need to refer to them. From the last meeting we had two things that came up. And we're going to – I'll discuss them a bit and then we'll hear from some of the participants on those two items. They both resulted in holding of Working Groups.

So let me take the first one was the issue of clearances and the database of clearances. Those of you who have been attending for a while know that we've been discussing this issue for at least two years, maybe three.

And in a nutshell the issue is that the SLTPS constituency, which is mostly cleared at the secret level, although some have top secret SCI, do not generally have visibility. Maybe that's too general of a statement. But those clearances are housed in separate databases depending on the clearance level.

So they certainly don't have visibility for the top secret SCI clearances, which as those of us on the government side know are in the Scattered Castle System.

The Central Verification System is supposed to be the database according to law. Those of you may recall the IRTP or the Intelligence Reform of Terrorism Prevention Act established that there will be a Central Verification Database System for all cleared people, not just SLTPS.

I'll remind you of the order for this program, the Classified Program for State Level Tribal Private Sector, requires that by way of the order of the President that there be a Central Database Tracking System that the Executive Agent, DHS, shall maintain in coordination with other bodies that are involved with those other databases so in coordination with ODNI, DoD and I believe it says OMB.

The issue at hand like I say is the visibility, the ability for our nonfederal partners to know where their clearance is, the date of the clearance in order to direct someone for example if there's a meeting that they have to attend, and they have to provide that information to someone who can then go and validate it, they need to know where to go to see it.

So there was two, maybe more than two agencies in particular where this surfaces as an issue, FBI which uses Scattered Castles when they process SLTPS persons for clearances and then DNI for CIA who I understand does the most of the clearances in this space, in the SLTPS space.

So we came together with a meeting in early December to discuss the matter. The takeaways that we had were that the FBI working with DoD, in particular DCSA would furnish. Oh again too much technical terms. What they call a flat file. To the FBI that was my understanding, was very easy to use and from that essentially upload data from the Scattered Castles that relates to the clearances of the SLTPS personnel, which could then be connected, conveyed to, stitched together, whichever term you want to use into JPAS or whatever the system of record is. I know that there's been some changes in DoD, the defense information or Investigative Security System. And I'll refer to you in a moment Patrick on that.

And then at the same time we asked DNI representing the Intel community to reach out to CIA and any other Intel component to see how many cleared individuals they had sponsored and processed under this program.

So I know there was some movement within the FBI and DCSA. So we're encouraged by that. I understand in terms of looking at something this morning that DNI did reach out to CIA. But the response was that they're not tracking this population.

So as I mentioned we do have an Executive Order that says this is supposed to be done. It does of course give the Executive Agent the primary responsibility. But it also at the same time gives agencies the responsibilities to furnish that data to DHS so that they can populate, fashion, stitch together again, however we want to term it. Some sort of a central database so that we know essentially where all the cleared SLTPS population is.

So with that I'll stop. But before we move to the second item, I want to turn to a couple of people in the room or on the phone. First, if I heard, I'm sorry I didn't catch your last name, Earl from FBI. I thought that's what I heard in the introductions, if you're on the phone.

Earl Camp: You did. That's Earl Camp, C-A-M-P.

Greg Pannoni: C-A-M-P. Thanks Earl. Could you give us an update from the FBI perspective on this issue please?

Earl Camp: All right. So I apologize for the confusion. So previous representation on this committee was from the technical side of the house for us, it was from our Office of IT Systems.

And what they didn't do is engage security folks in this discussion. So I am actually assigned to the FBI Security Division. And we handle the issuance, storage, passage and verification of all clearances throughout the FBI.

So when this issue came to us from the last meeting we presented this to our Office of General Counsel who does have concerns about submitting the information into CVS because we are bound by the Intelligence Community Policy Guide, which mandates that the FBI continue to use and leverage Scattered Castles.

We've also compared that to the Executive Order. And though the DHS Directive goes further in implementation and use of CVS, the Executive Order itself basically states that upon request from the Department of the Secretary of Homeland Security we're required to provide the information about our state, local, county, tribal and private sector clearances to DHS.

So there is kind of a gap there from providing upon request and then dumping our information into CVS, which is now not only a technical issue for us because we don't integrate with that system because we do leverage Scattered Castles as required by the IC Policy Guide, which is mandated by the ODNI. So it's basically not an FBI policy. It's an Intelligence Community policy.

And thus we don't have integration with CVS. So that's the technical piece. We are continuing to work with our OGC to see if there is anything in the Policy Guide that bars us, one, from sharing this information and they have yet to provide a determination about that. So that's just it's under legal review right now.

But it's my understanding that the crux of this issue is that our state, local, tribal and private partners don't have the ability to check on their clearances.

But from an FBI perspective that is not the case. There is a procedure and our state, local, county, tribal and private sector partners that for whom we sponsor clearances do have a mechanism where they can check the status of their clearances. They can check the date of the issuance of the clearance. They can check whether the clearance is in scope or not.

And they can also check on the status of any SCI and how they would do that is by reaching out to the Chief Security Officer and the sponsoring FBI Office and requesting that information and it would be provided to those partners.

So I'm not sure if that is going to be sufficient for the Advisory Committee because if the problem is that our state, local, county, tribal and private partners don't have the ability to check on the status of their clearances, the FBI has addressed that that they can do like every FBI employee does, which is they go through their Chief Security Office and for those partners it's in the Field Office that sponsored their clearance. And they have relationships with those Field Offices because if they didn't they wouldn't have been sponsored for a clearance.

So I don't know if that addresses the Advisory Committee's concerns. If not, then we're still waiting for our Office of General Counsel after reviewing the Executive Order, SEAD 4 or SEAD 7, and the IC Policy Guide to give us a legal read on whether we're barred from sharing that information.

And that unfortunately we do not have that legal determination yet. We – several lawyers have looked at this and they have been in discussion about this so until we have that determination we're not at liberty to share the information as of yet.

But I can share the process with you and our folks that we sponsor clearances for should know that process.

In regards to the second question, which was posed to the FBI which was how many sponsored clearances for a state, local, county, tribal and private sector partnerships do we currently have on the books, right now the FBI is the sponsor for 892 clearances nationwide that fall into that category.

Greg Pannoni: Yes. I think we have – thank you Earl for that comprehensive overview. We may want to get a little bit more specificity on that process of reaching out to CSOs and the sponsoring entity of a person.

But DHS would like to say a few words on this.

Charlie Rogers: Yes I'd like – this is Charlie Rogers. I'd like to clarify a little bit about our responsibilities as the Executive Agent and the – under the Executive Order regarding clearances. Within the Executive Order it says that DHS is responsible for documenting and tracking the final status of security clearances for all SLTPS personnel in consultation with the Office of Personnel Management, DoD and ODNI.

And right after the Executive Order was signed we stood up a Working Group Committee with those players as well as the FBI. And it was agreed that CVS was going to be the mechanism.

So DHS does not request clearance documentation from agencies. DHS expects agencies to migrate clearance documentation into CVS, which was designated by that Working Group of which FBI was representative and had input into the configuration of how CVS would work.

DoD modified JPAS to enable JPAS to communicate directly with CVS. And OPM created a portal for state and local Fusion Centers to access and verify clearances to CVS.

So I think for clarities point, DHS does have responsibilities in this matter. But the decision was made early on that the mechanism was going to be CVS and that that is how DHS would receive its information and fulfill its responsibilities.

Earl Camp: Right. And I understand that and as I expressed early on, unfortunately initially representing the FBI on this Advisory Committee was our Office of the Chief – our Chief Information Officer.

And they're a technical group. They didn't understand the sensitivity of the information that they were dealing with.

And we now have our Security Division, Office of General Counsel, reviewing that to ensure that we – so we don't currently, the FBI does not – we only use Scattered Castles as was mentioned early on in the opening for the meeting. We do not leverage JPAS. We do not leverage CVS.

And that we want to ensure that our legal folks are okay with us even proposing that even though it's a technical solution, which I understand that. But from a legal perspective we want to make sure that we're not in violation of the Intelligence Community Policy Guide, the SEADs that we're required to operate under and our own policies, which require us in line with the IC Policy Guide to use and leverage Scattered Castles.

So until I get a legal determination from our folks because we are the originators of that information we just want to make sure there's not an issue.

I think from a technical perspective I think we can iron that out. You know I don't know what a flat file is. But just, you know, I've heard that if we can put our data into that configuration then we can provide it to CVS.

But our question is we just want to ensure by doing that, by leveraging CVS, which is not in any of our policies, our rules, our regulations, and since it sits out on a non-secured. It's an Internet access domain that we're not in somehow violating the policies and that we're required to operate under that come down not only from the SEADs but through the ODNI to us as an Intelligence Community partner.

And I don't think that legal review ever occurred before because like I said, the people from the FBI that were representing this Advisory Group were technical in nature. They weren't dealing – they weren't used to dealing with the Security Division and the legal ramifications and the policies and procedures that we have to operate by in the process of vetting people for clearances, holding and storing that clearance data and in what systems we leverage to hold, house and review that data. And that's the issue here.

So I don't want to make it sound like we're stonewalling. It's just that until our Security Division, Office of General Counsel folks who are very familiar with the Security Division rules that we operate under outside the technical stuff, until they give us the blessing we're hesitant to move forward.

I think the technical fix is something we can come to. I mean computer people can talk to computer people and we get that ironed out. We just want to make sure that we're not violating some other policy as laid out by either the ODNI or SEADs 4 or 7, which are primarily our bible. So that's really the issue here.

And I know we don't have a quick fix for this and I apologize. But since the last meeting we've had our Office of General Counsel looking at this.

Mark Bradley: Earl this is Mark Bradley, the Chair. I understand. You know again I compliment you on your briefly. And, you know, I understand what you're saying.

But again my fear is if something goes wrong, having a congressional hearing on this. And people wondering why we didn't get the clearances passed.

When can we expect your legal review to be complete? Do you have any idea about that?

Earl Camp: Well I guess my question and first, I want to start with the issue is getting the clearances passed. There's no issue there because the state, local, county and tribal folks can always contact their local FBI office and facilitate that. So that mechanism has always been in place. I want to make that clear.

But in regards to when can we get a legal read on whether we can put this data into CVS, I don't – I can't give you a timeframe because I'm at the behest of our OGC attorneys. So I'm not setting…

Mark Bradley: Right.

Earl Camp: …the time (unintelligible).

((Crosstalk))

Mark Bradley: Perhaps a letter from me to Director Wray might prompt this along.

Earl Camp: Yes absolutely. I don't think that would hurt anything.

Mark Bradley: All right, good. Let me ask before I get to our DCSA partners. I mean state and local, I mean how do you feel about this? I mean have you been able to access this FBI…

Marc Sachs: Right.

Mark Bradley: …information?

Marc Sachs: So Marc Sachs here from private sector. If the individual knows who their Field Office is, which they should, that shouldn't be a problem. I think what the issue that's come up is in a timely manner. If somebody gets a phone call we need you down here right now so we can brief you on something. If they're already in a Central Verification System that location they're going to can immediately determine yes, come on in, join the meeting versus having to find your FSO, having to hunt that person down, having them go through the formal process of passing clearances which often you need to do a week in advance. That's the typical way if you're doing a scheduled classified briefing at some point in the future. It's the timeliness issue particularly with cyber stuff is…

Mark Bradley: Yes.

Marc Sachs: …what's at stake there.

Mark Bradley: (Unintelligible) pretty quick. Earl did you hear that?

Earl Camp: Yes I did. And I got to be honest with you. I don't agree with that only because in an emergency situation whoever was sponsoring the meeting so say it's a non-FBI Meeting, if they contacted the local Field Office they could easily provide a list of all the SLTP partners that they anticipate having at the meeting on short notice. And the Field Office would have the capability to query Scattered Castles and provide them a response back fairly quickly.

Keeping in mind, we're not asking our state, local, county and tribal partners to do anything different than we ask of our own employees. You know if we had to verify their clearance because they had an emergency briefing at an IC partner facility we would leverage that same procedure.

So in essence that procedure does exist regardless of whether the local partners are aware of it or not. It does exist. And it does take into account emergency needs as that – such as that described.

But other than that I also agree with the gentleman who spoke that normally we would require, you know, our policy requires a 14 day notice to pass clearance. And that's for our own employees. So we're not treating our state, local, county and tribal partners any differently than we treat our own employees when they are required to pass their clearances to an IC partner agency so that they can visit a facility and/or receive information controlled by that agency.

Charlie Rogers: This is Charlie Rogers again. The – to go back to the original intent of CVS it was to enable federal agencies and state and local partners to verify the final status of clearances in a quick and effective manner.

And the Fusion Centers frequently they're now new members of this classified environment after post-9/11. They've got classified secured facilities. They have security clearances. They frequently host meetings of which multiple federal agencies participate and in which other state and local partners show up on short notice.

And CVS is a mechanism not to create an emergency but to prevent an emergency situation to enable these people to go into the database and to quickly verify yes or no the person has a secret clearance.

And the secret clearance was the key because Fusion Centers operate at the secret level. And so it's basically a means to facilitate classified interactions without precluding people from coming to meetings and without causing an emergency and without having to plan a meeting 14 days or 3 weeks in advance and have a rigid attendee list.

Earl Camp: And I understand exactly what you're saying. And there's a couple of issues there. One, state Fusion Centers sharing classified information are never sharing their own information, right. They're always sharing some information that came from a federal IC partner entity.

And then two, to go back to my original point, we're not asking our state, local, county, tribal folks to do anything different than we would ask of our own employees.

So again in that situation if there's an impromptu meeting there's still a mechanism. The Fusion Center could call their local FBI Office and every Fusion Center has a relationship, a very close relationship with their local FBI Office. And say hey, we're holding a meeting this afternoon. Here's our planned list of attendees. Can you provide us, you know, and all they would need is verification that they hold a clearance at a Tier 3 secret level.

So again I don't think. If the intent is to allow entities to access their clearance data so they can participate in these meetings, the FBI does have a process in place for that. And it covers every scenario that I've heard to date.

I understand the added issue of hey we just want to make this as easy as possible for our state, local, county, tribal partners and I don't disagree with that either.

But we have to be very careful about how we do that. The biggest risk that we undertake as an IC partner is that as I see partners we have control over the clearances and the data.

But when we sponsor a state, local, county, tribal or private partnership we don't necessarily have that control, right, because the people come to the meetings. They receive classified information. They leave the meetings. But they're not in a controlled government environment. In other words there's no recourse if those people decide to somehow spill or leak that information, right, there's no reporting requirements. There's no repercussion for that.

So that entails a greater risk especially for the FBI. And that in the Security Division is what we're trying to manage. We're trying to balance the obligation from the result of the 9/11 Report to share information with our state, county, local and tribal officials with the risk that we assume by sponsoring those clearances and sharing that classified information.

And that's where the lawyers come in, right. And they're helping us determine the management of that risk.

Patrick Hogan: Has nothing to do with it. Yes.

((Crosstalk))

Woman 1: (Unintelligible) separate issue.

Patrick Hogan: Yes.

Mark Bradley: They're separate issues.

Patrick Hogan: Yes.

Mark Bradley: You're talking about passing clearances versus (unintelligible)…

((Crosstalk))

Patrick Hogan: (Unintelligible).

Mark Bradley: …information.

Patrick Hogan: Right.

Mark Bradley: Speak into the mike for everybody.

Patrick Hogan: All right so.

Mark Bradley: Identify yourself.

Patrick Hogan: Patrick Hogan, DoD. That to me is two different issues. And I don't really want to get into the middle of DHS's equities on that.

But purely in terms of the original issue the passing of the clearances…

Earl Camp: Yes.

Patrick Hogan: …I'm going to confirm that we have plenty of our IC partners in both JPAS and CVS. There's nothing illegal about it. You're mandate to put things into Scattered Castles, doesn't prohibit you from putting it in another approved system.

I just I assure you we have far more than the 820 or so members of the IC identified in CVS today. So from a legality perspective again I don't want to infringe on FBI's OGC's equities.

But I think in terms of OGC across the government we have plenty of legal precedent from putting IC members' clearances or any of those state, local, tribal partners at the ICs adjudicating into other secure Personnel Security Systems of record to include…

Earl Camp: All right well look and I…

Patrick Hogan: …CVS, PAS.

Earl Camp: …completely agree with you. But that's just it. I got to get the okay from my OGC first. They're trying to balance out all the policies, the rules, regulations, the SEADs and the laws that we operate under. I'm not against it. I just want to make sure that my legal folks buy off on it and they have not done that as of yet.

From the start of the last meeting we brought this to them. We laid it out for them. They raised some points and some policies that we were unaware of. They said they would look at this issue. I will definitely follow-up with them.

Again I think once they get the clearance to do it, I think we can work the technical issue out. But I'm just not in a position to say yes, we're going to do this right now until I have that green light from our OGC. That's what I'm saying.

But I'm also saying that in the meantime, our state, local, county, tribal and private partner folks that we sponsor for a clearance are not without a mechanism to verify and pass their clearances is my point. I'm not trying to say we're being a stick in the mud here. I'm just saying in the meantime there is a mechanism. Until such time as the legal folks can conduct a review and give us the green light to effect the technical fix and put this information into CVS, if that makes any sense.

((Crosstalk))

Mark Bradley: (Unintelligible) anything else?

Patrick Hogan: No.

Mark Bradley: All right, Earl thanks a lot. We appreciate that. That added much more clarity than we've had before.

That said, you know, I would tell Director Wray to expect a letter from us.

Earl Camp: Absolutely.

Mark Bradley: See if we can move this thing along because again, I understand what you're saying about there's a mechanism and all that. It's still not what the Executive Order contemplates.

And so we've got to figure out how to get this sorted out because…

Earl Camp: No. And I think we will. And I apologize for having - I think honestly the FBI had the wrong folks at the table previously. We – I do work in our Security Division. And I'm actually responsible for clearance issuance, of all clearances in the FBI. That's my primary function of my section.

And this is an important issue. And we do want to address this. But I don't want to give, you know, I just came into this in December when I was first – it was first recommended that I participate in this meeting. So I've only – I know there's a long history here.

But the history for me only goes back to the first week of December. And as soon as this issue came up unfortunately I was not able to attend the first meeting because I had two days' notice and it conflicted. So we did – I did have one of my subordinates attend. We took this issue immediately to our OGC.

So unfortunately the Security Division OGC has only been looking at this from about the day after the last meeting. So I'm not making excuses here. But I'm just apologizing for past representation and laying out where I'm coming from. This is an important issue for us. We are looking into this.

But for me I've only been looking at this issue since December.

Mark Bradley: No, I appreciate that.

Greg Pannoni: Yes.

Mark Bradley: Yes.

Greg Pannoni: Yes. Okay, again and this is Greg Pannoni. Thanks Earl for the update.

I think that we need to – we would be, you know, for lack of a better word we would not be doing our due diligence if we didn't bring ODNI back into the picture here because obviously the order mentions ODNI.

And we know that there are some number of CIA people, excuse me, CIA sponsored SLTPS personnel. So I think we still need to get that addressed beyond just saying CIA doesn't track these people because actually step one is they ought to be tracked somewhere. You know two different issues here.

But step one is somebody ought to be tracking them in the federal government. And then step two is how do we coordinate with DHS by way of the order, who has responsibility for fully tracking all SLTPS personnel.

So with the Chair (unintelligible).

((Crosstalk))

Earl Camp: I agree. I agree 100% and of course that's what I was referring to with the risk that we're assuming here. Because even my own agency since I have become aware of this issue in December, have come to find I don't believe that we have appropriate controls on that tracking as well.

And we're putting those mechanisms in place. And again previously it was technical folks looking at this, not security professionals.

So I do hope at least you have the right representation from the FBI and that we can get to the bottom of this and meet everybody's needs and minimize risk as well so.

Woman 2: Greg and just to follow-up on what I learned from CIA and of course we'll engage with them again and get more information. But when the request went to them to try and give us an idea of how, excuse me, how many at that point they weren't able to track it. It doesn't mean that maybe they have another mechanism or they're going to do it.

So I'm not speaking for them. But I just know that they weren't able to pull out a number to tell us how many are cleared for those particular sponsors.

And as you know, CIA does all the NC50 agencies for TS/SCI and depending on the agency and what they pass and what they ask to be processed. I'm not sure how they're tracking it.

So if one agency submits 100 cases we don't know how many of those 100 are really specifically for state, local, tribal.

So I'll say we'll still engage with CIA and determine if there's another way to maybe pull out a number or see how they could do future tracking.

In regard to Scattered Castles, as you know, yes, TS/SCI should be put into it. All the intelligence agencies should load to it.

And also all agencies that have access to it determine who should have access to it. DNI does not determine who gets access specifically. So it's up to an agency to sponsor their own people or their own FSOs. And they track who they're giving access to, to the database.

And regarding the SEADs, I know Earl you mentioned the SEADs, yes, talk about policy of reporting clearances to government wide databases. It does not say specifically who reports where.

So we all know that we're going to eventually have maybe two databases, a high side and a low side sponsored by DoD.

But at this point there are three. And we just want to encourage that everybody, you know, share what they need to in all the proper databases.

So I will go back to CIA, see how we can engage them and find out more.

But also we still also have procedures. And I know all agencies have procedures for sponsoring clearances and passing clearances so.

Greg Pannoni: Okay that's – unless DHS, do you have anything further to say on that since the mantle is given to DHS before we track all SLTPS persons?

Charlie Rogers: Well just that we have about 6000 state and local security clearances. And the great majority of those are sponsored by our Intelligence and Analysis Directorate. And they're all migrated into CVS.

Mark Bradley: Well that's good to hear. All right, I think we've beaten this one to death.

Greg Pannoni: Yes.

Mark Bradley: At least for this (unintelligible).

((Crosstalk))

Greg Pannoni: Okay. Let's just hope that…

Mark Bradley: And that was our first down.

Greg Pannoni: …when July comes around for the next meeting we're not still discussing this one I'd hope.

Mark Bradley: Yes we (don't want) to do that.

Greg Pannoni: Okay thank you Mr. Chair. So the other item we had maybe not as contentious. I don't know. We'll see. We're not done with it.

But at the last meeting our State Department representative, Mr. Masciana, gave briefing and fundamentally the issue that he presented was is the Classification System working to hinder or to help in the cooperation with our SLTPS partners essentially to defend the nation's critical infrastructure and from cyber threats.

And so I'll turn to Leo in a moment here to discuss a little bit of that.

So we had a meeting. It was DHS participated, ISOO. And who else did we have? Did we have – well obviously State Department participated with Leo being there.

And this is fundamental. I'm going to again go back to the Executive Order. This committee, its purpose, discuss policy issues and dispute and facilitate resolution and then also and this is key on this very point recommend changes to policies and procedures that remove undo impediments to information sharing. So spot on with what Mr. Masciana was presenting.

So we held the Working Group Meeting. And we had a number of items we discussed as far as the issue and how to overcome the issue. I think and I failed to mention, I'm sorry. We had an SLTPS participant on that call meeting as well.

Fundamentally is the issue is I think and I agree, I think this came from our SLTPS person is to how to desensitize that cyber threat information and to get it to the right people in an expeditious manner because it's perishable and especially in this area of cyber threat, 24 to 48 hours. And I've heard this in various venues as well from others. If that information is actionable and you don't have it within that timeframe generally speaking you've missed out and whatever vulnerability and threat was presented if the bad actors wanted to do damage they probably have already done it.

So that's kind of overall without going into a great deal of background what we talked about. There were other things we talked about and I will give you a chance Leo to speak to it as well.

Moving forward what we also quickly identified was we need to bring some of the right agencies in on this discussion that weren't at our meeting. And some of those agencies are U.S. Cyber Command, NSA, the Cybersecurity and Infrastructure Security Agency under DHS, FBI, National Council of Information Sharing and Analysis Center. So the places where this sort of data would come together and flow in and flow out so that's kind of in a nutshell what took place.

But Leo if you want to add any finer points to that.

Leo Masciana: Yes. Leo Masciana, STATE. I'd like to give an update on, what essentially a formal tasking to establish or form a Working Group. I think you've titled it Classification and Sharing Cyber Threat Working Group. And to get the right people at the table.

So, among those agencies which actually includes (DNI) representatives, we've been seeking the right subject matter experts to participate in a Working Group level meeting at Cyber Threat Task Group sometime in February. And the status I have so far, is that I am still in the process of getting someone from Cyber Command and NSA. But there have been feelers put out by colleagues, even DNI colleagues to the National Security Agency. I'm expecting a name soon.

I do have a member from the FBI's Cyber Engagement and Intelligence Division under this Cyber Division of the FBI, who is a solid volunteer. And I understand Marc Sachs has some people specifically in mind for this, sort of, private sector side of it and that DHS will be coming in soon with a few names.

These are important agencies in terms of expertise, in that what Greg said, that they tend to be the Nexus for where they the information comes in and gets processed. So, the idea is to have their members - in the (DNI), let me mention too, that I spoke to the ADNI for Cyber Engagement - no excuse me, Federal, State, Local, Tribal Information Sharing - Federal Partnership Engagement. (Steve Mabius) who is very interested in this and he has some names from the DNI, including NIM-Cyber as a possibility.

And I have one - a former colleague from the CIA who is looking for a CIA representative with the kind of background we're looking for. So, that's the update. The overview is that, this body ISOO, has the authority and expertise to review classification.

And so, it's a good segue to get started. There's considerably more that needs to be done to expedite cyber threat sharing then just classification. But it's a good place to start to ensure that the guidance is effective. And that's at multiple levels. It's at the Executive Order itself whether reform is needed in terms of a secrecy order within agencies. Whether their guidance is adequate to accomplish this and whether there is a need for guidance across the government, maybe even a joint classification guidance.

There's also implementation and procedural issues that maybe could be improved. So, with that - I think that the members of this PAC - this committee, should be encouraged to also participate directly, both in attending the working level and in providing names in these areas that we've identified that we're still seeking subject matter experts. Can't have enough suggested volunteers and then we'll have a basis for which this body can issue invitations for the upcoming working group.

Greg Pannoni: Thank you Leo. If you had to pinpoint one thing, would it be that the information is TS/SCI because of sources and methods, (and if that we strip down), we could push this down to a lower classification level?

Leo Masciana: The are many issues over classification or dealing with highly classified information procedurally is certainly front and center with the initial discussion. I had, in fact, submitted some bullet points on a possible set of agenda topics. I think it might be useful if we circulate that and get input prior to another working group meeting as to what to focus our initial time on and to invite additional suggestions for topics.

Greg Pannoni: Some of the things you suggest (I'm not saying they don't need to be done long-term, like revising the Executive Order. What I'm more interested in, again, is like the discussion we just had. I mean (in) short-term wins too, being able to push this stuff out quickly.

Leo Masciana: I'm very much looking forward to how these, sort of, fusion centers that are working the sharing as it is, can inform us as to their right to release their declassification or downgrading. And what they're actually doing in practice to expedite sharing. I think also, their opinion on whether there should be possibly a reform that sets up a whole new approach such as a modified handling procedure for this kind of information within the secrecy order.

But those are longer term, aren't they? To reform the Executive Order would take at least a year, maybe several years. But procedures within these organizations under existing authority could be done relatively quickly to better inform the operational elements of those organizations on how to better comply with the intent of the intelligence format.

Greg Pannoni: Marc Sachs from the private sector.

Marc Sachs: One of the pieces that we have to not lose sight of is that this is not just a drill to change the way we declassify information for the sake of declassification. The end state is how do we get timely information to the people who need it. Whether they may be government partners, private sector partners, it doesn't matter. And if that timeliness is blocked because of classification rules, then we need to address that classification. So, and that's part of what this party needs to worry about.

There may be other ways we can get information to those who need it. In the meantime, while we're working on how to do a more rapid declassification. So, that may be a different advisory committee that could work on that. But let me cite a timely example.

About two or three weeks ago, following the Iranian incident, DHS hosted a really good - I think they had 6-thousand some-odd people dial into it. Chris Krebs ran it, an hour-long session on here's what we know. Here's what - you know, sharing as best they could in a very open format. Very detailed, but Chris was limited in what he could talk about at a technical level because of it still being classified.

Two days later, the private sector had an unrelated, but very similar gathering. It included some of the more leading cybersecurity big companies that people are familiar with. And they gave a very technical, here's what we know, here's what we're seeing. But it's the private sector's view. I'll guarantee you that the private sector's view and the government's view are almost identical.

But the government can't talk about theirs because of classified reasons. The private sector can. It's the same technical data, but the private sector can talk about it because it's not encumbered by restrictions on classification.

A good role of government which was suggested after this, is perhaps the government while they can't right now talk about it because of classification rules, they can at least assist the private sector in prioritizing what the private sector already knows. Attend the meeting. Say worry about this, don't worry about this, worry about that. We're not breaking any security declassification rules yet. Where at least, it may be an interim step here in terms of getting towards that - that assistance that the government can provide.

So, this was - that idea was forwarded by a member of the banking community. Not that we're doing it yet, but it could be a way we can at least, get the information down faster. But we do agree that the long-term approach does need to - which this committee would be appropriate for - is to make recommendations on how to declassify the stuff in a more timely manner. And if it sources and methods, some way to separate that from the just pure technical knowledge. And how do we go about doing that? And who's - under who's authority, and what mechanisms can be done to do that?

Leo Masciana: Leo, again. One thought that's occurred off an on, is that ISOO has the authority to issue interim guidance across the government. And if we were to focus on emergency release section of the Executive Order and further clarify clarified it to a guidance for this particular category of information as a threat, it might be that we could get to a resolution more swiftly on taking what is now a vague emergency release procedures and defining cyber threat as a subset of that.

Including such creative possibilities as a modified handling approach, in addition to the established ones of right to release, declassification, downgrading, and so forth.

Marc Sachs: Marc Sachs. One more point I failed to make. At the same time all this was happening, the NSA, as you probably may remember - this was about two weeks ago, a little bit over two weeks ago - announced very quickly the finding of a vulnerability inside of Windows and worked with Microsoft and got those patches up. That shows you it can be done. So, when this information is picked up in a very sensitive world, and you recognize the impact it has, not only to U.S. infrastructure, but globally, you can fast-track it. And you can get the technical information out and divorce it from how they learned about it. What was the source of (the nebular)?

The fear (is the technical) and so it's needed right now. It just shows it can be done. And I realize NSA really, probably spent a lot of time working through the legal folks to get this done. But it was done. But that was a very costly effort they went through to get that done and it shouldn't be that costly. It ought to be more routine to be able to do that.

So, it did give you an example of how it can work. But it needs to be more institutional versus a (1R).

Greg Pannoni: (Unintelligible) (routine ideas of putting out a notice), we'd have to have obviously coordinated with our friends, but work into that.

Leo Masciana: And, I'll just say this - the modified (unintelligible) rules, for those who don't know, are really borrowed from the Executive Order for foreign government and information sharing and exchanges. So, my thinking is why can't that be also used in this context with ISOO authority to do so. That's a question I think the Working Group could take up.

Greg Pannoni: We don't have a date for that (unintelligible).

Leo Masciana: I think we're still waiting for - to firm up our participation list, which will probably take at least another week or two. We can shoot for, I think, the third or fourth week in February.

Greg Pannoni: All right. That's good. That's constructive. Thank you, Leo.

Leo Masciana: And again, my appeal to the members of this body to also indicate their interest.

Greg Pannoni: Anybody have any comments on that?

Tiffany Kleemann: Tiffany Kleemann, private sector. I couldn't agree more, but I also feel like, wow, these are the same conversations we had when I was back at the White House in 2001 to 2003, as we were standing (unintelligible) as we were doing a number of things to try to help drive the (Unintelligible) Process.

We made some progress obviously, including the establishment of organizations like this and others to be able to allow for other folks in the private sector, state, local, tribal territories, to have a seat at the table. But it's slightly disappointing to me, I will just say, that we haven't made further progress.

But I also understand the challenges and the equities that go into this. And I really do like the idea Marc has provided. And in my past jobs, right, one of the places I worked was Eye Sight Partners, now FireEye Cyberthreat Intelligence Provider to both the government and the private sector.

And it was constant that I would be pulled into meetings, various meetings across multiple agencies to actually (unintelligible) government entities on various threats.

And so, the other thing I just wanted add is, this isn't just about the government contributing information and intelligence to, you know, folks in state, local, tribal, private sector entities. It's about sharing information both ways. Because as Marcus indicated, there are many private sector entities that have just as much to contribute. And in many cases, a lot of information the government can't today gain access to because of its limitations and title authorities.

So, I think the other thing to think about is, you know, how can, you know, both sides work more collaboratively together to provide more of a comprehensive picture (at large), as well.

Greg Pannoni: Yes, well I was going to save this until the open forum, but talking to Greg last night, one of the things I'd like to do is to have a classified section of this meeting. And that means going different door (unintelligible) and actually doing exactly that, trying to share some information. It would be interesting Leo, to have somebody from the (ATTF) come in and explain how their - (a few of their centers) - how they're doing. What they're supposed to be doing?

And just to kind of have a more - how can I put this? A franker discussion about some of these issues.

And we have a (unintelligible) up on the fifth floor. We'll take the clearances and we'll go in and we'll have briefings - actual briefings on threats. And issues that you might not feel comfortable about talking about in an open forum. But we should, I think, start making this what it's supposed to be, sharing information. So, stay tuned for that. That's all I have unless there're any other questions? I think we're going to turn to you talk about DHS.

Charlie Rogers: Okay. This is Charlie Rogers. What I'm going to say is kind of a repeat of what I've said before. But I was asked to kind of give an overview of the Executive Order and a little bit about DHS activities, because we have a number of new members. So, this is more of a refresher and a thumbnail sketch.

But just to go over the E.O. You know, the purpose of the E.O. was to standardize the way in which classified information is safeguarded to make it consistent between federal agencies and the state and locals. And to ensure that the safeguarding is done in concurrence with other Executive Orders.

So, the Executive Order doesn't really create whole new procedures. It connects those procedures together into a single document. It also directed the creation of an Implementing Directive. So, that was accomplished, which amplified the content of the Executive Order in more granular detail. It talked about how federal agencies are responsible for sponsoring clearances.

And that the basic operating level is secret. First think local tribal, which does not mean that you can't have a higher clearance, but that it's an exceptional action. It's a case-by-case decision. It formalized the governors having clearances without a background investigation. And I think later to that will be an (I-Issue) Guidance that governors can be read into special access - or TSCI - TS and CI, also without any special investigation.

It affirms in the Executive Order, where other Executive Orders have done this, that clearances and room certifications are reciprocally accepted between agencies. It called out that states could have physical custody of classified information at the secret level. It limited that anything above secret, you know, TS or TS-SCI would be managed by federal agencies.

It doesn't mean it couldn't be collocated with the states, but that the management of that storage would be at TS-SCI. It reaffirmed the National Industrial Security Programs, cognizance over contractors. It established this committee, the Policy Advisory Committee. And it did call for the establishment of a database or for a mechanism to verify clearances and that was completed in 2014. So, it's been around for a while. And OPM stood up at that time and volunteered to do CVS.

So, that's the broad overview of the Executive Order. So, then the thumbnail part I'll talk about is that DHS has a lot of activities that I'm not necessarily a subject matter expert in granular details. But there's a lot of activities in which classified information is involved and so we have the Cyber and Infrastructure Security Agency - the newly named previously NPPD. And it has 16 critical infrastructures, of which there are multiple committees and multiple interactions that CISA has with those infrastructures and they involve security clearances and the sharing of, not only cyber, but other threat information.

And within CISA, you know, there's the 16-critical infrastructures, but there's also a new subsector. The Election Infrastructure Subsector and we're clearing - DHS is clearing election officials through all 50 states - on behalf of CISA, we're doing that to enable the sharing and interacting of threat information.

Within CISA, they also have the NCCIC, which is - I'm reading some of this - it's the National Cybersecurity and Communications Integration Center. And that's a 24/7 Incident Response and Management Center and we are clearing a fair number of people at the TS/SCI level. There are both state and local, and private sector people who are detailed on a rotational basis to the NCCIC. And so, we are involved in that.

CISA also has protective security advisors, which are subject matter experts who go out and do threat assessments, for the infrastructure in the United States. They work closely with fusion centers. They also sponsor select private sector personnel for security clearances as they deemed necessary, whether they're managers of dams or other electrical grids. So, we're involved in providing security clearances on behalf of the other Protective Security Advisors.

And then the intelligence and analysis directorate has a responsibility for classified information sharing in DHS. And they are the primary interactors with the state fusion centers, of which there are like 82 right now. And all the fusion centers have classified connectivity through our Homeland Security Data Network for which DHS Office of Security has certified 65 rooms that are managed by the states. There are another 15 rooms and fusion centers that the FBI manages, but which allow the states to interact with in which HSDN is deployed. And there are a couple of DoD facilities that are collocated with the fusion centers.

So, within the fusion centers, we have required and identified what they call security liaisons, which are state and local employees who are trained by us and I&A to manage the classified holdings within their facilities. I&A, in July of this year, sponsored a Workshop in Ohio in which 70 federal and state and local people came to receive training. The FBI participated, DHS Office of Security and Intelligence and Analysis and some of the state organizations participated as a training event.

So, that gives, kind of, a broad overview of some of DHS's classified interactions. And there are a lot more. I worked in the Office of Security. I don't necessarily have my finger on every operational activity in DHS.

Within the Office of Security, we do compliance reviews of fusion centers. So, last year we did 14, in which we go out and we utilize a checklist based on federal and DHS policy regarding INFOSEC and physical security and personnel security, OPSEC, and we evaluate the fusion centers. We did 14 last year. We expect to do 16 of these audits this year. When we do the audits, we also provide training and listen and interact with them.

And then, I was going to finally just give you some basic metrics. These are average metrics for what we've done. We currently have 21-hundred cleared private sector personnel that DHS has cleared. We have six-thousand-two hundred state and local personal who were cleared. It's a total of about eight-thousand-three hundred people that we've cleared in total. And they are all NCVS, I will say that.

And then of that number, there are 475, approximately, that have TSSCI. Now they have that for a variety of reasons. Either they sit in with a particular Working Group, or they are detailed within DHS. Or, maybe they are working with a JTTF, or they have some other role or responsibility that requires it. So, those are the exceptions to the secret level established by the Executive Order.

So, that's my thumbnail sketch about DHS and the Executive Order. Are there any questions?

Greg Pannoni: Hey Charlie, this is Greg. Do you have any (I'm going to ask you) - do you have an approximate number of how many state, local, tribal, (non NIST private sector) facilities have actual physical custody, authorization at the secret level?

Charlie Rogers: (Non) NIST?

Man: That's right.

Greg Pannoni: Under this program. Because that capability does exist, right? It's secret level?

Charlie Rogers: Well - well not storage. What do you mean?

Greg Pannoni: That's what I'm asking. Storage.

Charlie Rogers: No, the only storage we've approved is for state and local.

Greg Pannoni: That's what I'm saying. And approximately…

Charlie Rogers: Oh, oh.

(Crosstalk))

Greg Pannoni: It's the 65…

Charlie Rogers: Well the 82 fusion - there's 82 fusion centers.

Greg Pannoni: Okay.

Charlie Rogers: And there are probably - I mean I'd have to - I'd have to do a data run. We also have a number of states that - Maryland is one and Florida is another - that have requested and been sponsored by I&A to have minimal storage. Where they may have (STE) at some regional state police facilities. Because they have (STE), we require that they have a safe because there's not much robust storage.

Greg Pannoni: So, I'm asking the question because just trying to make the link between an earlier discussion on sharing of cyber threat information. If there's a way to express it at the secret level, since we - you know, this program is largely, as we know, is centered around secret, not SCI top secret, as far as access by state and locals. Except for the exceptional basis to access above that.

But you still say it's the issue of the actual storage requirements when accessing the information. So, if it were able to be operated on a secret level where more of these places could essentially operate the access secret information via systems - whatever it is, HSDN or whatever. So, that's where I was going. Why I was asking that question.

Charlie Rogers: Yes, so yes. HSDN is an (AD SUM) locations. Really, even at the secret level, there's a limit to what you can share because we can't clear every executive in every company in every company in the United States. So, I think with the cyber, there is - being able to get actionable unclassified products is going to be helpful too.

Greg Pannoni: Actually, it's easier.

Charlie Rogers: Yes.

Woman: (Unintelligible).

Marc Sachs And when you get a declass (unintelligible), which is - you still have controlled access to it. You still have to be vetted into it. But now you can get at it very quickly.

Charlie Rogers: Yes and (isn't it) a bigger platform. And I - you know, we have gotten I&A to come and talk about how - the fusion centers do interact in a wide variety of ways and they vary within their own states, with information sharing. But still, the classified footprint is largely focused on the fusion center itself.

Rich McComb: Hi, this is Rich McComb, the Chief Security Officer. So, you know, the component heads in DHS, that's the Administrators, the Directors, the Undersecretaries, do have authority for one-time relations. Obviously, they've got to go (through that information on their own net). And they do, do that on a regular basis. So, I think part of this conversation is actually getting the (system folks) here to explain, kind of, what they do. They do, do that on a regular basis through the ISACS - the Information Sharing Analysis Councils, through other venues.

Obviously the (unintelligible) that Marc talked about earlier, I assume that obviously was unclassified with 6-thousand people. So, obviously that's a logistics issue there with regard to how you get that out to that large number of people in that short period of time.

But they do have that authority. They do exercise that authority, because we get those notifications, so it does happen. But I do agree that if back in the day, there could be, I'll say, a more blanket emergency release type policy that might allow for something like that to happen on a quicker basis, that could probably be beneficial to the overall process.

Mark Bradley: Any other questions to VHS? Controlled Unclassified Information Program briefing from Devin Casey (unintelligible).

Devin Casey: Good morning, I'm Devin Casey from the CUI Team. Just an update on the Controlled Unclassified Information Program which is not related to the Classified Program, but may help facilitate and standardize the way we protect and share unclassified information. So, it's an information security reform that the Executive Branch is currently going through. It's built off of standardizing the protections for information their already required to protect, (unintelligible) into a law regulation or government wide policy.

As their implementing, those agencies are in the final stages of their policy creation phase, which is really, kind of, when the first domino falls for implementation on that agency. Most agencies have reported to us that policies will be out this fiscal year. (Then most of the) (unintelligible) within the end of the calendar year.

So, you'll see some pretty quick implementation over the next year or two of CUI Programs at agencies. That'll mean that they'll become a bit more deliberate with what they mark and protect as CUI, but they will also be pushing, perhaps, more onerous requirements to protect unclassified information, especially in areas where they weren't pushing requirements.

We have a lot of current engagement with the private sector. We are working on a FAR clause - FAR case that will address Controlled Unclassified Information through contracts. We do have a CUI notice that discusses the sharing of CUI through agreements. As far as representatives from states here, we have met with multiple Chief Data Officers from different states - Virginia, Florida, Texas, New Hampshire. A few Councils have had most of the states represented, as well as some private meetings with Chief Data Officers, because a lot of agreements that agencies have will be modified to adjust to these new standards. Things like the NIST 800-171, which is a cyber security standard for nonfederal information systems. And other things will be pushed.

So, we're engaging on all those. We do have a stakeholder meeting, which is an invite to everyone here. If you join our CUI blog, which you can find by googling CUI blog, you'll be invited to a quarterly stakeholder meeting that we do. And that's for anyone who has a stake in the CUI Program. State, local, tribal, private sector are all encouraged to attend.

We do have a lot of private sector. We do have some state (CDOs). We get a lot of academia involved, as well. We just give an update, much - very similar to this, but about an hour to two hours long of what's happening in the CUI Program? We do a little bit of a deep dive into what's going on about that. When our FAR comes out for public comment, we'll have an exclusive meeting to discuss the content of that.

So, there's a lot of good time there. It's also about 50% question and answer period. So, we do take question in live. Or you can send them to us beforehand and we will answer them. We will have a chance to have a dialogue then. At the Webex it's online. So, everybody can attend. It's pretty easy to call into or sign into from a computer. And it's a great way to stay up-to-date on the CUI Program.

As far as what our office is, kind of, focusing on as agencies are implementing for an oversight office, so our task now is currently helping agencies implement the programs the best they can. With a specific focus on ensuring standardization through these agreements to industry, as well as to other nonfederal entities, working with DoD especially currently on their plans for how they're going to actually go through the process of certifying people to work with their unclassified but sensitive information.

But I'll take - a couple questions, I think I have a few minutes left. If not, please join the stakeholder meetings. Their a great way to get involved.

Greg Pannoni: I just had one point because it's such a large scope and we're working closely - relatively closely - with DoD. The method that they're moving forward with in terms of certifying all of their contractors that they're having access to controlled unclassified information is the Cybersecurity Maturity Model, CMMC, you may have heard about that.

They're moving relatively quickly, especially for the government, hoping to have a certification body or more than one body, who would then certify entities to would go out and certify, the however, hundred or more thousand of DOD contractors that are accessing CUI. So, we view it as a positive and maybe a model that the rest of the government will adopt.

Devin Casey: And hopefully reduces confusion about the standard for protecting sensitive information outside of the federal government and it deconflicts (review) system reciprocity when you've actually certified systems to handle this. And hopefully that increase in trust to protect this information, provide an avenue for things like declassification of certain things that can be shared in a wider circle, because you can see a little bit more trust in the more real walls around that newer, larger group of CUI. Thank you.

Mark Bradley: Thanks Devin.

Devin Casey: I have to run back to another meeting.

Mark Bradley: Yes, thanks Devin. I appreciate it. Sorry. Deadlines, right? So, we're going to move into our general open forum discussion. And what we're going to do is have the new members tell us a little bit about themselves. But let me give a preamble to that.

I think once a year - at least once a year - I'm asked to justify why this committee should continue? There's a move afoot - there has been for some time, to reduce the number of FACA Committees in government. We always push back saying that this one is absolutely critical. Because it's the only forum I know that's like this. That allows the government and SLTPS partners to come together in a forum such as this.

Where we try to actually not be a debating society, but actually solve problems. And so, that said, the committee is no better than who sits on it. It's no better than the interest people take in it. It's no better than the interest or the issues that are brought to the committee.

And so, I implore everyone who sits on this committee to take this committee as a real opportunity to be of service to - not only to our country - but also to your own areas. I mean, we can try to do things here - again, you can see some of the issues we confront. They are not easy. They require a lot of shoulder at the wheel. But I believe with the right people in the room, and the right sensibilities and the right civility, we can actually get something done.

So, that's the whole point of this FACA. As I said earlier, what I'd like to do is just figure out a way - and again, we're FACA, which means we have public responsibilities - how to work in more of a classified element to this. I don't know legally what that means. I'm a lawyer, but I'm no FACA expert, so we'll consult with our own people. It may be an informal meeting in the (unintelligible) that, I don't know.

Whatever it is, I want this committee to be real. I want it to actually do something. And I encourage you new members, particularly take an interest in this. We are delighted to have fresh blood. It's needed in this area. And particularly such experts as yourself.

So, anyway, without further ado, Eric I'm going to start with you. Would you tell us a little bit about your background and who you are?

Eric Tysarczyk: Sure. Thanks Marc, I appreciate it and thanks everybody for having me. As Marc said, my name's Eric Tysarczyk. I'm currently the Director of Preparedness for New Jersey's Office of Homeland Security and Preparedness, specific day-to-day stuff. I oversee all of the state's infrastructure security work, our training and exercise and our risk management efforts.

Our organization - my organization also oversees the state and local clearance process throughout the state. So, we are liaising with both DHS and our FBI field office. So, that initial discussion was actually very helpful to me. So, I appreciate that.

This is my second governor in New Jersey. I've worked for two governors in Pennsylvania, as counsel, so I'm a recovering attorney as well. In a previous life, I was on the White House Homeland Security Council as Director for National Preparedness, as well as at DHS Headquarters in some of the early days.

I spent some time in the private sector doing cybersecurity work back in the '90s and so a career path that has handled and dealt with information sharing and the importance of it for some time, which motivated me to come to this body and apply to try to be a part of some of those solutions you mentioned Marc.

So, I appreciate to be a part of it and I look forward to adding some value to it.

Mark Bradley: Glad to have you and thank you for your willingness to serve. Tiffany?

Tiffany Kleemann: Hi, Tiffany Kleemann. As I mentioned, most recently CEO of Distil Networks, a Bot Mitigation, Cybersecurity Company. Prior to that was at FireEye for a couple of years through another acquisition of a company Eye Sight Partners a cyberthreat intelligence firm. Prior to that I was at Symantec for 10 years. running government programs and also leading the policy shop for the company.

And got there by way of a White House (stint). I actually served with Marc way back when. And I'm a former Coast Guard Officer as well. Thank you.

Mark Bradley: Meghann?

Meghann Teubner: Meghann Teubner. I'm the Director of Counter Terrorism Intelligence Analysis with the New York City Police Department. I'm really excited to be here. I think we're very lucky in New York that we don't face some of the challenges that some of our other local partners face, as far as access to spaces to (read) classified information. In fact, we have the ability to do that right in our headquarters building, which is very convenient for us.

But our, kind of focus, in our analytic shop is on information sharing for awareness and prevention of terrorism. Not only in New York, but in the surrounding areas and across the U.S. because we kind of see our CT mission as being the CT mission of all of our partners.

So, we do a lot of work with our private sector on terrorism (planned) tactics, indicators of mobilization to violence. We also do this now in the cyber realm and we have a lot of partnerships within New York City to make sure that we're kind of sharing all new cyber attack factors that we are getting awareness on. So, it's really important to us to make sure that information is shared in a timely manner, because from our perspective it keeps people safe on the streets of New York City, or globally really.

So, this is - I have been with NYPD for four years. Before that I was 10 years at the National Counterterrorism Center under the (DNI). So, I am looking forward to kind of learning. This is a new environment for me as far as the technical side of sharing clearances, et cetera. So, I'm looking to kind of figure out how I can plug in and represent the NYPD and other local organizations as far as, like, how that impacts our day-to-day life. So, I'm very excited to be on board. Thank you.

Mark Bradley: Well I'm delighted to have you. I remember Mr. Cohen when he went up to - form the CIA. So, anyway, it would be perhaps helpful for you all to share best practices with us and some of the lessons learned. I mean (you all basically become) your own CIA for lack of a better way to describe.

Meghann Teubner: Yes, (we took part in that).

Mark Bradley: No, I really do. Anyway, we're delighted to have you.

Meghann Teubner: Thank you very much.

Mark Bradley: Is (Mary Schechter) on the phone? No. It's a new member, okay. It's important to attend, so.

Greg Pannoni: She's the Director of Division of Community and Maternal Child Health Nassau County Department of Health New York.

Mark Bradley: Yes, okay. Well, indeed. We hope, at some point, we'll track her down and have her tell us who she is. Okay, with that, let's turn it into open - open forum - open mic time. Anybody have anything they want to discuss, or bring up, or say? Or anything?

Meghann Teubner: I'd like to ask a really quick question and it's a technical question and one that we've been throwing around in our space and it might make us sound kind of greedy, since we already have access at our headquarters building. I'd be curious to learn more about the process of actually creating access - how you go about getting access to an HSDN System and the facility that our unit is based is not at our headquarters.

We're in a HIDTAS - a High Intensity Drug Trafficking Association Space and below us is a DEA Strike Force Space and they have an area in which they can access classified information, one floor below us. I don't know technically what it entails to create a space from one that already exists. But I think that would be - it would be interesting or, I think, we would be interested to learn how you - how we can kind of expand that access. And again, I recognize that that may sound greedy, because we already have access at our headquarters, but that's something that has kind of come up in our discussion as far as getting access to HSDN Systems in different spaces. But I don't know if that's an easy answer or a long, very complicated one. And it sounds like it may be a more long complicated one, so.

Charlie Rogers: Well (Unintelligible) we would have you work with you I&A partner and then they would evaluate it and there are some folks here, but they evaluate the requirement. And once the decision is made, then it goes from - the construction and the physical part goes from there.

But the first step is to be sponsored, have someone validate the requirement and endorse the requirement. So…

((Crosstalk))

Mark Bradley: Are there contacts either that they know about? Or that DHS could share? Or have they already?

((Crosstalk))

Meghann Teubner: We work very closely with I&A our - they manage our (unintelligible) secure space at police headquarters, so.

Marc Sachs: This is Marc Sachs. But that raises a good question. If you're asking and you're already working with I&A, how many other people don't know that's the process? And is there some way to kind of make that more widely known? So, the question doesn't - because there may be other police departments and sheriff's departments that just don't know…

Charlie Rogers: Right and to be honest, I mean, the fusion centers aren't really designed to centralize the classified footprint. So, we - you know, there's a limit to, you know, every police department's not going to get HSDN in. But hopefully they're close enough to fusion centers. But those are decisions that we in the security world don't make. It's the operational side that is involved in the informational sharing. They decide where the Nexus is between the federal mission and the state and local mission and then, once they make that decision, we're empowered to help build the environment that works.

Mark Bradley: Anyone else?

Leo Masciana: The point that you raised about facilitating cost finding information within this body. So, I'd like to recommend that you (need) to list those classified mailing addresses that we already have and then we can start some - some exchange work that way.

Mark Bradley: Okay. Yes, That's good.

Marc Sachs: Marc\k, having worked with several other FACA groups, classified's not a problem. You can do that. You can absolutely do it.

((Crosstalk))

Mark Bradley: No, we can. We've been raising hell downtown. Right. Anything else? Again, this has been a good and fruitful meeting giving ideas to make these things real. Pray God, when July comes - I'm not talking about databases and security clearances.

((Crosstalk))

(Earl Camp): (I'm just closing out for the FBI. So, I have been on the) meeting. I've reached out to my (OGC). We're going to have an answer on this by the next meeting.

Man: (Unintelligible).

Mark Bradley: Oh, I'm sorry Bob, yes good. Yes, good. Thank you, Bob. Sure.

Man: There's somebody on the phone that wants to ask a question.

Mark Bradley: Yes, please. Who's got a question on the phone?

(Earl Camp): This is (Earl Camp) with the FBI. I just wanted to say, as we were chatting, I tried to reach out to my OGC rep here and we're going to try to get an answer on that for the next meeting. And I'm going to have my technical folks go ahead and work on the technical solution, so if we get the green light, we can just basically affect everything. And I'm thinking, we could probably do a, like a quarterly flat (unintelligible) passage as long as we get the green light. That's kind of my initial thoughts.

But I will have some clarity for the next meeting.

Mark Bradley: Okay, let's - (Earl) you're a great man.

(Earl Camp): I - I'm just trying to do the right thing for everybody. There's nothing great about it. We just got to get this done.

Mark Bradley: I know you're a patriot and I appreciate that. All right. Going once, going twice. I think (unintelligible). Thank you.

END