State, Local, Tribal, and Private Sector Policy Advisory Committee Meeting, July 26, 2017

M:

Everyone please take your seats.

Bradley:

Pete, let's go.

M:

Everybody present? Everybody in here somewhere?

Pannoni:

They should. We have some on the phone, too. You're right, I guess it's all connected to the microphone.

Bradley:

OK, good morning, everyone. We're going to start. I was telling somebody a while ago, these rooms are kind of, like, flying out of O'Hare Airport. We have a short runway here, and we lose these rooms, almost promptly. So we need to move on. OK, let me just start. I am Mark Bradley, the director of ISOO, and also the chair. So one ground rule before we start; these

meetings are being recorded. So when you speak, it is very important that you identify yourselves, because what we're doing is, we're preparing a transcript of this. So it is almost impossible for us to reconstruct some of this if you don't identify yourselves. So if I interrupt you, it's not because I'm rude. It's because I'm reminding you again that this thing is being transcribed, and that we're doing it for your benefit, because obviously we post these so you can read them too, and say, "OK, that's what Tip said," or, "This is what Carl said," or, "John said," or "Ben," or somebody. OK.

Without further ado, this is the second SLTPS-slash-PAC meeting of 2017, and the 13th overall. This is a public meeting, subject to the Federal Advisory Committee Act, the FACA. The minutes of the SLTPS-PAC meetings are available to the public -- again, another reason why we want to make the transcript as clear as we can.

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, so when you want to speak, just pull it a little closer to you, all right? A (inaudible) microphone is located at the left side of the room for audience members to

use. That's over there. So any of you all sitting around the wall, if you want to speak, please come up to the mic.

Anyone who is making a presentation but not sitting at the table can use the podium to give your briefing. So the podium is down at the end of the table, right?

Pannoni:

Over here.

Bradley:

Right behind me. Please identify yourselves when speaking, again, so we have an accurate recording of your comments. It's particular important because many of our members are participating by teleconference.

Membership changes, first order. I'm very pleased to announce that there have been no changes in membership to the State, Local, Tribal and Private Sector members. We've had stability, which is always nice for an organization such as this. On the federal side, though, there have been a number of changes. Number one, Marissa Bailey, director, Division of Security Operations, Office of Nuclear Security and Incident Response, is

a new member from the Nuclear Regulatory Commission, replacing Mike Layton.

Keith Szakal, acting director, Security, Office of Security, is acting as a member for the Department of Transportation. I noted at the last meeting the retirement of Lou Widawski. So where's Keith? Is he here? Or on the phone? Anyway, welcome, Keith, wherever you are. Keith indicated he would be participating by teleconference, so that's why he's not physically sitting here at the table.

Joan Harris, who was the DOT alternate, retired. There is currently no alternate for the DOT. So we have a vacancy there. More retirements -- Joe Lambert and Harry Cooper of CIA have both retired. So it's quite a loss, I think, for us. But be that as it is, we go on. Nancy Morgan, director, Information Management Services Group, is a new CIA member. Welcome, Nancy.

The CIA alternate position is vacant. I assume you --

Morgan:

We're working on that.

Bradley:

You're working on that, right. That's my favorite answer.

Morgan:

Retirements.

Bradley:

Yeah. No, indeed. We just learned that Mark Pekrul is no longer with the Department of Energy, and there's currently no alternate for him. So anyway, the federal side's got to do a bit of work. Nancy said we're working on it.

All right. Before I give you all the opportunities to go around the table and around the phone to introduce yourselves, I'd like to introduce several individuals who have joined us here today. They are members of the state, local Homeland Security and Law Enforcement Advisory Board, which is hosted by the ODNI. Russ Porter from ODNI was able to schedule a meeting of the Advisory Board coincident to our meetings, so these folks can now join our meeting. So please welcome: Number 1 -- over here, yeah, you look just like your photograph. Van Godsey, assistant director, Division of Drug and Crime Control, Missouri State Highway Patrol. Welcome.

Godsey:

Thank you.

Bradley:

You're welcome. Mike Sena, director, Northern California High Intensity Drug Trafficking Area, and Northern California Regional Intelligence Center. Steve Hewitt, director, Strategic Information and Analysis Center, Utah Department of Public Safety. All right. Russ, thanks for arranging this. Do you want to talk a little bit about your board and what it does, before we kick this thing off?

Porter:

Me be at a mic?

Bradley:

Please. Yeah, easier to transcribe.

Pannoni:

Either one.

Porter:

I'll be brief, and thanks for the opportunity to bring some folks down and hear the conversations, and be a part of the meeting. As the chairman said, I'm Russ Porter. I am the director of federal State, Local and Tribal Partnerships at the Office of the Director of National Intelligence. With me is my colleague, Dr. Sam Smith-Pritchard, who works in our Homeland Security and Law Enforcement partnership group. We've coordinated with others in the inner agency, and as the chairman said, we synchronized our meetings. These meetings that occur with about a dozen state and local law enforcement Homeland Security executives, who are appointed by the DNI to be his advisors about the state and local apparatus, helps the DNI understand what takes place in the domestic field. Certainly, the DNI in his role as the security executive agent has an interest in how well all of that is working. I just appreciate the opportunity to come down, Mark, and Greg, team, Tip, and being a part -- Charlie -- being a part of the meeting and allowing us all to participate.

Bradley:

Oh, you're most welcome. And thank you, having such a distinguished guest. Again, welcome. This is a democracy, so

please participate. Anything you want to have answered or asked, this is the forum to do it. All right?

So anyway, without further ado, let's go around the table. We'll go from me, Mark Bradley, the director of ISOO.

Pannoni:

Greg Pannoni, the designated federal official for the meeting, and associate director, ISOO.

Wight:

Lee Wight, vice chair.

Morgan:

Nancy Morgan, director, Information Management Services at CIA.

Richardson:

Ben Richardson, Industrial Base Protection, DOD.

Ederheimer:

I'm Josh Ederheimer with the Department of Justice, Office of Tribal Justice. I just want to say to Mark and Greg, and also Bob, thanks for bringing in the Tribal law enforcement

perspective, and recognizing the federal government's role in working with tribes and how it relates to national security.

Bob:

Sure. It's our pleasure.

Masciana:

Leo Masciana, State Department Office of Information Security, diplomatic security.

Licht:

Rich Licht, the Center for Internet Security and Multi-State Information Sharing and Analysis Center.

Cummins:

Elaine Cummins, FBI, Chief Information Sharing and Safeguarding officer.

Rogers:

I'm Charlie Rogers with the DHS Office of Security.

Dejausserand:

Rich Dejausserand, DHS Office of Security.

Lew:

Kimberly Lew, DHS Office, Chief Security Officer.

Ervin:

Jim Ervin, with the Office of Security at DHS.

Buckley:

Steven Buckley, DHS, Office of Intelligence Analysis.

Pichardo:

Millie Pichardo, FBI, (inaudible).

Jones:

Chris Jones, FBI, (inaudible).

Polk:

Ken Polk, Office of Intelligence Analysis, Department of Homeland Security.

M:

You guys still there?

DeLawter:

Denise DeLawter, Field Operations, Office of Intelligence and Analysis.

M:

Yeah, I think we lost them.

M:

Yeah, are you on the call?

F:

(inaudible)

M:

Yeah, I'm on the call.

M:

Yeah, I think the call is still there, it's just we lost the room.

M:

Yeah.

Bradley:

Excuse me, on the phone, can you hear us?

M:

We can now. We lost you there for about 30 seconds.

Bradley:

Just hang on, we'll get to you, just in a second. We're going around the room, introducing who's in the room. Then we're going to come to you all. All right. Please continue.

Johnson:

Kim Johnson from DHS, Office of Intergovernmental Affairs.

F:

(inaudible)

F:

(inaudible)

F:

(inaudible)

Bradley:

All right, and we've already heard from these gentlemen. So anyway, OK, on the phone, let me just start. Is Keith Szakal there? DO-- Department of Transportation?

M:

Yeah.

Bradley:

Glen Bensley, DOJ?

Patorini:

This is Rob [Patorini?], filling in for Glen today.

Bradley:

OK. Hey Ron, how are you doing?

Patorini:

Doing well. Thank you.

Bradley:

Good. Jeff Friedland, SLTPS Entity Member?

Friedland:

Yes, I'm here.

Bradley:

OK, good. Ben Leingang, SLTPS Entity Member?

Leingang:

Yes, I'm here. Thank you.

Bradley:

You're welcome. Dori Koren, SLTPS Entity Member? No?

Mark Jay Schouten, SLTPS Entity Member?

Schouten:

Present, and good morning.

Bradley:

Dewey Webb, SLTPS Entity Member?

Webb:

Yes, Dewey Webb (inaudible) is here.

Bradley:

Great. Angus Kirk? SLTPS Entity Member?

Kirk:

Yes. It's Agnes Kirk.

Bradley:

Yes, ma'am. Jessica Davenport, SLTPS Entity Member?

Davenport:

I'm here, thank you.

Bradley:

OK, and George Goodwin, Defense Security Service, observer. All right, anybody else on the phone who has yet to be identified?

Parsons:

Good morning, this is Darryl Parsons, Nuclear Regulatory Commission.

Bradley:

OK. Good morning. Anyone else?

Manley:

Good morning. Gary Manley from ODNI.

Bradley:

OK. Anyone else? All right. That's it. OK. One interesting housecleaning activity -- yeah?

M:

(inaudible) also wants to ask you on the phone, while they're not speaking to mute their phones, all the people on the line will be creating noise.

Bradley:

OK. Did everyone hear that? Those of you who are on the telephone, if you would mute your own personal phones so it won't interfere with your ability to hear or to speak.

Friedland:

OK, Mark, I am muted, I will be muted, but the closer you can get to the microphone, the better. We're having a little trouble hearing you here in Iowa.

Bradley:

Got it. Got it. I'm violating my own rules. All right. Let me just hold onto this thing, then. OK, one interesting housecleaning bit, and I'll pass this on. As you know, the SLTPS-PAC was created by EO13549. It does not have a sunset date, but like many federal advisory committees and the Executive branch, it's subject to renewal by the president every two years, in order to continue. For us, that means September 30th, 2017. So it's coming upon us. In the past, renewal process has been pretty straight-forward. The NARA Committee Management officer contacts us to confirm that the committee should continue, and it's always a yes. It's a pretty simple conversation. She then advises the Committee Management secretariat of GSA of this, and GSA obtains the information throughout the Executive branch, and EO then continues. This year though, it's been a little different. Last week, the archivist came down to see me twice and asked pointedly about this committee, and whether or not it should continue. I said it should, and I explained why. Then we had to give written justification for it to. And the questions weren't coming from him. They were coming from the White House and others in OMB. So I wouldn't be worried by that, but it's kind of pro forma. But we're in an environment where a lot of things are being looked at, and a lot of things are being cut. So again, I think

we've made a fulsome justification for why this should continue, and the importance of it. So again, I would be very surprised if anything were to change. But again, we're in, as you know, anybody who reads the newspapers, we're in uncertain times in a lot of different areas. So just kind of stay tuned, and we'll keep you posted as soon as we hear from GSA and everybody else that we've got the green light to continue. So hopefully, this won't be the 13th and last meeting. But anyway, I thought I would just make you aware of it, it's the first time it had ever happened to us.

All right. Lastly, please note that in your folders, these, we've got copies of the meeting agenda, the slides of one of the presentations, and the minutes of the last meeting. So at this juncture, I'm going to turn it over to Greg Pannoni, who will discuss old business.

Pannoni:

Thank you, Mr. Chair. This is Greg Pannoni. I did want to the mention, too, the full -- one of the handouts, we just have an excerpt, of the IG report that was done, just a couple of pages that pertained to one of the action items. But the full report we will provide to all the members electronically, and it's all

copied. It's 80-some pages, so we don't want to kill a tree to provide that here.

So as far as the minutes from the last meeting, they're in your packages. They were certified April 25th. One of the points about utilizing the audio recording, we're going to get these minutes out much, much quicker, by leveraging the use of the transcript from the audio recording. Along with minutes, together they will form a comprehensive summary of the meeting. That's why we're going to provide all of you with a copy of the actual transcripts. We want you to continue, even though it's redundant, to say your name each time you speak. That'll help with that.

Again, with the budgetary limitations, we don't have funds for travel and per diem to come to these meetings. But we do want to, again, note Rich Licht coming from New York to attend in person, the meeting. Thank you, Rich.

There were three action items from the last meeting, and each of those will be addressed later as we go through the agenda of the meeting. So I'll just quickly review them, and we'll move on. The one was to explore the issues related to fusion centers and

other state, local and travel personnel seeking to obtain JWICS' access, without the requirement of being detailed to a federal agency, or in any way having some hard-wired connection to a federal agency. Tip Wight is going to give us a brief update on that issue.

Next, DHS to invite a guest speaker for the meeting from the Office of Intelligence and Analysis, to discuss the issue -- excuse me, to discuss the process to prioritize Homeland Security Data Network, the HSDN, deployment for their Field Operations. So we'll have Denise DeLawter, I believe, here from the Executive office, she's the Executive officer of Field Operations.

Bradley:

Yes, and there's some additional folks from INA here, too.

Pannoni:

OK. All right, very good -- to have that issue discussed. So we're going to discuss HSDN deployment during that briefing later in the meeting.

Last, we have DHS is going to provide us an update on the implementation of what we refer to in the vernacular as the "hybrid approach." This, specifically, is adding to the National Industrial Security program procedures for sharing and safeguarding classified information with certain private sector and other non-federal entities. So we have Jim Ervin, deputy director from the National Security Services Division, who will speak to that later in the program. Any questions? Back to you, Mr. Chair.

Bradley:

Mark Bradley again, the chair. I am going to introduce Charlie Rogers, who will provide an update on the DHS SLTPS Security program and information about the realignment of SLTPS functions in the office of the chief security officer at the Department of Homeland Security. Charlie?

Rogers:

If this picks up -- so I'm Charlie Rogers. Any of you who have been to these meetings previously have heard me go over what we do, but I'm just going to give a few broad overviews of some metrics in the last year, what we've done. So part of the Security Management program for state and locals involve

security compliance reviews. We established a Security Compliance Review program in late 2012 that primarily visits state fusion centers that have HSDN at their locations. Those are our primary targets. Since 2012, we've done to date 83 compliance reviews. We've been to all the fusion centers more than once. We are -- this year, we've competed 12 compliance reviews. We expect to complete two more, which will give 14 for the year. We kind of average around 14, 16 a year at the state and local program. The purpose of the reviews are to validate that the state and locals are managing their classified information. They have a secure room. Part of getting a secure room and getting HSDN, there's a requirement that they appoint a security liaison, and that's a state employee who has responsibility to manage the classified holdings, manage the secure room, to assist the federal government in getting the appropriate training done. So we go out and we validate that that's being done. We identify problems. We help solve problems. We get involved in training the security liaisons. And they're really a key part to this program to make it work.

And then I'll talk a few words about the Security Liaison Training program. All facilities are required to appoint a security liaison. There has been, and will probably continue to

be, a certain amount of turnover with these folks. Some of them have a lot of longevity; they've been at locations for five, six, seven years, and they're really pretty good at what they do. Others rotate more frequently. So we always have a challenge to make sure that we're keeping them trained and appropriately knowledgeable on federal policies and regulations.

So one of the things we do in cooperation with Intelligence and Analysis is, we have these webinars. They're not exactly monthly, but we do about eight to ten a year. And we -- newly-appointed security liaisons, or liaisons who want to have a refresher training will call in to the webinar, and they'll receive a broad overview of training through the webinar, and be able to ask questions and talk to their counterparts in the federal government. So we've done that since, I think, 2013 that was started. About eight folks participate for these webinars, so we get about 60 to 80 people a year calling in and receiving the training. Then INA funds for newly-appointed security liaisons to come to D.C., for a two-day training session. They're about twice a year, I think, now. There's a pretty broad curriculum. I think it's two days you've got training provided by the Office of Security, training provided by Intelligence and Analysis. They receive training on

counterterrorism, on insider threat, a little bit. They'll get training on COMSEC, on OPSEC, on how to manage the secure room.

So there has been two of those -- well, there has been one this year thus far. And there's another scheduled for August first and second? Yeah. And that's coming up with additional four folks who are coming into town.

I think that covers pretty -- oh, just a few words on our personnel security metrics. We've been pretty stable. DHS has cleared approximately 7500 State, Local, Tribal, Private Sector folks. And the breakout is about fifty-five hundred of them, or state and local personnel, and about two thousand of them, nineteen hundred are private sector folks, who are working primarily with NPPD, and to some extent with cybersecurity, and those areas. Almost all of them are cleared at the secret level, that's the operating level of the Homeland Security Data Network. There are about 260 of them that are cleared to top secret SCI. They access SCI at a federally-managed [SCF?]; there's, what, one in Chicago and one in New York that are associated with both of those police departments, but they have a federal presence. And then the others access them at other federal entities, whether it be JWICS with the FBI -- or, not

JWICS, JTTF with the FBI, or they come to a DHS facility and receive briefings. So there's only about 260 out of the -- and there's no limit. It really is mission-driven what the requirements are.

And then the final thing I was going to talk about is, a little bit about a realignment, that I just thought it might be appropriate. The Office of Security was stood up when DHS was stood up in 2003. In the last year, we were told to review our internal structure to see whether it could be improved for efficiency. And the goal was really to look at how we can become a more enterprise-oriented, or enterprise-wide-oriented Office of Security, how to identify any redundant functions. Any duplicate of functions, how could we co-locate those? And so it was a long process of about nine months or so to go through trying to identify the new structure. The new structure was implemented in February. How it impacts the state and local is fairly minimal. The division that I had up previously was 100 percent focused on state and local activity. So we had direct support to fusion centers, the compliance review program, and we had a team of personnel security adjudicators who did state, local and private sector.

Well, under the realignment, we continue to have the state and local program. The adjudicators have been relocated back to the personnel security division. It was thought that putting them back with a larger division was a good idea. In addition, the division I have received, the training branch, was moved into my division. Because we did -- we have a pretty successful compliance review program, they decided to give the us all the compliance review programs in the Office of Security. So we're working to absorb all of that.

And in addition, there's the hybrid program that Jim Ervin will talk about. There's a compliance piece to that, which would eventually move into this division, which is an industrial security kind of compliance program. But because there were concerns that maybe moving the adjudicators out of the office and these other duties might create a problem, we stood up an internal Office of Security coordination working group. So that group has touched points to industrial security, which has touch points to the private sector. We have membership from the personnel security division so that we're meeting with those adjudicators. We've got my division, and then we've invited some other divisions to participate. So we're just working through that to have maybe monthly meetings and set up a mailbox

so that we know what each other is doing, so we're not acting independently. So that's what we've done to make sure that reorganization doesn't impinge on our formal structure.

And I think that's pretty much what I have to cover today.

Bradley:

All right. Mark Bradley, the chair -- does anybody have any questions for Charlie?

Pannoni:

I have one.

Bradley:

Go ahead. Yeah.

Pannoni:

It's Greg Pannoni. So Charlie, you mentioned, I think, 260 of that total number of clear people have top secret SCI:

Rogers:

Yes.

Pannoni:

So maybe you don't know right now, but of all the fusion centers, is there at least representation by one person or more at the TS SCI level?

Rogers:

Not necessarily, no.

Pannoni:

So OK, but my next question is, should that be a recommendation or a goal, that we have at least one person represented at every fusion center, at the TS SCI level

Rogers:

Well, I don't know that it's -- I don't know that it's necessary, because it's mission-driven. I mean, there are fusion centers that have people who are working in the JTTFs. There are fusion centers that have people who are traveling to D.C., or who are on committees, and they're -- but I don't know that just giving someone TS SCI access and just having them sitting somewhere --

Pannoni:

Right, putting it out there as far as the beginning of a process --

Rogers:

I mean, there's no restriction, you know --

Pannoni:

-- to enable quick access at every fusion center.

Rogers:

Yeah, and then the governors --

Pannoni:

To that level of information --

Rogers:

You know, the governors have TS clearances and are immediately eligible for SCI access without an investigation.

Pannoni:

Right. True. True.

Rogers:

They can be read in. But, I mean, if somebody else wants to weigh in on this.

M:

I think Mike would like to comment.

Sena:

You mind if I pop in?

Bradley:

Just introduce yourself, Mike.

M:

Yeah, speak into that microphone.

Sena:

Mike Sena from Northern California HIDA and Regional Intelligence Center. Just as was said, if you don't have access to (inaudible) for the data, going through an SCI process may not be the bests scenario, and may be a waste of resources. So I think it's got to be role-based on the clearance level that the person receives. If there is a need, then maybe there should be more than one person in that center that has a SCF

nearby, or the need based on the roles and responsibilities within the center. But I wouldn't say that, hey, we want to put 78 SCI clearances out there across the country, just because. It has to be through that evaluation process. Because I think that's one of our biggest issues right now is, you know, we have individuals that do not have even their secret clearance, and are unable to get into their own workspace up to a year or to a year and a half. So that compromises our business capabilities. So I think in those areas, we should focus on what they need to get into their seats.

Bradley:

I just have one question. You mentioned -- this is Mark Bradley -- the NYPD and the Chicago Police Department. What about something like the LAPD? I mean, how does a police department --?

Rogers:

Well, I have to previse this. You know, I work for the Office of Security, and we facilitate the classified mission. But we really -- it's Intelligence and Analysis within DHS that identifies where the requirement is. And that has to do -- and anybody from INA who wants to weigh in -- that has to do with a

conversation between INA and their mission relationship with the state and local partners, when it reaches a threshold that they've made some decision that this is necessary, then the Office of Security gets involved in helping to certify. But did you want to say something, Ken?

Polk:

Ken Polk form INA Office of Security. So when Secretary Napolitano was the secretary for Homeland Security, she authorized five tier one USA cities to have SCFs that we would support. Three of those, I already had them -- or, excuse me, two of those I already had them. One is still outstanding, and that would be Houston. But then New York and Chicago. So that was to try and contain the number of SCFs, because we could see SCF creep going throughout the country. So now what we're doing is managing. It's up to the individual fusion center or entities, because there's more than just the fusion centers out there, that it's their requirement to provide to us their justification as to why they need access.

The other challenge that we have is, DHS does not have SCFs in all of these major cities where the access is required. So part of the package that's required to DHS is that there must be an

agreement with a SCF that's willing to sponsor you, because as was mentioned by Mr. Sena, it makes no sense to process you for a TS SCI clearance if you're not going to have access to that information. And all the fusion centers are at the secret level.

The other piece that we factor in is, who are you going to be sharing this information with? Because the majority, obviously, with 260 plus TS SCI clearances, the majority of those folks aren't going to have access to it. And I would just add that the bulk of those 260 plus clearances are those that are assigned to New York, Chicago, Kansas City. You know, we do have some that are scattered throughout the states. But others are the [NOC?], the rotation officers, for the NOC. So that's a large percentage. In 2015, I believe it was June of 2015, then under Secretary Taylor signed out a policy guidance on how to obtain access at the TS SCI level, if there's a bona fide justification to have such access.

So we do have those processes in place. We've had a few that have trickled in requesting access under that policy, and the first ones, I'll be completely honest, was a bit of a challenge. But there have been a few that have come in that it's been a lot

easier to process. And the other fact is, we've now got the SCF where we can get the individuals induct once they're cleared by DHS. That was the biggest challenge that we were facing at that time. But I think we've resolved that. I haven't heard too many other issues there.

Wight:

Thank you very much. And if I could -- this is Tip Wight -- just to kind of piggyback on that, keep in mind when we talk about this that there's kind of three levels of use of TS SCI clearance. You know, the comment about who you're going to share the information with off times. And most of the senior leaders that fusion centers support, i.e., governor, Homeland Security advisor, mayor, have a top secret clearance. And if the fusion center leader is supposed to be their senior Intelligence advisor, being able to share that information with the senior leader is critical. To do that, you have to have the access at all levels. Again, obviously, what's at the SCI level is often not significantly more than is available at a terror line level or below, however common. There's the ability, number one, to attend meetings just to get into the spaces. You have to have a TS clearance. There is the -- then, which is why I'm pushing for this and have been advocating, that once you

have the clearance, there's -- you're not able to communicate and share with your peer analysts at a peer to peer level, other than physical going and sitting in a room and talking with them. Which, again, is why I'm pushing for state and local appropriately-cleared analysts with the appropriate need to have access to JWICS, so they can go to the National Counterterrorism TS site, which is where most of their content's supposed to -- or collaborate on a peer to peer level.

So there's the information sharing to your senior leadership, as the senior Intel advisor. There's the meeting attendance, you know, participation, and the peer to peer functioning as full-fledged Intelligence analysts, which is, for the most part, what's being hired across the country in these fusion centers, professionalized, trained. But then you get them to a level to where, well, there's a point where you can't evaluate Intelligence on your own. And you can't see sources and methods, which doesn't make sense, in my estimation.

Bradley:

Thank you very much. OK, we're going to move on. James Ervin, deputy director, National Security Services Division, DHS, will provide an update on the hybrid.

Ervin:

If you don't mind, sir, I'm going to sit up here at the podium.

Bradley:

Not at all.

Ervin:

I apologize to be at your back, but thank you. Good morning, ladies and gentlemen. Appreciate the opportunity to come to you and give you an update, if you would, on the hybrid program. As Greg alluded to, it's called a "hybrid program." It's a classified critical information protection program that was derived from a 2014 Cybersecurity Act that was implemented. In December of this past year, the White House approved additional requirements associated with this effort, so we're underway at this point.

Let me pose a few things, if I can, for you. This is a joint effort between our Office of Security and the NPDD, which is the national responsible party, if you would, for the sharing of information, classified information, with the private sector, and specifically companies that are not being processed under

the traditional National Intelligent -- National Industrial Security program. And the reason they're not being processed through there is because they're not considered contractors to the government. However, they require cybersecurity threat information so that they can perform activities at their end to protect the critical infrastructure of that organization, because the government felt that those entities needed to be protected, OK.

So I'm going to go through a few things, if you would. Charlie has briefed us before, my understanding. So I'm going to make an assumption that most of you know what this program is about. But I will try to strike a balance in between those who are not aware of it, as opposed to those who are.

So the foundation document for this is EO13691, and that is the document that basically calls out the need for this mission to be performed, and provide that threat information to the organizations, the companies, if you would. CSO's role is solely for the safeguarding portion of this task, if you would. And what we have done is, we're working with NPPD to identify and prioritize the companies that need to be protected. We have deemed those companies to be, at the front end, Section nine

companies, which are critical to our infrastructure, that in the event something were to happen to those organizations, those companies, that might be considered a catastrophic or grave damage to national security. It's based off a White House memo as I mentioned to you earlier. But I want to touch on a couple of things that we're at today, is basically a progress report for you.

We're trying to reach what we call, "initial operating capability." In order to do so, what we had to do was identify what are the critical needs, requirements at the front end that need to be performed, in order to get to a final operating capability? So what we've done is, we've coordinated our efforts with NPPD and asked them to prioritize our list of companies. Might I offer that the company list was extensive at first, we've asked them to narrow it down, and they've come back with the Section nine companies that they feel are critical and need to be addressed first. So we are looking at taking on those for evaluation. In addition to that, what we've done is, we've established a management directive, which equates to a policy for the purpose of the government at large, on how we will operate going forward. And in addition to that, we have

generated quite a few product lines that need to be performed to process these requirements.

For instance, each one of the companies will nominate, if you would, individuals to have TS SCI clearances. We have asked that that number be kept at a minimum, so that the threat information could be passed to those individuals. We've also asked that the individuals assigned that the hierarchy within those companies not be engaged with the individuals that we clear at TS SCI. So we've asked them to execute Exclusionary Forms, so that will exempt them and keep them out of the forward, if you would, from having access to that information.

As I go further, we've done fact sheets, checklists, training materials. Charlie mentioned earlier that the hybrid will also consist of a compliance and oversight piece, and yes, we are working on those products as well.

So to touch on initial operating capability -- one of the items that we need to gain approval for is information collection. So DHS has to have information collection authority in order to collect the information from the companies, and then proceed through what we call a foreign ownership control and influence

evaluation. And then we identify what mitigation can be put in place to offset that threat that might be posed with regards to these companies.

Working with the DSS and the DOD, we have identified -- we're in the process of identifying what is it going to take to do FOCI analysis; what I term "FOCI analysis," as well as mitigation procedures. We have resources dedicated to this level of effort for hybrid. Current standing is four, and we anticipate an FY19 obtaining additional resources. We have projected out 18. Those 18 individuals will be assigned to the hybrid program, specifically working on policy and procedure. Security clearances will be required for each one of the company reps, so we're going to have to have a staff that's going to look at and evaluate their security processing forms, and take care of that action. We've also identified a need to put individuals into compliance and oversights, so Charlie will gain some additional bodies that will be responsible for doing oversight. I would not anticipate oversight being executed in FY19, but in the out years you could see that happening, because we have to make sure that we have a uniformity and compliance issue consistent throughout. Currently we have two resources of our four, down at DSS Quantico, for the purpose of understanding the folk I

process and the mitigation procedures that they are utilizing. We've also benchmarked, if you would, NRC, DOE and some of the other CSAs, in terms of how they are proceeding with regards to FOCI analysis of a company. These companies will still go through FOCI, and at the point in which we feel that they cannot clear FOCI, they will be referred back into the NISP process, if you would. But it's anticipated that we'll try to work with the companies as best we can, so we can clear as many individuals as possible for the access to classified.

One other thing that we've done in terms of proposed resources in the FY19 period are, we're looking at a system of record, if you would. We need to be able to put this information somewhere, and our current setting, if you would, our data system that we have at DHS, we can't -- we want to separate these companies from that system. And the reason being is because they will be providing quite a bit of input to us that is deemed proprietary in nature and cannot be shared out, so we want to give them the secure means by which they can forward that information, and we can evaluate it.

So what we've done is, we've benchmarked some systems, e-FOCI and e-FCL. And we also have looked at NIS' system, that DSS is

looking to run, I think, in the fall time. They'll go active on that system. We're trying to figure out which one would best fit our needs. So right now, we're working that through. We haven't made a commitment per se, but we're in current evaluation in that forward, if you would.

Now, one of the things that I'm going to point out for the purpose of the panel here, is the notion that we have two issues that are pending that are associated with this program, in my view. And what they are is, information collection authority, if you would. We determined that the existing form, standard form 328, cannot be utilized by DHS in its current state, and the reason being is because it was intended for select organizations only; that being primarily DSS. But it was never intended for DHS use. Our office paper reduction action, our office has reviewed that and determined that there's a need to develop a light form, and/or go back to DOD and request that the form be, if you would, improvised, or changed a bit to become a common use form for more organizations. So DOD is working on that right now. We're anticipated response back on that in four to six months, and that's underway. So we appreciate that from DOD.

The second piece, of course, being in the out year funding efforts. We projected again FY19 to have 18 personnel assigned to the program. Of course, that will come back to us with the final disposition as to whether we get 18 or less. From there, we'll further grow out the program in the out years as well. That I bring up to your attention because of impact to the program. We have to have resources in place to support the program. The four personnel right now are -- two of those four, if not three, two of those four actually spending half their time doing their daily operational mission that they have, in addition to hybrid. So we've split that resource as well.

Finally, the program is needed because the classified information with regards to these critical infrastructure entitles that we're sharing with needs to go to their attention, so that they could, in turn, respond appropriately and protect our national security interest needs. The government has determined that the lack of that information to them poses significant issue for our organization, for our government at large, if you would.

Are there any questions for me at this time? Yes, sir?

Licht:

Rich Licht, CIS. (inaudible) cross sector, even if you can't name them? What do they represent?

Ervin:

They represent some critical entities within the gov-- not -- within the private sector that need to be protected. And I'll give you an example, if you would. Banking industry, energy, and some of the other critical infrastructure sectors that we have. So we're trying to protect those organizations. And they normally don't have -- they don't have agreements with us in place right now as contractors to obtain information, or provide them information. So we need to be able to provide information back to them so that they can effect some change within their organization. Cyber threat-related information.

Licht:

So this supposition is the information flow is one way? Or both ways?

Ervin:

So the idea would be, its sub-position is that it goes to them. And what we would hope is that there's a reciprocal, because in

the event that information comes to their attention, and they want the government to be informed, it would come back to us.

Licht:

But not a requirement, just --

Ervin:

Not a requirement. Exactly.

Licht:

OK. Thank you.

Ervin:

OK. Any other questions you might have? All right. Thank you very much.

Rogers:

I'd like to add a couple of comments.

Bradley:

Charlie. Introduce yourself.

Rogers:

One thing about the hybrid, or this program, is that it's very complex. It's -- DSS has been doing industrial security for years. They have hundreds of employees who have a history of doing it. So we are struggling with the limited resources we currently have to acquire some pretty robust expertise. So Jim and other people in the office have made a lot of progress. But we know that it's going to take us time to develop the real depth of expertise that is in the existing industrial security program.

Bradley:

Well said. OK. We're now going to hear from Denise DeLawter, executive officer, Field Operations, Office of Intelligence and Analysis, DHS who will provide an overview of DHS' Field Operations SLTPS support. Welcome, Denise.

DeLawter:

So how do we change slides? Do I just say, "slide?"

Bob:

Sure.

DeLawter:

You'll do that for me?

Bob:

Or can press there. But I am very happy to do it, yes.

DeLawter:

OK, sir. I appreciate that. And your name is?

Bob:

Bob.

DeLawter:

Bob. OK. Good morning. My name is Denise DeLawter. I'm the executive officer for Field Operations. Thank you for having me come here. I've been briefed that this is a very friendly and congenial group, and I look forward to briefing you. I apologize up front if this is a very nascent briefing for some of you that are in this room, so bear with me.

A little bit about me; I'm a retired Lieutenant Colonel from the Army. I spent my last tour at the Pentagon. The plane, unfortunately, hit my section of the Pentagon. We lost 26 out of my office. So when I retired, I decided to give back to the

country and go to work for DHS. And a lot of people at INA have done the same, and I'd like to think that that's why we're there, is to give back to the country. And so I'm fortunate enough to be working in Field Operations, and we consider -- and pardon me for you that work in INA -- we consider Field Operations the center of the universe for that organization. OK. Slide, please.

So, there's the center. This is the INA. And as you can see, we have an acting under secretary, Patty Cogswell. Field Operations, in the red circle, is under our -- under secretary for Intelligence Operations, is currently being directed by Vince Smith, because our current director is acting Intel Ops until Mr. -- hopefully Mr. [Glowie?] is confirmed as the under secretary, then we will hire an Intelligence Operations director, and then Robin Taylor can come back down to be our director. Next slide.

This is Field Operations Division. Under the Division, we have a deputy director. I'm the executive officer. And then Field Operations, most importantly, consists of 12 divisions, regions within that division. Each region is broken out across the country. Next slide.

We have, by billet, 113 personnel across the entire division, with 12 division directors -- excuse me -- regional directors, 61 Intel officers, 29 Reports officers, only one Intel analyst -- and we hope to change that -- and then, at the headquarters, the tooth to tail ratio is a little bit small, but we have 10 personnel. Next slide.

This is the map, we call it our "field footprint." It's broken out into 12 regions across 14 time zones. The regions are aligned with the domestic DNI regions on purpose, as directed by Congress. The stars represent the regional directors where our IOs, Intel officers, are deployed, our Reports officers and our one Intel analyst. We also -- I just want to point out that we have an IA -- excuse me -- an IO in Guam, in Hawaii, in the Virgin Islands and Puerto Rico. A lot of people say, "Ah, the Virgin Islands -- great place to be," however, it's not all that it's cracked up to be. It's not a vacation spot. The fusion center director's house was actually shot up. We had our IO deploy there with a pregnant wife. We had to deploy special security for his house; it's a high gain threat area. It's not the garden spot that some would think it might be. Next slide.

And this actually lays out the fusion center names. It's a bit busy; we are in the process of updating this slide, because it is changing, as you might expect. It's only as good as the week that it's printed, and then it continues to evolve. But it lays out where we have deployed our personnel. Currently, we're at 102, deployed across the country, in our territories. It's really important to note that it take a really unique individual to be an IO, and I'll get into that in a little bit. Next slide. Oh -- and let me just say, I'm not going to take 40 minutes of your time. I know this is -- you have a very short period here.

I and A, an overview -- the highlight of this slide, please just understand that our deployed personnel are trying to build relationships and enhance the Intelligence and information sharing mission, focusing on and sharing information with our private sector partners, working with the IE, the IC and our Homeland Security partners. Our IOs specifically work on the Intel in the Intelligence cycle, support the threat-related information sharing, and support fusion center partners. Next slide.

Field personnel responsibilities, the focus of this slide -- well, it was our deployment of personnel was initiated based on the recommendations of the 9/11 Commission. The assist fusion centers and the SLTTP partners and sharing and analyzing Intelligence information, they provide production and dissemination of intelligence and information to our partners. They facilitate the fusion center access to training through our partner engagement branch -- thank you. They facilitate -- or, excuse me -- they assist in identification of threats and hazards, and they facilitate access to specialize subject matter expertise within DHS and the IC. Next slide -- and I think some of you have seen this slide before.

What a fusion center is and what it is not -- I just want to focus, and I'm just going to hammer this home -- it is state-owned, it is state-owned, it is state-owned. It's hard to get people to understand that. You in here understand that. It is positioned to provide a local context, and it is flexible. Each fusion center is different. I'm going to read this quote; it's dated, but it really rams this home: "Fusion centers, which I think are a great step forward, something that didn't exist 10 years ago, and there are now some 72 of them. And very candidly, some are much better than others. I visited some that

I think are extremely capable. There is a federal nexus to ensure that appropriately-designated information is shared quickly with state and local officials." Director of National Intelligence, James Clapper, to the House and Senate Select Committees at a joint hearing on threats against the U.S., September 11th, 2001. He actually made that quote in September, 2011. That's how important fusion centers are, in his mind, that long ago.

What a fusion center is not -- it is not focused on terrorism, and it is not owned by the federal government. Next slide.

An overview of what fusion centers are -- just one -- I know you're not supposed to read your slides, I know that's PowerPoint 101. But just in that blue box, "A fusion center is a collaborative effort of two or more agencies that provide resources, expertise and information to the center with the goal of maximizing their ability to detect, prevent, investigate and respond to criminal and terrorist activity." A fusion center can contain one or more -- actually two or more -- of the following entities: Health, private sector, fire, National Guard, FBI, law enforcement, public safety, criminal bureau, emergency management, state police, and corrections. The fusion

center has a conglomeration of all of those individuals. They work together during a crisis -- again, you all know this. Sorry if I'm being so nascent about it, but the idea is to come together during a crisis, even during non-crisis, to work through issues; the idea, again, to gather and share information. Next slide.

Our resources: We send Intelligence officers. We deploy them to these fusion centers. Our current strength, as of this week, is 62 Intelligence officers, 26 Reports officers, SROs and ROs -- Senior Reports Officers -- one Intel analyst and 12 regional directors. It takes a very unique individual to be an Intelligence officer. We go through a vetting process to ensure we have the right person to be an Intelligence officer. We can't have an extreme introvert that just sits in the corner and waits to be told what to do. We can't have an extreme extravert that is overbearing and aggressive; i.e., I would fail as an IO. We have to have the right mix; the right kind of person that waits for the right time to walk up to the fusion center director and say, "Hey sir, I'm here to help." Our initial -- when we initially deployed IOs to the field, they were told, "Yeah, you're from DHS? Why don't you go sit back there in that corner?" And then at the appropriate time the IO would come

forward and say, "You know, sir, I can get you a clearance, and we can get HSDN deployed," -- which I know that's why I'm here, just wait, give me your time -- "we can get HSDN deployed to your fusion center. We can have classified, secret level information. We can start sharing that information with the appropriate people. We can help you do your job." "Oh, really? OK. Why don't you move up a row?" And so that kind of rapport, that kind of information sharing helped establish a network, helped establish the network of national fusion centers across the United States.

Our IOs are very unique individuals. They are interviewed and selected and then deployed, and they're part of that regional team. Our regional director right now in the New England area, she, Lisa [Palmieri?], used to be a military and state analyst. She was part of the presidential IACEU team. She was an IO, and she is now an RD. Roger Blair is a retired metro police department officer. He led the Special Ops team. He was a regional threat analyst, he was on the bomb squad, and he worked in our headquarters, and he's now an IO in D.C. Macy Huntsinger, very young, oh my, was a Navy officer. She was an IO at headquar-- and then she worked at headquarters. She was the RD for the mid-Atlantic region, she is now the RD for the

Central region. And Eric Kennedy is a retired Lieutenant Army Colonel, with extensive tactical Intelligence experience. And he is now the regional director for the Southeast. A lot of military in there. That helps during a crisis situation. But these individuals bring a lot to the table, and they bring a lot to our team.

OK, the next bullet -- we currently, as of this week, have 77 deployed HSDNs to our fusion centers. And they provide that secret connectivity to those fusion centers. Next slide.

Regional directors -- these are the individuals that are part of the military speak, are the chain of command. They run all of our assets in that region, to include the Reports officers and the IOs and the IAs in those regions. They are the DHS representative to the DomDNI in that area. They supervise the national level Intelligence support, with our partners in federal agencies representing DHS. And they supervise and engage information sharing with our SLTTP partners. Next slide.

IOs, I've kind of gone on and on about them. Basically, they execute the collection, analysis, and engagement of information sharing, the implementation of intelligence cycle. Next slide.

Reports officers -- Reports officers, importantly, help develop and write our IIRs and FIRs. They support the RD in the development of our regional collection plans. They focus our planning and collection efforts in that region, and they review and evaluate our regional IIR submissions. Normally, I throw up a map again, just to reorient you, but I think you guys got it.

And finally -- next slide -- our Intel analysts. We have proposed to provide an Intel analyst to each region to help facilitate that analysis and to help fusion centers, help develop that analysis process as well. Last slide.

Do you have any questions? I knew you would have a question, sir.

Wight:

Just quickly -- Tip Wight again -- previously, I believe all the IOs assigned to fusion centers were sent to be reclassified as ROs. But I see you're breaking that out separately. Has that been a policy change to DHS slightly, or not?

DeLawter:

No. We always separate IOs and ROs. There was a discussion in 2014 when Congress directed us to limit our number of IOs to 60. We looked at re-designating them, but we have since decided to keep them separate. We are in the process of looking at and designating HCOMs, Human Collection Operation Managers, to help define and focus that collection effort, but we are keeping the ROs separate from the IOs.

Any other questions?

Scott:

Mark Scott from Iowa. I want to thank you for the work that [Jerry McNitch?] has done, our acting IO from Omaha, to help connect our state's emergency operations center and joint forces headquarters secure room through HSDN. Very helpful. Going to be very convenient during a significant event. Thank you.

DeLawter:

Thank you, sir. I cannot believe there are no other questions. I thought that the whole point of me coming was for how to -- I'm sorry, I don't mean to bring upon any sort of firing here.

Bradley:

Yeah, there was some discussion about the criteria for deploying HSDN was what --

DeLawter:

Yes. To my understanding, and you can -- I would have you just sit at the table by the microphone, but to my understanding, the deployment of HSDNs is designated by the primary, the designated and the recognized fusion centers by those states. And so if there's a designated or a recognized fusion center, they are authorized in HSDN. If -- and that is it. There is no other authorization for HSDNs to my knowledge. Now, I also know, and we are feeling the pain of moving HSDNs when that designated fusion center changes. So when a state decides to change their designated fusion center from one location to another, because we -- or excuse me -- DHS pays to stand up that room and pays for that equipment, we then have to burden that cost to move that equipment. And it's not a cheap thing to do. But that -- HSDNs are authorized at the designed and the recognized location-- or state fusion centers only.

Pannoni:

Greg Pannoni. I have a different question that goes to the map and the deployment of all the Intelligence officers and Report

officers, and the discussion that you had about -- or one of the slides talks about sharing among federal entities. I know it's a different mission, but DOD, DSS in particular, they have Intelligence analysts spread throughout the country. They're working more with contractors. But with today's environment, and so much goes back to cyber, there could be a bleed-over in issues, whether it be concerning the Homeland Security or the resiliency of a system that applies to classified and other areas. So I'm asking, is there any collaboration that the group that you represent does with DSS and their Intel folks that are spread throughout the country, similar to how your group is?

DeLawter:

I can just tell you that that collaboration happens uniquely with each fusion center. I, personally, experienced it when I was able -- lucky enough to support the Republican convention. And I went up and was able to sit in the FBI building and work with the entire group that supported that convention. So if there are other entities supporting in a fusion center to include DSS, they will have -- they will collaborate within that environment. So if there was a fusion center that has that type of -- those people with that type of information, there is collaboration. But each fusion center is unique. So if there

is secret information, if there's an HSDN room, and they need to collaborate that information, yes, that kind of collaboration is going on. The IO's role is not to just sit at the table and work on his computer, or her computer. The IO's role is establish relationships, establish rapport with all of the people within the fusion center, with the community, with the police, with first responders, with the mayor, with the HAS, obviously. The IO needs to work with all of the primary players within that fusion center. So if there are other members within that fusion center, then yes, they would be collaboration. Did that answer your question?

Pannoni:

Somewhat. I don't know that -- I don't think, in fact, that DSS folks are directly affiliated with the fusion centers, so it will require reaching outside of the fusion center for this coordination/collaboration to take place. It just seems to me that there might be some valuable information that both sides could share with each other, on occasion, if those connections are established.

Richardson:

Ben Richardson from DOD. So DSS is highly connected with the FBI and local law enforcement and all the different regions they're at, against specifically, and can definitely do an RFI out to the regional offices to see how well they're engaged. I think it is unique in each region, depending what the industry is there. DSS's location across the country is not as evenly spread. It is based upon where (inaudible) industry is at. And so I do think there is a level of engagement there. I think it just varies, depending on the region.

Polk:

Ken Polk, INA DHS. And I would just add, recently, Vince Smith and I met with the National Guard bureau, because that seems to be where a lot of the collaboration has taken place in the state and local. Working with the National Guard bureau to kind of leverage and work some information sharing initiatives there, as well as utilization of facilities, co-utilization, both of our -- our fusion centers are areas that we have and they're their facilities as well. So that's happening at the national level. It's not necessarily -- I'm sure that there's one-off at the fusion centers, but it's not a national effort. But it is at the national level.

Scott:

Morris Scott -- and to follow up, not only are all fusion centers are different, there are a lot of differences among them. Same is true for states and the relationships between the Homeland Security office, the governor, the fusion center. Sometimes in some states, the fusion centers contain the Homeland Security advisors, or they're part of the Department of Public Safety, in other states they're not. And if you put all your eggs in one basket, I think you're going to miss 10 to 15 states where the Homeland Security advisors are separate from the fusion centers. I understand the convenience, and understand the need for maybe administrative streamlining. But I think at the local level, one size does not fit all for fusion centers and for states.

DeLawter:

No, I totally agree, sir.

Bradley:

I've got one question -- Mark Bradley. Could you comment on what kind of finished Intelligence products your analysts produce? And who do they disseminate them to?

DeLawter:

So our finished Intelligence products include FARs, Field Analytic Reports, IIRs, and they are disseminated back to the headquarters, and then they go out to the IC.

Bradley:

Does anybody else have any questions for our speaker? Gentlemen, don't be shy. All right. Thank you very much.

DeLawter:

OK. Thank you for your time.

Bradley:

Not at all. All right, I'm going to try to inject a little bit of fireworks in to this meeting here. We're going to turn to a different topic, brought to us courtesy of our friend over here from the DNI. We're going to talk about the joint IG report, "Review of Domestic Sharing of Counterterrorism Information," which came out on March -- in March 2017, by the Inspectors General of the Intelligence community. Also, the Department of Homeland Security and the Department of Justice on the topic, "Review of Domestic Sharing of Counterterrorism Information." There's good news and interesting news in this report. The good

news is that the OIGs concluded that the partners and the information sharing environment, DHS, DNI, DOJ and the state and local counterparts are committed to sharing counterterrorism information. I mean, that's good to know that this isn't all going to waste. But you never have an IG report without some recommendations and maybe some criticisms. And so in this one, the OIGs identified improvements that needed to be made, and practices and processes. One of their findings was that varying requirements for state and local security clearances sponsored by federal agencies can impede access to classified systems and facilities. It's kind of a straight-forward recommendation that we've heard over and over again. The DHS OIG recommended that DHS coordinate with the ODNI and FBI to develop and implement a strategy to efficiently and effectively provide security clearances and reciprocity to state and local personnel.

Because clearances and reciprocity touch on the core of information sharing for this program, we thought it was important to discuss this issue. So we're going to have a -- I wouldn't say a debate, but perhaps a discussion --

Cummins:

We're not debating, we're agreeing (inaudible).

Bradley:

OK. All right. So what we're going to do is, we're going to hear from you, the FBI? Identify yourself.

Cummins:

Well, I have some support here. But I did want to include everyone. But I think when this first came to my attention, I thought, gosh, we settled all that seven or eight years ago. And as I dug in, it turns out that it was nine years ago in 2008. It has always been the FBI's policy that everyone -- all FBI employees who were going to be in our secret space have to have a TS clearance. It's a complicated explanation, but that's just always been our policy, right? We all have TS clearances. Most of our space is secret, that's just the way it's always been. So as the fusion centers emerged, and as we realize that there was a problem, so it's not a matter of reciprocity -- so we had to -- but it's a matter of the FBI requirements for a TS clearance, as opposed to a secret.

So we worked out, in 2008, an agreement that we would permit, not just in fusion centers, but in joint spaces, we would allow the -- we would mitigate that requirement. And we put out an EC

in 2008. Were you in SAC in 2008? You might have seen the CC. But where we gave instructions that, again, stating that a top security clearance is required for unescorted access in proximity of FBI.net, and a lot of it did have to do with the security requirements around our system -- the EC actually came from the CIO, and was jointly signed with the security division, AD. But we decided that it was an acceptable risk for non-FBI fusion center personnel to be granted unescorted access, with physical access to FBI.net desktops, as long as they possess at least a secret security clearance. And so that went out in March of '08 to everyone. And then in November of '08, the MOU was signed by, I think -- I don't think DNI -- yeah, I think it was just FBI and DHS -- signed a -- it's not an MOU, it's a reciprocal security construction standard for DHS, FBI, sponsored state and local secure areas. But anyway, the mitigation -- it didn't -- this agreement doesn't specifically state that standard.

But I wanted to mention it because it really was about standards for facilities, and how to build them, and how to make spaces secure and so forth. It was more of that kind of agreement. But the mitigation, the reason that we were able to mitigate this problem is that in these secure areas, classified

information that's not under control and observation of an authorized person is to be stored in a GSA-approved security container, and the standards for that. So if we felt that with that mitigation -- in other words, you have to be more careful with your classified information when you're in a fusion center, or something that's not FBI space. If people who don't have these clearances are in that space, just being more careful with it. Basically, I think it translates into, they lock it up at night, or put it away at night, I think.

Bradley:

They remove the hard drives, I think, too.

Cummins:

Yes. So what happened in New York, nobody knows exactly how -- there was -- what happened was, the location moved, the (inaudible) moved to a new location. So we're assuming that the new security officer probably didn't know about these 2008 documents. And that's what caused the problem. But we didn't change our policy in 2015. The IG report just -- they just missed it. I'm not sure they talk to -- but it's not correct, what's in there. But our folks, our security people, are working with Charlie and other of his folks to straighten that

out in New York. And once they get all that straightened out, then I'll work with our office of partner engagement, and we'll send out some kind of refresher. We'll re-publicize these nine-year-old documents just to try to make sure that -- in nine years, faces change. People forget, and so forth. So we're going to do something. But I want to let these guys finish their negot-- what they're working on, to straighten out the New York situation. Then I don't know, Charlie, you may have more --

Bradley:

For the record, that was Elaine Cummins of the FBI.

Cummins:

Yes, excuse me.

Bradley:

All right, Charlie, you want to go ahead and amplify?

Rogers:

Charlie Rogers. So we initially met with our representative from the FBI on June 6th, and ODNI was there; Valerie [Corbin?] from ODNI. We found out didn't have the exact right person in

the room. She was very helpful. She was out of their personal security division. So we subsequently met, and a number of people in this room met with the FBI. And there were about seven FBI employees in the room to discuss this issue. And pretty much, it's what Elaine said. They have the existing policy, the policy permits access to occur. They were going to -- the last takeaway was, they were going to -- the FBI was going to reach back to New York, make sure they understood clearly the context, which they believe they understand, and then they were going to get back to this.

Bradley:

Let's stop this for a minute -- Mark Bradley. Would you amplify a little bit of exactly what happened in New York, for those of us who don't know? Or the people on the phone?

Rogers:

Well, all I know is, from what the FBI report states --

Bradley:

An incident of some sort.

Rogers:

Yeah.

Cummins:

Well, yes. An I don't think either one of us know exactly what happened, but --

Rogers:

The way it's written in the IG report was, they could not get on an escorted access with a secret clearance unless they had an SBI investigation to support that secret clearance. It's written as if there's a reciprocal clearance issue, and actually it was a criterial of applying an SSBI to get access to a room and access to the proximity to the systems, which I believe the FBI policy already addresses. But maybe the locals weren't away. But I don't want to speak to what I don't know.

Cummins:

We don't know.

Pannoni:

But fundamentally -- this is Greg Pannoni -- I want to make sure I understand clearly, and all of us do. We're talking about a

room or an area that is authorized to store up to secret information, correct?

Cummins:

Right.

Pannoni:

So I'm baffled, I really am. I don't understand what it is that causes the Bureau to say that a secret clearance is not acceptable for a room that is authorized to store only up to the secret level.

Cummins:

I don't know why that's true, either. But that's true for all FBI employees. Do you know? You were -- do you know why -- he's a former SIC.

Licht:

I can tell you -- no, I was there at the time that it happened.

Bradley:

Identify yourself, please.

Licht:

It's Rich Licht, with the Center for Internet Security. But when I was in the Albany division of the FBI before I retired, which is where I retired from, there was two issues. One is the diffusion center, which is run -- at the time it was a (inaudible), it wasn't the (inaudible). That was a predecessor to the statewide effort; it was the upstate New York Intelligence Center. That was a state facility that was very early on accredited -- it was never accredited for the open storage of secret. The FBI field offices, the entire facilities accredited for the open storage of secret. That confluence of what the requirement is to hire FBI employees, which is the SSBI that results in the TS clearance -- not necessarily SCI, but TS -- that's an employment requirement. So the assumption is that everybody on the floor of the FBI as an FBI employee has a TS clearance. That's true. That does not mean that you need to have -- what that resulted in is a requirement that anybody who didn't have that, regardless if they were cleared to the secret level, was required to have escorted access within the FBI office space. That was not the (inaudible). The translation of that to the (inaudible) was done in error. It was remedied, and my belief is -- and I left there in 2012 -- there was no issues with it, because we co-locate our space right now, the

(inaudible) is co-located in the building on the first floor, with the (inaudible), which is on the second floor. We share facilities, we share -- some of our people are cleared just to the secret level. And there's never been an issue relative to the ability to move about the space. I think you've hit it right on the head by stating that it might be an access to systems issue because --

Cummins:

It is.

Licht:

-- there was a room within which HSDN, or the predecessor to that, and the FBI's whatever the system is now located, sometimes there was some confusion about access to those rooms. But my understanding was that four and a half or five years ago, that was completely resolved, at least for the area that I had oversight for. So that's my historical experience. I do not have all the facts that the IG might have looked at. But that was my personal experience with it. I thought it was resolved. And I don't know that there was ever an issue with it at the time, going forward. So that's what I know.

Cummins:

I don't know. I'm guessing, and I shouldn't guess when I'm being typed, I guess, but I'm guessing that it had to do with the move and a new security officer who wasn't aware that --

Pannoni:

Greg Pannoni again. I understand, suitability requirements may necessitate, as you mentioned, Elaine, all the employees of the Bureau have to undergo an SSBI. So I understand that part. But when it comes to access to information and at what level, one of the things that ISU does, its role was, need to know the clearance, and that's what it's based on. Typically, anyway.

Cummins:

Exactly. That this was access to the space. This had to do with the space. And so it was just -- it was kind of a knotty -- K-N-O-T-T-Y -- it was kind of a sticky problem at first. Russ, I'm sure you were in some of those meetings, or not, we talked about it? I don't know. I remember a lot of meetings where we talked about it a lot. And this was the resolution. And it had to do with space, not information. And it's not a clearance issue, strictly speaking. So I don't know who the Inspectors General spoke with. It's -- there's a lot of

mistakes in what they said. And obviously, somebody was not very happy about it, and that's understandable. But we're working on it. And I know within the FBI -- see, and I want to wait until these guys are finished, and then I'll make sure that we --

Bradley:

Yeah, we're going to give Tip a chance to weigh in on that.

Polk:

Ken Polk from INA Security. And I was part of some of these discussions on the access to the space, and why FBI was requiring a single scope background investigation. And I think it's important to understand that what we're dealing with here is three separate things. One is, FBI has their suitability requirements. Then you have the clearance requirement. The piece that this is addressing, and I think that is problematic and has come up, is each agency has the authority to set their investigative requirements for their system access. So even though the room is at a secret level and you only require a secret clearance, in order to have access -- whether it's physical or proximity access to the system -- there's a single scope background investigation. Now you could have a single

scope background investigation and only be granted a secret clearance, although FBI does the TS, but you could still have that. And you could even have that for an unclassified system, especially if your root -- you know, if you have root access, and you can completely wipe out thousands of dollars, or records, or whatever. So that is based off of the type of investigation. And I think that's where we're coming from on this IG investigation. Unfortunately, we still have a lot of problems where people say reciprocity, and they automatically think clearance. Reciprocity is not only clearance, it's IT system access, and it's suitability reciprocity. So I think -- and it was the IG. So whether they consulted with any security professionals, I don't know.

Bradley:

All right. Thank you for that. Charlie, do you have anything else to say before I turn it over to Tip?

Rogers:

No, just that there was a collaborative meeting with the FBI. And as Elaine said, they believe the existing policy addresses the issue. They just wanted to revisit New York, and then as appropriate, recommunicate the policy.

Bradley:

Tip, do you have a different perspective on this? This is Mark Bradley again.

Wight:

Well, again -- Tip Wight -- I don't believe it's necessarily this specific issue. That may well be just a miscommunication, or whatever. And I think the situation that I've run into recently, we've got the right folks in the room. So it may well just be another simple miscommunication of what we're actually trying to accomplish. But what we have is a lot of our police department leadership with MPD has their TS clearances through FBI. And we're trying to get HSDN access, because there are HSDN terminals at other agencies besides fusion centers. And we're getting told, and I'm not sure where, Nicole's been bleeding over this, I know, reading the email trails, that it requires a perm cert to DHS to validate the clearance. It just seems odd, and we're having a lot of back and forth, trying to get the right people connected to do that, although it's not a visit request, in any sense. So I'm not even sure is where the right -- what we need is DHS to be able to validate the FBI

clearance, and then issue the HSDN request form. Is that all we're trying to do, Nicole?

Nicole:

(inaudible)

Bradley:

Come to the microphone, please.

Nicole:

I wasn't expecting to talk. I think that, at least from my perspective, what a little bit of that issue is, and hopefully we can work through that, is when we do all of our clearance stuff, "we" meaning DHS, we have a pretty small group compared to the FBI, in terms of how we can get that stuff processed. We know who to contact. Everyone for headquarters sits here in D.C., so it's easier to make those connections, as opposed to FBI. You know, they have their different field officers are responsible in those fields. So it's getting information to the field officers, but we have to connect with their headquarters. So it's just the way it travels is a little bit longer. But we are looking to fix your issue, and hopefully in general we can fix the issue for everyone. But I think, in my opinion, that's

where a little bit of that gets muddled. We can call someone easily at DHS, but it's not as easy to contact the FBI folks to get that disseminated into the fields and things like that, from my opinion.

Wight:

So I guess the policy issue that I would look at, and maybe it's a technical issue, but it would seem like there ought to be a central database of clearances somewhere at the federal level, that --

Cummins:

There is. That's what I'm confused about.

Wight:

Right. So it would seem that rather than having a letter on DHS letterhead sent to an FBI office to request a perm cert to validate a clearance, that all -- in order to validate the clearance, all we'd have to do is access the database, validate the clearance and go from there. So I guess that's where I'm lost from a policy perspective.

Rogers:

Charlie Rogers. Perm certs are to use more than for visit replace. They're to enable an agency to validate that someone has a clearance. And I'm not sure the FBI has its clearances. It may have them on JWICS, but may not have it in the central verification system. I'm not sure. But --

Cummins:

Do you know?

Porter:

I don't know for sure -- this is Russ Porter from ODNI. I'm not a security person. I'm a partner engagement person. But if, Charlie, if I understood what you were just saying, you weren't sure if the state and local clearances were in CVS, if they through FBI?

Rogers:

Yeah. If you have an FBI clearance. I'm not sure FBI transmits all of its clearances to CVS.

Porter:

I have been told that that is the case, what you just said.

Rogers:

OK. OK, then.

Bradley:

That they do?

Porter:

That they do not.

Bradley:

Oh, they do not. OK.

Porter:

Which then makes it difficult to see --

Rogers:

So the perm cert then gives us -- the perm cert to DHS then gives us a record that they're -- and can then be put into our database, so we can validate it to our CIO and the other folks that manage their system.

Bradley:

Mark Bradley. Why doesn't the FBI do that? Do we know?

Licht:

Well, Charlie's exactly right. This is Rich Licht. The FBI leverages something called "Scattered Castles," there's JPAS, there's a number of different systems, you know, it's like Beta, VHS, DV-- pick one. A format. They just use a different system, and there should be a unified database from which you can extract information about the clearance level, the frequency of the five-year reinvestigation, or seven or six, or whatever you choose. But agencies have chosen not to do that. So there was an executive order under the Clinton administration that mandated that the standards be the same, the reciprocity be granted. And one of the things I think that was in there -- I have to go back and look -- was that you have a uniform system, a singular system within which you can look, with minimal information available. The alternative to that is the perm cert. You know, it sounds silly, but they leverage what they've got. You know, if the windows close, they'll use the door, or vice versa. And that's what they use right now to perm cert. We have to do it all the time. And it's a real administrative mess. But it's just what we've got. So rather --

Sena:

You know, that is the huge issue. Mike Sena from Northern California, HIDA, and Regional Intelligence Center. Recently, within the last three months, I had an issue with perm cert for -- or actually, just getting the clearance pass from DHS to the folks that work in DEA space in my building. It took three weeks for them to get the door so that it would be open, so that they can walk in their own door. And they'd been working the space for 12 years. So those issues happen all the time. It's very disruptive to the work flow and the way we do business. And I know there's got to be a better way. But these issues have, ever since I've been in government, have continued. I mean, I'm hoping that we can get some direction on that. But without it, without being able to get people in their offices and actually working, they can't get things done.

Bradley:

Russ, can the DNI help us with this? I mean...

Porter:

This is Russ Porter again. It's me. I've got a hole in my pocket. I'm worried about my cash more than my coin. So Mark's question was, can the DNI help with this? So I can't speak to the security part of the apparatus and what they can and can't

do. So just a little bit of additional background on this, as I mentioned, I'm with the partner engagement officer at ODNI. And some of our partners from state and local law enforcement and Homeland Security met not only with the DNI, but with the director of ODNI's National Counterintelligence and Security Center, Bill Evanina, with the director of NCTC, Nick Rasmussen, with, from DHS INA principal deputy under secretary David Grannis, and from the FBI, assistant director Kerry Sleeper, all within the last two days. So all of these clearance issues weave through those conversations, because of the nature of the work that gets done with all of those parts of the federal interagency and the partners.

One of the things we discussed, and one of the things that my office in partner engagement is responsible for doing, is assembling the responses that are to the recommendations that are directed to the DNI on the parts of this joint IG review. That particular recommendation, number 23, dealing with security clearance, in particular reciprocity, I think, is really what the issue is, and on provisioning those clearances, is not directed to the DNI. But I was asked the question, what's the status on this? So I just raised it to say, what is there that's occurring that if we can make sure we're helping the

partners understand what, to me, after eight years in the IC, but having spent all my times in the state and local law enforcement intelligence guy, are still complex to me. And I think they're probably complex to our partners. So just helping ensure people are communicating and on track, just as you said, Mr. Chair, at the beginning, the federal partners, ODNI, FBI, DOJ, DHS and the state and local partners are committed to sharing terrorism-related information in the information sharing environment. And we're just trying to ensure people understand what the status is on these particular issues. So that's why we just ask the question about, is this working for everybody or not? I know that's not an answer about what we can do, but we'll certainly be in touch with our folks at NCSC to help ensure you're getting to the right people on the conversation.

Bradley:

Right. It just disturbs me, the chair, that it's 2017, we've executive orders that are mandating this. And we're having trouble with this. I mean, this seems to be a fairly basic thing we should be able to fix.

Richardson:

I can speak --

Bradley:

Yeah, Ben, you go ahead.

Richardson:

-- for me with the DISS, and don't ask me (inaudible). But to that point, DOD is funding the upgrade to JPAS, which will bring in CVS. So we are combining those. And that's going to be rolled out in late 2017 into 2018. But I don't think there's any intent in there to bringing Scattered Castles or that database into that group. So I turn to ISOO to kind of discussions around that, as a follow-up on that.

Bradley:

Well, maybe we should pick this up, then.

Pannoni:

Yeah, Greg Pannoni. I think we should. At least there ought to be a way, I would say, up to the TS level that that data can go in -- still can go into Scattered Castles. But at least put it into CVS, since that's supposed to be, as we all know, the Intelligence Reform Terrorism Prevention Act of, what, 2004 or something, said there shall be a central verification database.

And like you say, we're all frustrated. It's 13 or so years later. And the problem is, there's a number of organizations that can't connect to Scattered Castles. It would be OK if everybody had the interconnection, but they don't. Some don't. So there's an inability there to see what records are there for people that are getting their clearances by way of the IC in a lot of instances. So we should take that on.

Bradley:

Yeah, Mark Bradley. Well, we'll get involved and see what we can do. You may be getting a meeting request to come back to one of our (inaudible) rooms here. But again, this sounds like a fundamental, off-guard, off-tackle thing that we ought to straighten out. Otherwise, how can we share this information if we can't get access to facilities and everything else? That's crazy.

All right, on that happy note -- you want to say anything else? Tip, you want to amplify anything?

Wight:

No. You had just asked earlier for a follow-up on the JWICS discussions that we had had. And again, I reached out to

Kurt Reuther, who has work-- again, in the context of this, we had originally worked trying to get JWICS access for fusion center personnel who were not detailed to a federal agency. And we're working under that context. Since then, obviously, I've changed positions, although still retaining the clearances and working at MPD's real-time crime center. The piece was an MOU that was being negotiated at the time between D.C.'s Homeland Security, Emergency Management Agency and DHS. Obviously, given the change, that is no longer the appropriate route, we felt, for working this. And Kurt had elevated up through the chain, and they felt that it was going to require something beyond an MOU. So that was -- he's tabled that. He's forwarded it up the DHS chain, and unless anybody has any updates on that, he's just awaiting further guidance at the DHS policy level on how they're going to approach this. So that's the only update I have.

Rogers:

Any application?

Porter:

No, I'm not aware of it.

Rogers:

Who did he go to? The CIO?

Wight:

I don't know what Kurt did. He just told me they had had internal discussions, that probably the MOU route wasn't the right approach.

Rogers:

OK. I'm not familiar with it.

Bradley:

All right. Thank you, Tip. OK. Now we're going to move to what we call the "open mic session." Given what you've heard here today, or what you haven't heard, would anybody like to say anything to the group? Any issues you'd like to bring? Or esteemed guests? Anything you guys would like to raise?

M:

No, just thank you for th

e invitation.

Bradley:

Oh, no, no. Not at all. Anybody on the phone have anything to say? Any comments? Issues you can bring to the table?

Scouten:

Let me make some brief comments. Certainly appreciate the complexity of the issues at the federal level, and the need to get them resolved, particular as it pertains to cyber and information sharing. I trust you're going to do it, I trust it's going to be a heavy burden. But from the state's standpoint, and the local standpoint, the people we work with in our state, we would implore you not to transfer that complexity down to the state level. We need simplicity. We need information flowing easily and quickly. What we perhaps don't need is a lot of -- are a lot of rules that would impede that process.

So right now, we're having trouble getting security clearances for our secret -- not top secret, not SCI -- we're having trouble getting secret clearances for our private sector utility folks. So we've had municipal folks contact us about topics that have been in very recent DHS briefings at the secret level that we're unable to talk about. So again, I'd make the pitch that you need to get those worked out, and they'll get worked

out. You folks are some of the best and brightest in the business. But meanwhile, back in small-town Iowa, we would hope that you would allow the information to flow easily here, so that when an event happens, which probably -- when it does it'll happen at the local area. And we need to deal with it. We'd like to have the information that we need to affect a proper response, or even engage in some protective measures. Thank you.

Bradley:

Mark Bradley. That's hard to argue with. So your points are well-taken. Anyone else?

Rogers:

I can make a general statement, this is Charlie Rogers, about private sector clearances. We can clear subject matter experts who do not represent their company, but represent their infrastructure under EO13549. So there may be companies that we cannot clear or engage with, unless they have a facilities clearance, or unless they get engaged in this hybrid program, the purpose of which is to enable companies to get clearances outside of 1349, without getting a full facilities clearance. So some of the roadblocks to getting private sector

clearances -- and I don't know this particular instance -- may well be that the individual is representing their company. The engagement has to do with the company's structure, the company's network. And now we're no longer clearing them as a private sector subject matter expert, who represents an infrastructure. We're now clearing them as a representative of their company. And they would thus fall under the hybrid, which is under construction.

Scott:

And Charlie, we -- Mark Scott -- again, we talked about this in January. And I thought we had it resolved. I was going to call you, didn't think we needed to. But now we've had three clearances that have been kicked back. And so I will get some more information and give you a recall. But in respect to the hybrid, as I understand the discussion we had earlier this morning, if that deals with Section nine property, that really isn't our issue, although we have, I believe, one Section nine entity in the state. We're dealing with small-town utilities that we expect are going to be the avenue of attack, a way of getting at our large investor-owned utilities that have huge footprints within the state.

Rogers:

Yeah, I think the Section nine companies are the priorities. They're not exclu-- the hybrid's not exclusive for them. But I would need more information to see whether 13549 could be applied to these clearances, or whether it pivots to an industrial security program.

Scott:

Charlie, I'll give you a call. Thank you very much.

Rogers:

OK.

Bradley:

Thank you. Anyone else have anything to say? We've got -- are you sure? We've got 15 minutes left, so -- no?

Pannoni:

We actually adjusted it on the schedule to 11:45.

Bradley:

Right. OK. So actually, we're right on time.

Pannoni:

Yeah.

Bradley:

Well, let me wrap up, then. The next SLTPS-PAC meeting, hopefully, will be held on Wednesday, January 24th, 2018. Again, that's January 24th, 2018, at 10:00 until noon, here at the National Archives. After that, the next one beyond that will be July 25th, a Wednesday, 2018, 10:00 a.m. to noon here at the National Archives. Again, let's pray that both of those are still on rails by the time we get to them. OK? Please mark your calendars for those. Thank everyone for attending. Also on the phone, thank you. And meeting is adjourned.

Friedland:

Thank you, Mark, good job.

END OF AUDIO FILE