INFORMATION SECURITY OVERSIGHT OFFICE
State, Local, Tribal, and Private Sector Policy Advisory Committee
July 24, 2019

Mark A. Bradley: Okay. Mark A. Bradley, Chair of the Policy and Action Committee here, also the director of ISOO. I want to welcome you to our 16th meeting of the committee. This is our first and last 2019 thanks to the government shutdown we suffered in January. So I'm not going to be able to make up everything today, but we will certainly try to push us back on firm footing.

This is a public meeting subject to the Federal Advisory Committee Act and the minutes of the SLTPS-PAC are available to the public. Meeting is being audio recorded. Microphones around the table should give us sufficient fire power to have people be able to speak and to be heard.

One caveat on that, when you do speak, will you please identify yourselves because, again, these minutes are transcribed and it makes it almost impossible to go back and try to figure out who that really was. So again, if I interrupt you and ask you to identify yourself, it's not because I'm being rude. It's because we're trying to get an accurate record of exactly what happened here today.

We've had some membership changes in the SLTPS. And it's one of the interesting things since I've been the chair is the -- I wouldn't say the instability of this body but certainly the change that it goes through. It seems to be continual. It's hard to get a group that actually stays together for very long, which I think hinders our ability to do some of the things that we've got to do.

Anyway, what we're missing now, we have four vacancies. We lost Jeff Friedland who was the director of Saint Claire County Michigan Homeland Security and Emergency Management who is the SLTPS vice chair. He retired. Doug Reynolds left his position with the Mall of AmErika. Mike Steinmetz, Cyber Security Officer and Senior Homeland Security Advisor, State of Rhode Island, left government service for the private sector. Also Hans Olson, Assistant Undersecretary for Homeland Security, Commonwealth of Massachusetts, also left government service for the private sector. So we're down.

Now any member of the SLTPS can submit nomination. I strongly encourage you to do so if you know good candidates who are up on these issues and who would be a plus up for us. We'd be very interested in taking them. I am this selecting official, but again, I am - I don't think I've ever turned down anyone who is qualified. So please, we're looking for diverse members. We're looking for people who want to take these issues to heart.

I also remind the SLTPS members that you need to select a vice chair. Jeff Friedland has gone. That's up to you all. Per the bylaws, it's done by majority vote. We have one person who's put his name forward. Marc Sachs has expressed a willingness to serve and was nominated by (Dori Koren). But the remaining three members have not entered the discussion yet. So again, I can't move until you all move. I'm like a piece on a chess board, all right? So please select a vice chair.

On the federal side, there were changes at the CIA. Brian O'Neill, Director of Information Management Services Group, replaced Nancy Morgan as a CIA member. Riggs Monforte), Chief Information Review and Release Division, Information Management Services -- where do they get these titles -- is now the alternate, the CIA. So it - anyway, you can see what I was talking about. We have - we've had a lot of change, and we're still in a change. And it'd be nice to have this board stabilized a bit.

All right. So we're going to go around the table now and introduce ourselves. As I said, I'm Mark A. Bradley, the chair of the SLTPS-PAC and also the director of ISOO.

Greg Pannoni: I'm also Greg Pannoni. I'm ISOO associate director and the designated federal officer for the meeting.

Marc Sachs: I'm Marc Sachs, CSO at Pattern Computer.

Leo Masciana: Leo Masciana, State Department Representative.

Marvin Mackey: Marvin Mackey, (unintelligible) for the Department of Transportation.

Erik Galow: Erik Galow, FBI (unintelligible).

Pam Miles: Pam Miles with ODNI.

Charlie Rogers: Charlie Rogers, DHS representative.

Mark A. Bradley: Okay. To you all on the telephone, would you please identify yourselves?

Marcia Good: This is Marcia Good from the Department of Justice, Office of Tribal Justice.

Darryl Parsons: Darryl Parsons, Nuclear Regulatory Commission.

Sidonie Dunham: Sidonie Dunham, DOT.

Natasha Wright: Natasha Wright, Department of Energy.

Kelbie Kennedy: This is Kelbie Kennedy from the National Congress of AmErikan Indians.

Tom Woolworth: Good morning. My name is Tom Woolworth. I'm the president of the National Native AmErikan Law Enforcement Association.

Mark A. Bradley: Okay. Anyone else?

Jessica Davenport: Jessica Davenport with the Florida Fusion Center.

Mark A. Bradley: Yes. Anyone else on the telephone? For those of you on the phone, will you please mute your lines when you're not speaking? We had trouble at...

Greg Pannoni: What was it, up in the NISPPAC?

Mark A. Bradley: NISPPAC, yes, when we just had a awful time trying to understand what people were saying.

All right. Anyone else on the telephone? All right. Let's go.

All right. Lastly, as you can see in front of you, you have your blue folders. They have the minutes from the last time and some of the issues.

All right. I'm going to turn it over to Greg now for old business.

Greg Pannoni: Okay. All right.

Mark A. Bradley: (Unintelligible).

Greg Pannoni: Yep.

Mark A. Bradley: Thank you.

Greg Pannoni: Mister - thank you Mr. Chair, and good morning everyone.

So you should have all the handouts and the minutes, and those members or alternates that are on the phone should have received those also electronically.

We only had the one item from our meeting last - which was a year ago. And that one was concerning the issue of clearances - personal security clearances being populated in the Central Verification System which is the recognized database for all clearances. There's also, of course, two other systems, the JPAS -- which Joint Personnel Adjudication System -- which is transferring into the DISS system. I think that's the Defense Investigative Security System that is also under DOD now. As you know, the clearance process in general has transferred over to what is now the DCSA -- the Defense Counter Intelligence and Security Agency -- formerly established by executive order a month or two ago.

And so that's the repository where all SLTPS personnel clearances should be maintained or at least accessible through that portal. So we have the issue that was identified with one agency. There may be a few others, but the FBI in this case that utilizes the third system, the Scattered Castle System, which is for the intelligence community and is limited to those who, A, have an SCI and I believe also require JWICS access to the system. Both of those are not available to the SLTPS members. So we need to come up with a solution to this.

So we discussed this a year ago. There was some follow-on discussion after that meeting, but today we're going to have Erik Galow from the FBI give us further update on that issue, and I'm going to ask that you do that right now.

Erik Galow: Thank you sir. Again this is Erik Galow from the FBI, and I (unintelligible) prepared statement on behalf of the Office of the Chief - Information Officer of the FBI and Security Division as well.

The FBI is awaiting further guidance before making any determinations about the future of its security clearance processes due to the recent announcements of the merger of DSS and NBIB, that being the DCSA, and the Trusted Workforce 2.0 Initiative. Those determinations include prospective planning and budgeting for technical interoperability with systems other than Scattered Castles, and that includes CVS, which is among the issues that we addressed last year for storage of clearance related information for FBI and FBI-sponsored personnel.

At this time the bureau has no plans to change its standard operating procedure regarding the continued exclusive use of Scattered Castles until otherwise directed. It is the system that all FBI personnel and sponsored personnel in which their information is stored and at this time we haven't budgeted for any technical interoperability with CVS, to make a long story short.

Pannoni: Okay. Thank you. Does anyone have any questions for Erik or the committee? Okay. Well -

Mark A. Bradley: So basically we don't have an answer to that then?

Erik Galow: The answer is that the Trusted Workforce Initiative 2.0 is likely going to change the entire manner in which...

Mark A. Bradley: Right.

Erik Galow: ...not just IC personnel but the infusion center -- let's say local tribal private sector personnel's...

Mark A. Bradley: Sure.

Erik Galow: ...clearances are vetted, processed and ultimately stored. So we aren't necessarily in a position to appropriate money and then budget for anything at this point until we've received that topical guidance. And if I recall, there was also an action from last year. There was nobody in (iAttorney). I can't remember what their name was, but they stated that at that time, it was last July 2018 that they hadn't heard of any guidance from ODNI to not declassify but downgrade certain fields that are currently found in Scattered Castles such that clearances could be cleared or passaged down to a lower enclave, and I'm not sure if any headway had been made on that, but I was going to pose that question to ODNI.

Mark A. Bradley: (Unintelligible).

Erik Galow: I'm sorry?

Mark A. Bradley: So you think this committee to it to spur this along a bit (unintelligible)?

Erik Galow: The best recommendation that I could make would be to actively follow and participate in the Trusted Workforce Initiative. There's a Policy Advisory Committee that was stood up...

Mark A. Bradley: Yes.

Erik Galow: ...at the highest levels, from my understanding, the...

Mark A. Bradley: (Unintelligible).

Erik Galow: ...executives and Dexcoms. So I would continue tracking that and we'll be held accountable just as DHS, the CIA...

Mark A. Bradley: Okay.

Erik Galow: ...et cetera, et cetera will be based on the guidance from that committee and (unintelligible).

Man 2: (Unintelligible). Again, you know, we are fully aware of all the transition and all the (unintelligible) causing.

Erik Galow: Yes.

Mark A. Bradley: It would take some time to iron it out, but this is critical that we get this particular solved...

Erik Galow: I agree.

Mark A. Bradley: And the threats are growing. The (unintelligible) - we're on borrowed time for this, it seems to me, and we need to get this fixed.

Erik Galow: Yes. It's a far-reaching issue that doesn't just effect, for example, fusion personnel that...

Mark A. Bradley: Oh, the...

Erik Galow: ...can't access their...

Mark A. Bradley: ...there's actually (unintelligible).

Erik Galow: ...clearances. We have people waiting in the wings for - I don't want to quote a number, but for a very long time for a prospective hiring initiatives.

Mark A. Bradley: Yes.

Erik Galow: And they can't find out, nor can our state local travel private sector personnel.

Leo Masciana: Okay. I believe I...

Mark A. Bradley: Leo, identify yourself.

Leo Masciana: Leo Masciana. I believe I've heard the discussion in the past about establishing a sort of customer service point of contact. DHS has access to both CBS and Scattered Castles as do many other agencies.

Charlie Rogers: We have access, yes.

Leo Masciana: Right. So the feasibility of having a point of contact who can do a customer service check on behalf of the private sector in the states and locals as a - as sort of a patch, an interim mechanical fix until the systems do speak to one another and share a database that's consolidated.

I think the feasibility of that is worth looking into. It requires some dedicated individual or individuals to serve the partnership.

Marc Sachs: Right. (Unintelligible). I'll second that.

Charlie Rogers: Charlie Rogers. I'll make a couple of notes somewhat related to that. Under the executive order, the 13549, we were directed - DHS was directed to work with OPM, DOD, ISOO to find a central verification- or a central database. We got the database identified as CVS. OPM stood up. OPM had - FBI was at the meetings. DOD was at the meetings. They made a pathway for JPAS to reach into CVS.

And everything was accomplished, which is required by the executive order. And those clearances which were higher and secret because fusion centers only house secret, and so they only need to verify for their own meetings at the secret level. From JPAS, those clearances were stripped down to the secret level.

So there wasn't any issue with someone having TS/SCI. All that was resolved. What prevents it from working is people don't put the data into CVS. So I can't speak authoritatively for DHS. I know we don't have bodies to do the work for the other federal agencies to try and stand up a team to sit there and access Scattered Castles on behalf of other agencies who have issued clearances but are not either standing up their own services. So I don't want to say we're not going to cooperate in this matter, but I think cooperation means there are other players in DHS to solve those problems.

So that's my two cents. And I'm not the authoritative person for DHS, and we absolutely wouldn't know it. I know that in - within the Office of Security, it's very difficult to get federal employees approved, you know, and we are resourced with a lot of unfunded mandates. So - but we did do a lot of effort to get this system to work, but it requires people to participate, so...

Greg Pannoni: This is Greg Pannoni. So I agree it's going to take a collective effort. DOD has an important rule now that the investigative process is transferred over to them. And they're going to be overseeing now the bulk of all the clearances. So I think we ought to - I would recommend a small group DOD, DHS, DNI, ISOO come together, take a look at this issue and try to come up with a fix, not just a short term fix but - the data is there. It's just a matter of somehow transferring that data that's in Scattered Castles that is applicable to the SLTPS personnel into the CVS where it's accessible...

Charlie Rogers: Making - make it accessible, yes.

Greg Pannoni: ...by just about everyone. So I think that's the challenge we have and that's what the executive order, as you've said, Charlie, really mandates it. It's not an option for anyone. But it's not just a DHS issue. It's - you're correct.

Charlie Rogers: Right.

Greg Pannoni: It's the other agencies that are issuing personnel security clearances to SLTPS personnel as well who are not utilizing CVS. And so - yes.

Marc Sachs: Marc Sachs. And I'm private sector but former govie, so I know frustrations on both sides. The number one issue in the private sector is an individual who is cleared, knows they're cleared but usually do not know who their SSO is. They don't know who holds their clearance, they don't know when it expires, things that a government employee can fairly easy figure out but a private sector person working at a power company or a power - or a bank or whatever.

And that's where the suggestion of, be it DHS or whomever, have this single point where a private sector person can work with that single point even though somebody else might hold their clearance. But at least to find out is my clearance still valid? Do - who do I need to call to update it, you know, all these basic questions that a government employee generally has easy access to but a cleared private sector person doesn't.

Charlie Rogers: I wouldn't say - yes, I know what the problem is. I wouldn't say DHS has easy access to other agency...

Marc Sachs: Right. And again...

Charlie Rogers: ...clearance (unintelligible).

Marc Sachs: ...you may not, but it's just a...

Charlie Rogers: ...you know.

Marc Sachs: ...single point, whether it's...

Charlie Rogers: Yes.

Marc Sachs: ...DHS or whomever, but just to try and (unintelligible)...

Charlie Rogers: I mean we are available to track down people we clear, and we - but it's - you know, it's typical if someone calls us and says, "Who has my clearance," we don't know if DOE issued that clearance...

Marc Sachs: Exactly.

Charlie Rogers: ...or not.

Marc Sachs: Well, and that's - you see that with...

Charlie Rogers: Yes.

Marc Sachs: ...DOE. They might have...

Charlie Rogers: And if people put it into these...

Marc Sachs: ...emergency meetings, yes.

Charlie Rogers: ...into the universal database it would be possible to verify.

Marc Sachs: It might (unintelligible) work.

Charlie Rogers: But otherwise - and it's some individual making multiple phone calls...

Marc Sachs: Right.

Charlie Rogers: ...and - I'm just - it's a challenge. I'm not saying we can't work to solve it, but it's complicated.

Mark A. Bradley: Well, this is the chair. Is there any reason why these agencies aren't entering this information in the database? Is it willful disregard of the order? Is it lack of resources? Is it not knowing the order? So I mean what are your best guess on this?

Charlie Rogers: Well, I don't - I think the big players is the FBI and DHS.

Mark A. Bradley: Right.

Charlie Rogers: So I don't know. The FBI may have its own reasons or maybe...

Mark A. Bradley: Erik, do you have any reason for us?

Charlie Rogers: I - yes.

Erik Galow: Well, it's (unintelligible) - this Erik Galow from FBI.

Mark A. Bradley: Yes.

Erik Galow: The policy that I translated into my previously read statement is the stated policy of the FBI, and they - we use exclusively Scattered Castles (unintelligible).

Mark A. Bradley: Even though it conflicts with the executive order?

Erik Galow: Even though, in this case, it conflicts with the executive order, although (unintelligible) the FBI's not exclusively called out, so...

Mark A. Bradley: All right. Well...

Charlie Rogers: All right.

Mark A. Bradley: As the chair, this is what we're going to do. We're going to convene a working group. As Greg said, we're going to have ISOO and DNI, DOD and DHS. Anyone else you can think of that that needs to participate in this?

Charlie Rogers: I don't know. We...

Mark A. Bradley: Well, let's start with that group...

Charlie Rogers: Yes, we - yes.

Mark A. Bradley: ...and then we'll branch out as need be.

Charlie Rogers: But another point we -- and we could probably fine tune this -- DHS has stood up a outward facing web site that you can get to from DHS.gov. So I could share that link. And it has a lot of forms. It doesn’t necessarily solve who has your clearance, but it does help to inform people of the clearance process. And it's a work in progress. So more could be done to improve that web site or, you know, to incorporate other ideas. So I can send a link out to (Bob) and...

Mark A. Bradley: Okay.

Charlie Rogers: ...have it disseminated out. It's a public...

Mark A. Bradley: (Unintelligible).

Charlie Rogers: ...you know, site.

Mark A. Bradley: Yes. And so...

Marc Sachs: Or even HSIN.

Charlie Rogers: So we've been trying to...

Marc Sachs: (Unintelligible)...

Charlie Rogers: ...develop fact sheets, you know, but it's really to our customers not for the entire federal government.

Mark A. Bradley: Right.

Charlie Rogers: So - but I'll share that, and then if there are ideas about improving that web site or, you know...

Mark A. Bradley: Right.

Erik Galow: I'd recommend including DOE, Energy (unintelligible) because they issue clearances to the utilities.

Charlie Rogers: Yes. Okay. Yes. We can do that.

Mark A. Bradley: All right. Thank you Erik for that. Appreciate that.

Erik Galow: Yes, sir.

Greg Pannoni: Okay. So we - that's it really for the action items. What we did (unintelligible) right here Mr. Sachs, SLTPS member Sachs, had an item concerning use of (taralines) I think from our last meeting, and then you also put forth a number of other things, as you just mentioned, single point of contact, declassification of time-sensitive cyberinformation, one-day read-ons for private sector officials that don't have a clearance and the ability to maintain access even after separating. We will address those in - during the open forum session of the meeting since this is the old business section.

So other than that are there any questions? Okay. Thank you.

Bradley: All right. Let's turn to the new business, all right? And that will be Charlie Rogers, DHS Vice Chair. We've got an update on the DHS SLTPS Security Program. Charlie?

Charlie Rogers: Yes. I sort of do this at every meeting just to give a little bit of update about the piece that we are very actively working. And so I'll talk a little bit about, you know, the executive order tells us that we have to recertify rooms for state and local. We do compliance reviews, and the Compliance Review Program we really stood up in 2012. I always give these metrics. By the end of this year we will have done 108 compliance reviews since 2012 or the end of 2012.

There are about approximately 80 recognized fusion centers, some of which are accessing classified from an FBI secure space, but the great majority are DHS certified secure rooms. And so we - that's where we do the compliance reviews. We go out and, you know, verify that the rooms are still secure, that people are following the federal and national policies for safeguarding classified, provide training, et cetera.

So last year we did 16 of these compliance reviews at fusion centers. We did an additional seven room certifications because, you know, centers move. They change, go to a new building, a larger building. They want a bigger room, so we've certified seven rooms last year. This year we're on track to do 19 security compliance reviews by the end of the year, and we're probably going to do a half a dozen room certifications for the same reasons. People are relocating to other buildings or need to expand the room.

Related to the security compliance reviews, we have appointed security liaisons at every fusion center. It's a requirement. And we are responsible to train these folks as best we can. There's a fair amount of turnover because some of them are - other duties is assigned or they might be temporary law enforcement people who move into the fusion center.

But the security liaisons are basically our security officers out in the field. So we're constantly working with them on the telephone and we conduct webinars with them. In '18 we did 21 webinars and directly trained about 48 security liaisons. This year - well, also in '18 we did a trial concept of a regional training so we brought - we went to Tennessee and - Nashville, Tennessee and we had ten state liaisons come in - well, representing ten states. Seventeen different liaisons came in and they got training for a couple of days as a regional. We hope to duplicate it depending on funding and opportunities, but that's another way in which we try to train the liaisons.

Thus far in '19 we've conducted 12 webinars with a total of 48 participants, and next week in Columbus, Ohio, the DHS Office of Intelligence and Analysis (I&A) is sponsoring a security liaison training venue for two days in Columbus, Ohio, and we've got a team of our folks going out there, and the I&A folks are going out there. So they're - so that's another opportunity to do a training for them. So that's a complete challenge because the compliance reviews help us understand what's going on at the fusion center, but the liaisons are really the workforce that ensures that security is adhered to at the locations.

And then the final little metric I give is our current numbers -- and these are approximate -- that we have approximately 2100 cleared private sector people nationwide. We have 6150 state local personnel. And that comes to about 8250, more or less. The numbers change a little bit. Total clearances, most of them are the collateral level, at the secret level.

We do have 450 out of that 8000 number who have TS/SCI. And a lot of those folks - well, some of those folks through the state and local who are working with the FBI on JTTFs and other task forces. But a good number of these folks are private sector who are involved in cybersecurity and need that level of access to get the information they need.

So that's just a snapshot of what's going on.

Greg Pannoni: Greg Pannoni, ISOO. This question not only for DHS but for other US government members that may or may not be doing this. But are there other - any entities besides the fusion centers where a state local or tribal has been authorized the physical custody of classified information, of course only up to the secret level?

Charlie Rogers: A limited number. We work with our Intelligence and Analysis Office to sponsor the capability. The Office of Security doesn't determine who needs it. So we have some states that have a robust outstation. So Florida, for example, might have some regional state police offices that have secure communications and thus they have a - we require they have a security container because if you've got a secure communications you might make classified notes.

But there's not a great deal of storage at these locations. It's primarily secured coms from the state fusion center out to manage an emergency and to - if necessary to share classified. But no, there's not a large number. But there are some police departments, some state police officers that have that storage, you know. So...

Greg Pannoni: Have any of the other federal government agencies, do any of you have locations where there's physical custody up to the secret level?

Erik Galow: This is Erik Galow from the FBI. I'll have to go back to the office and look into that a little bit. I can't answer off hand.

Greg Pannoni: Okay.

Charlie Rogers: Yes. I don't think they do because under the executive order we're supposed to approve storage.

Erik Galow: A certificate's supposed to be executed.

Charlie Rogers: Yes. There's no negotiating.

Erik Galow: (Unintelligible) government person regularly on site.

Charlie Rogers: Yes. But the FBI has a lot of locations where they invite state and locals in, but that's different than...

Erik Galow: That's the...

Charlie Rogers: ...the state and local having custody.

Greg Pannoni: Right.

Charlie Rogers: It's - they're co-located or they're one floor up in a building and...

Marc Sachs: What about the Guard, National Guard?

Charlie Rogers: Well, the National Guard could independently do it too. But I don't - I'm not if we were aware we would have engaged because they're under the order they're supposed to engage with us if there's storage.

Mark A. Bradley: Okay. And...

Charlie Rogers: And we're supposed to manage a national database...

Mark A. Bradley: Right.

Charlie Rogers: ...of those locations.

Greg Pannoni: But part of why I'm bringing this up is the other point is to use it as a force multiplier, if in fact there are some of these places beyond fusion centers where the state and local tribal community -- and not in this private sector -- could perhaps gain access to information that would be in closer proximity to where they may be located.

Charlie Rogers: Yes.

Marc Sachs: Yes. This is Marc Sachs. Typically we use the FBI field offices.

(Leo Masciana): Yes. The FBI's very open to it.

Marc Sachs: Those are easy to get to and...

Charlie Rogers: I know the secret service is - whatever their mission requirements are but have opened up their secure space to state and local, especially when you have these national security events like the - you know, the Super Bowl and those kind of things that they open it up. I know there's an ICE facility in Florida that actually is a fusion center. It's - you know, the fusion center is in an ICE facility which is unusual.

And certainly there's FBI places that are the - they're the primary classified holder that we don't even certify a room at that location. You know, at - in New York, I think, in Albany the FBI has a facility. And so we're not involved because - but the states don't have custody of the doc - you know, they're within a FBI certified space, so...

Mark A. Bradley: Thank you. Anyone else have any questions for Charlie? Anyone on the phone for Charlie? All right. Thank you Charlie. Appreciate it.

All right. Now we're going to turn to Leo Masciana from the State Department, who will give us an interesting, I guess, view or strong opinion on examining classification of cyber drug information could be a better test to our nonfederal partners.

(Leo), please.

Leo Masciana: Sorry, this works from here?

Mark A. Bradley: One hopes.

Leo Masciana: Okay. Before I begin, would like to thank Marc Sachs and Kate Connor for your suggestions, thoughtful suggestions. I'd like to thank the chair and the advisory committee staff for giving me the opportunity to extend the discussions that we have already started in January and July in this committee last year.

On the subject of classification as an impediment to sharing cyberthreat information with critical infrastructure partners and a with classification reform. Next. These high level authorities provide the basis for much of our national security information doctrine today. Beginning with 13549, as you know, that's the order that established this advisory committee with the primary purpose of ensuring protection of classified information entrusted to US entities.

The Policy Advisory Committee has two other responsibilities -- addressing and resolving program related policy issues in dispute and recommending changes to policies and priorities that are designed to remove impediments to sharing classified information under the program. Executive Order 13587, generally known as the insider threat order, has also a set of contrasting missions.

Setting aside the order's primary focus on hunting down moles and leakers, 13587 also directs federal agencies to share classified information immediately with authorized users around the world, extending its scope to foreign governments and including an element of urgency that's important to note that.

The National Security Strategy issued in December 2017 directs the US Government to work with critical infrastructure partners to assess their information needs and to reduce barriers to sharing. It specifically sites classification levels and speed and of dissemination as barriers. Next.

To provide a historical perspective, these devastating attacks on AmErika have come to define much of our national security priorities today. The Pearl Harbor attack is attributed to a failure in communications to warn the base of imminent attack by the Japanese. The alert was received after the attack had concluded. The Oklahoma City bombing at the Murrah Federal Building occurred as mutual mistrust by FBI and ATF contributed to a critical lapse information sharing between the agencies. Both were aware something was going to happen, but neither had all the pieces.

On September 11, 2001, the devastating attacks on AmErika were largely attributed by the 9-11 Commission to be a failure of US intelligence to connect the dots. All these national tragedies may have been prevented had we done a better job of communications and information sharing.

Official reactions that followed the Oklahoma City bombing and the terrorist attacks on 9-11 comprised the following three broad shifts. The first shift relates to defense of cyberspace -- exploitation, theft, disruption through public - private partnerships and resulted in a large body of executive directives to - in the interest of cybersecurity. PDD 63 is entitled Critical Infrastructure Protection and issued the Critical infrastructure Assurance Office, the National Infrastructure Protection Center, the (Fed's) Computer Incident Response Capability and the Information Sharing and Advisory Council.

Executive Order 12333 entitled US Intelligence Activities notes the critical partnership with private sector and state and local governments and calls for sharing both information and intelligence information with our infrastructure partners. I've touched on EO 549, 587 and the National Security Strategy. The Comprehensive National Cyber Initiative has its mandate to create shared situational awareness and the ability to respond quickly to prevent intrusions within the federal government with other government entities in the private sector. DOD JTF-CNO is a joint task force computer network operations at Stratcom, which back in 1998 integrated computer network defense and computer network attack capabilities into the operations of the US military forces.

Moving on to the terrorism shift, which is a smaller span of time, but important in that has created and promoted an unprecedented information sharing with critical infrastructure partners, I cite three pieces of key legislation -- the US Patriot Act, the Homeland Security Act and the Intelligence Form of Terrorism Act, especially Section 1016 on information sharing.

As far as directives go, HSPD 5 and 7 -- 5 is one of my personal favorites because of its focus on preventing, preempting and deterring -- in other words, what emergency preparedness people and bomb experts call left of boom. After the bomb goes off, it's a bit late. It's a cleanup effect. So to get in front of it is the priority of these HSPDs.

Executive Order 13388 called for sharing Homeland Security information relevant to terrorist threats and vulnerabilities in the National CIKR, Critical Infrastructure Key Resources, with federal agencies and SLTPS in a timely manner. I added 13526 on Classified National Security Information for its contribution in eliminating the third agency rule.

Okay. Oh, one last item. In the third shift I added cyberwarfare as we're now entering into - I think we're - it's being acknowledged, a persistent state of nation states aggressively using the Internet as a weapons platform to launch tremendously destructive cyberattacks. I've added that because of the pressure it puts on the first shift, which is cyber defense, to make sure that we are collaborating in a full partnership on cyber threats with the private sector. Go ahead.

Okay. Based on this rather large body of statutory and policy authority and direction, I think it's reasonable to ask do US government agencies' classification guidance and practices help or hinder cooperation with SLTPS partners to defend the nation's critical infrastructure from cyber threats? What we know -- we know that the National Security Council's priorities have shifted clearly to embrace collaboration with non-USC partners to unify the nation's efforts in overcoming emerging cyberthreats.

The National Security Strategy in 2017 emphasized the emergence of a great power competition and noted its spread into cyberspace. The National Cybersecurity Strategy in 2018 asserted that the US Government will strengthen efforts to share information with information and communication technology providers to respond to and remediate malicious cyber activity at the network level to include sharing classified threat and vulnerability information. Next.

The private sector owns and operates about 85% of the critical, physical and economic infrastructure of the United States. We know that industry cannot defend itself against cyberattacks by nation states without US Government assistance. Likewise, the government cannot protect the nation without private sector assistance.

We also know that cyberattacks are very different than traditional national security threats. The director of NSA and head of Cyber Com General Nakasone calls them corrosive threats by malicious actors who weaponize personal information, steal intellectual property and mount influence campaigns. His assessment as of February this year in testimony before the

Senate Armed Services Committee is that globally the scope and pace of malicious cyberactivity continues to rise and the growing dependence on cyberspace for nearly every essential civilian and military function makes this an urgent and unacceptable risk to the nation.

My research finding based on transcripts of Senate Armed Services Committee testimony, both General Nakasone's and 2010 and 2016 testimony by the first director of Cyber Com Keith Alexander and an OMB memorandum issued in October is that government efforts to share classified cyberthreat information with critical infrastructure partners are being hindered by the classification process. This is because cyberthreat tactics, techniques and procedures are frequently classified at the top secret level.

By comparison, SLTPS partners access both systems and their clearances are limited to the secret level. This results in a misalignment between fusion center staffers who hold secret clearances have classified system access, a need to know, and are nevertheless unable to receive or share timely cyberthreat information because it is classified top secret. Consequently, federal cooperation with our infrastructure partners largely takes place through sensitive but unclassified information exchanges.

The issues and concerns I have highlighted are four -- whether there is over-classification of cyberthreat information, applying blanket classification as a default practice without a determination that each classification decision meets the standards for classification contributing to the Executive Order 13526. Second, whether adequate oversight and accountability is in place to ensure balance, well considered classification decisions with respect to cyberthreat information. Third, whether cyberthreat classification guides exist at all. If they do, are they consistent and contain subject matter relevance and specificity. Fourth, whether the relevant cyberthreat agencies should continue to issue individual guides or enter into a joint classification guide.

My recommendations for the Advisory Committee are to continue resolving procedural gaps that hinder reciprocity access to secret information by secret clearance holders assigned to state and local fusion centers. Those efforts, however, do not improve sharing of cyberthreats classified top secret when our SLTPS partners clearances accesses are limited to the secret level.

Consistent with the committee's responsibility to remove undo impediments to the sharing of classified information under the program, the committee should take a fresh look at the executive order's provisions on classification guidance. Such a review should take a multifaceted approach to reforming classification in the executive order with the objective improving the federal partnership.

I break down my recommendations to two broad initiatives to establish effective oversight of - to ensure classification training requires a risk balancing approach to classification decisions. And the second initiative is to amend Executive Order 13526 to include minimum standards and new requirements for ISOO review of classification guides.

Specific actions would be to require ISOO approval of classification guides to require previsions in the guides for expediting dissemination and prompt releases of threat information to US entities to seek a statutory FOIA exemption for classification - for cyberthreat information to require drafters of threat based guides to seek input from infrastructure partners and to authorize ISOO importantly to establish a working group to get started on these proposals.

In conclusion, much has been accomplished and much remains to be done. The most important thing the government can do is to enter into a full cooperative partnership with the private sector at every level -- technology, policy, governance and operations -- in order to provide critical protection to the nation.

Encountering cyberthreats, the Critical Infrastructure Partnership must be a two-way effort. It must be able to anticipate and prevent, or at least minimize threats. If collaboration is to be effective, US classification policies and practices must be sufficiently flexible and balanced to address the emerging threats of our time.

The NSC's evolving vision and strategic direction have converged on the right path forward. Cooperation to counter serious threats to US interests must be made predictive rather than reactive if we are to harden the nation's networks. This is a logical and reasonable national security objective, but it will require a much more dynamic collaboration with our critical infrastructure partners. An important step in getting there is for ISOO to pursue classification reform as a mission priority.

As I conclude this, I would ask the committee at the appropriate time to take action in recommending a formal path forward to classification reform to include both better enforcement of the existing rules and amending the executive order to fill the gaps that are needed.

Mark A. Bradley: Anyone have any questions for Leo? I mean it was a lot to chew on there.

Leo Masciana: Well, this is on the record now.

Mark A. Bradley: Yes. We're on the record. Yes. Question? Reactions?

Marc Sachs: Marc Sachs, private sector. I think the big takeaway for most of us is that mismatch between top secret and secret, where threat intelligence, people who are actually, you know, working these cases are very comfortable creating TS/SCI, you know, internal consumption stuff, but with the timely nature of cyberspace, higher incidence and a half-life of 24 hours or less, the normal downgrading process that could take weeks or months or years doesn't work in cyberspace.

And that's a key area we have to figure out is how do you quickly get actionable information, not necessarily sources and methods but actual information in a very timely -- as in minutes or hours -- down to asset operators in the private sector so they can do something about it and not read about it later after a breech happens or after there's a congressional hearing or something and - only to find out the government knew what was going on but couldn't tell anybody because of the classification rules.

Mark A. Bradley: This is the chair. (Leo), is it your opinion -- formed opinion, that is -- that information is being overclassified or is it...

(Leo Masciana): That's one of the concerns for oversight that I would like to see direct oversight focused on that. It's very possible. As you know, the executive order we have that was originally issued by Jimmy Carter in '78 is based on Cold War mindset. And very little has changed. The elimination of third agency rule is a good step forward, but it does not ensure that each classification decision weighs the need to share that information with the private sector and yet you have the head of Cyber Com, you have the National Security Council and all these high-level directors say...

Mark A. Bradley: Yes.

(Leo Masciana): ...it must be done in the national interest to save our infrastructure and yet it's not happening. So I think ISOO's role in oversight, I would like to see that fast tracked to this particular area and those key agencies that are classifying information.

Greg Pannoni: This is Greg Pannoni, ISOO. Thank you (Leo) for that comprehensive overview of where you see the ability for us to combat the threat collectively in the cyberspace.

There may be, in one facet, a sort of middle ground area for improvement -- and I'm referring to what NGA did with their - it's referred to as the Consolidated Classification Guide -- wherein they require enhanced statements that go with every classification guide that they prepare. So there's a value statement, what's the value, there's a damage statement.

And the one that I think is particularly germane to this discussion is an unclassified statement, the ability to express the classified information in an unclassified manner or at least that's what they say, but if we could even say at the secret level, if that became something that was part of the process of all classification guides, I think that would be a helpful step in terms of the ability to share.

Marc Sachs: Marc Sachs, private sector. Could I suggest perhaps the actionable level -- if it can be actioned at the TS level, fine, actioned at the secret level, fine, but if it requires unclassified downgrading to take action, so be it.

Mark A. Bradley: Action.

Marc Sachs: Actionable level is in order.

Mark A. Bradley: (Unintelligible).

Leo Masciana: I do think the recommendation about joint classification guide's a very positive step forward, doesn't point at anyone. I had worked on the Counter-IED Government Wide Classification Guide and others and there is an example where for a foreign government collaboration we actually have an introduction section on international cooperation and put in there what is required for release of the information including markings to share the information with foreign governments.

I think models like that exist and could be done for US entity rapid cooperation on classified information as well. So the guide I think is one that really positive immediate step forward, it - not that they have to have that, but the discussions are constructed, and those key agencies - it would be revealing as to how they're classifying the information if they enter into that discussion, maybe reform what they're doing.

Marc Sachs: One last comment. Marc Sachs, private sector. The - over the last couple of decades the private sector working with the government has a information handling regime has emerged called Traffic Light Protocol, or TLP. And there's probably a lot of wisdom in that because it's - it works well between the bureau, homeland, private sector and others. It's for unclassified information but it sets out a way to - how to handle it based on the sensitivity of unclassified information.

And because it's so well known, it's internationally adopted. That language, the understanding that's inside of TLP might also apply here about how to handle the information once it's been properly classified. And this is for mostly cyber, but also applies genErikally to any critical infrastructure information.

Mark A. Bradley: Yes. This is the chair. There is a process under way now being led by John Fitzpatrick, my predecessor, at the NSC to reform 13526.

It's, again, I mean (Leo), you're right. What we have is we have a Cold War regime in place. The problem is that the government's process for doing this is glacial. And the threats are not. And so at some point we've got to come up with a whole better way to do this. I mean we are looking at - especially looking at the definitions of top secret, secret and confidential. Will they even make sense anymore or whether we can consolidate them or streamline them or what's the difference between exceptionally grave and grave. And I mean this stuff you could - how many angels dance on the head of a pin.

But it is time. It is time to start thinking in a new way. And (Leo) you're absolutely right. I don't know whether it - I mean just nimbly whether it means giving more top secret clearances to the private sector, whether it means reforming these guides. Whatever it is, we need to do it before we get hit again. And so we will take this back to the NSC.

Leo Masciana: I would like to see the committee actually formalize recommendations for you to take back...

Mark A. Bradley: Yes.

Leo Masciana: ...either similar to or the ones I've come up with or convene to draft new ones.

Mark A. Bradley: Yes. No, I think you're right. I mean one of the things I was going to say is at the end of the meeting but I'll say it now is I'd like to see this committee become more of a committee instead of a debating society where we actually solve problems and actually do things. We're under pressure all the time, and it's coming from OMB, you know, to cut the (unintelligible) committees, and we always have to justify this one. And it gets harder and harder, A, when you're meeting once a year and, two, when you come back and the issues are the same. And it's like, well, what are you doing? And the answer is, we're talking about it. Well, that's not good enough.

Leo Masciana: (Unintelligible).

Mark A. Bradley: So we're going to have to actually decide among ourselves whether we want this committee to be real. I think the issues are serious enough. I think the threats are dire enough. I think the minds around this table are good enough that we should be able to come up with some solutions to some of these problems. But it's going to be a collective effort. And so I think you're absolutely right. We need to start memorializing some of this and pushing it forward. So anyway...

Charlie Rogers: This is Charlie Rogers. I'd like to add just another element that has been on my mind. So we've got the clearance levels with private sector, but EO 13549 primarily identifies subject matter experts and the relationship is with the individual, although there's some gray area there, and then you have the National Industrial Security Program that deals with classified relationships between the government and the corporate entity, and then you have the hybrid program, but that's a very time consuming process to get a company approved in that interim.

So I think National Industrial Security Policy should be looked as far as how do we facilitate threat information sharing without undermining the NISP but recognizing that maybe the full authority of the NISP can't come into play, even whether it's the hybrid which is a partial NISP, because - you know, and because people are bending 13549 to say, "Well, I need to have this relationship with this company because I need to share this data with this company so that this company can engage with their networks." And you go, "Well, wait a second. That's not exactly a 13549 relationship. That's...

Mark A. Bradley: Right. Yes.

Charlie Rogers: ...more of a NISP, you know." So I do think added to all this is how do we talk about the National Industry Security Program requirements that could be modified without undermining the intent of the NISP...

Mark A. Bradley: (Unintelligible) that's right.

Charlie Rogers: ...but with still facilitating...

Mark A. Bradley: Yes.

Charlie Rogers: ...classified information sharing because the hybrid's not as quick process either. You don't call up and say, "I need threat information. I'll go on the hybrid program and..."

Mark A. Bradley: It's not. And...

Charlie Rogers: Yes.

Mark A. Bradley: ...you know, the NISP is a great thing, but it's not a Gumby. It can't...

Charlie Rogers: Yes.

Mark A. Bradley: ...be twisted in 20 different...

Charlie Rogers: So...

Mark A. Bradley: ...20 different kinds of ways.

Charlie Rogers: ...I just think all of this is good, but I think, you know, unless we actually articulate that under certain circumstances this kind of information can be shared without undermining or without compromising the NISP -- whatever that right language is, I don't know. But...

Mark A. Bradley: Yes.

Charlie Rogers: ...so...

Mark A. Bradley: It's very complex. But anyway, it's worth it. It is.

Greg Pannoni: I mean - Greg Pannoni, ISOO. The one concern, of course, with the sharing of threat data and not making an informed decision at all is the entity could, in an extreme case, be ultimately (unintelligible) and controlled by one of our...

Mark A. Bradley: Right.

Greg Pannoni: ...adversaries, you know. And that would not be beneficial...

Leo Masciana: Because that's the whole problem with all of this.

Mark A. Bradley: That's exactly right.

Greg Pannoni: ...so with clearances...

Charlie Rogers: (Unintelligible) minimal level (unintelligible).

Greg Pannoni: ...emergency one-day read-ins and...

Charlie Rogers: Right.

Greg Pannoni: ...a similar problem.

(Leo Masciana: Well, we do have, and that's something that is also - and I think, (Marc), you brought it up as - for points the...

Greg Pannoni: Emergency...

Leo Masciana: ...emergent risk. There are...

Greg Pannoni: ...there (unintelligible)...

Leo Masciana: ...built in...

Mark A. Bradley: Yes.

Leo Masciana: ...already mechanisms for emergency sharing. I don't know how much we've taken advantage of that, but there is a mechanism for that to take place...

Mark A. Bradley: Yes, right.

Leo Masciana:...under the Classified National Security Program, so - but...

Mark A. Bradley: All right.

Leo Masciana: ...I agree with most of what's been said here. We definitely have a Cold War system that needs to be revamped.

Mark A. Bradley: Okay. All right. Anybody else have any reactions or questions for Leo before we turn to DHS and it's Insider Threat Program?

Marc Sachs: Will a decision be made as to what to do next...

Mark A. Bradley: Well...

Marc Sachs: ...to your point of we shouldn't just admire the problem...

Mark A. Bradley: Yes. No, no, no...

Marc Sachs: ...and actually do something.

Greg Pannoni: Can I recommend, Mr. Chair, to follow up on Leo's suggestion is that why doesn't this committee collectively come up with, you know, perhaps using Leo's as the starting point with however many, five or ten recommendations that you think are the most significant and important that could then be brought by the committee to the chair and then the chair could take them to the NSC as far as revolving around a amending of policies in particular, because if it's an implementation thing, we can work that. But if it's a policy thing, then we've got to go to the next level.

Leo Masciana: So (Leo) here. I think that because of the frequency of these meetings, if the staff could prepare a strawman paper of recommendations and then circulate that for comment and revision by the members we might be able to have something in place prior to the next scheduled meeting.

Mark A. Bradley: The next meeting's in January, so...

Leo Masciana: Or well before.

Mark A. Bradley: Well before, yes.

Greg Pannoni: So Greg Pannoni again. We could, you know, do something like that. We'll work with you offline but then I would, again, recommend - this would be another small working group, ad hoc group that would come together to focus solely on that and then we would...

Mark A. Bradley: Okay.

Greg Pannoni: ...once we've developed a consensus, set of recommendations, hand those off to the chair. So that would be my suggestion.

Mark A. Bradley: Right. No, I think that's right. (Leo, I'm going to point you to this group. Mr. Sachs...

Marc Sachs: (Unintelligible).

Mark A. Bradley: ...you're on it too...

Marc Sachs: Okay.

Mark A. Bradley: ...and anyone else who wishes to join. This is an important initiative, and again, it would - as I said, we need to start actually getting some concrete things for it. So let's go ahead and do this, all right?

Okay. Shall we turn to DHS now and Insider Threat Program?

Greg Pannoni: Yes.

Mark A. Bradley: And I'll let you all identify yourselves as you come up to the mikes.

Greg Pannoni: Okay. (Peter)...

Mark A. Bradley: ...or up here to the (unintelligible).

Megan Davey: Good morning. Thank you all for having me today. Thank you Charlie for asking us to speak. Before we get started, I just wanted to introduce myself. I am Megan Davey. I'm with the Insider Threat Program at DHS Headquarters. I have recently taken on the role as the branch chief for strategic planning and policy. And a common theme that I am seeing from you all and that I will have in my presentation today is collaboration.

So part of my new roles and responsibilities are to work on developing strategic plans way forward for us, initiatives communicating with the our internal and external stakeholders. So today I'm going to give a little bit of a history overview, then talk about stakeholder consensus and collaboration and then strategic plans, way forward for us. Initiatives, communicating with our internal and external stakeholders. So today I'm going to give a little bit of a history overview and then talk about stakeholder consensus and collaboration and then discuss our core mission areas and our critical assets.

So the insider threat program was developed based off of Executive Order 13587 that I've heard a few of you reference today already. So this was issued October 2011 and this mandated all federal agencies to develop an insider threat program. Based off of this executive order the National Insider

Threat Taskforce, the NITTF was established and this group is responsible for the oversight and development for government standards.

This NITTF then took on the next step and developed minimum standards in November of 2012 that was pushed out for all of these insider threat program to abide by. They've actually taken it one step further - November 2018 they have issued ITP maturity framework. So this is going beyond the minimum standards and talking about how to continue the program to go beyond the basic minimum standards they developed and have a more comprehensive proactive approach. To note DHS insider threat program does have FOC, that full operating capability there. So this is in regards to our system so we are doing user activity monitoring. And this would apply for any SLTPS that has DHS classified networks. Next slide. Thank you.

So just taking it back to the basics - we have to first define our mission at DHS. So verbatim here, we have our program deters, detects, identifies and mitigates insider threats to DHS to protect the department's mission, resources, personnel, facilities, information, equipment, networks and systems. So what's important to note by this definition is that it's beyond the executive order that was issued; beyond the protection of just classified. It's looking at that - those critical assets that we have. So that is one thing that's definitely unique to DHS.

Mark A. Bradley: Does that include unclassified information too?

Megan Davey: Yes. So all of our information. Okay. So we have to look at the actual definition of an insider so this was a task considering DHS has multiple components, whether they're operational or subcomponents. We have to identify what that means to us so anyone who uses authorized access wittingly or unwittingly, to do harm to all of those critical assets that I mentioned before. And this is a person who has or had authorized access to our facilities, information, equipment, networks and systems. An insider is someone who is motivated by money, ideology, compromise, ego, etc. So this is something that's unique. For example, with our partners TSA, their insider is beyond that government employee. It's anyone who has badges that accesses their airport. So a much bigger scope beyond the basic there.

The (SIDA) - there are a lot of acronyms up there that I'm sure some of you know. This puts the big picture together that we have a lot of players involved at the department. So we have this umbrella organization where we have eight operational components and seven support components. So this makes us very unique but also presents challenges when developing all of our standards. So a way we do this, much like this group here today, we run an insider threat working group meeting that encompasses all of these players listed. So yes. Please yes.

Charlie Rogers: So we also have a diversity of networks. So we're not like some agencies that have single networks. These components represent I don't know if they all have individual but a lot of them have individual networks.

Megan Davey: Yes. So we currently have the UAM on the classified networks and some of these components have unique classified networks outside of our traditional secret level and TS/SCI level. Yes. So it's making sure we're getting that technology piece in play and working with our (unintelligible) and CIO to identify those networks to make sure we have that coverage.

Greg Pannoni: Okay. And just to reiterate what the Chair said, Greg Pannoni, this extends beyond the classified networks. Correct?

Megan Davey: Well currently we are on the classified networks.

Greg Pannoni: Okay. Okay.

Megan Davey: So it's beyond the protection of classified information. So we…

Greg Pannoni: But the networks right now are at the classified…

Megan Davey: Yes. At the classified level.

Greg Pannoni: Okay.

Megan Davey: Yes. So…

Mark A. Bradley: Yes. That's important to the program.

Megan Davey: Yes. So that brings a bigger point that with this working group we address those types of questions and getting everyone to speak up and say what they need protected at their individual component. So this working group - we meet biweekly; we also form sub working groups like you guys do here as well. We have representation at the level of a senior insider threat official and an insider threat program manager that sit at the table every two weeks. And we utilize them to be our eyes and ears at the components and to let us know what's going on; how we can service them.

The insider threat director and I are currently doing what I'm calling a roadshow and visiting all of our components to see how we can better work together in the future and what they need from us to be more successful. So lots of liaisoning, coordination and working to standardize our strategic framework across the department. Next slide please.

So we have to build that consensus across the department and know who we are billing this consensus for. So we have to look at the strategic, oversight programmatic, operational and technical. So with strategic it's those overarching authorities that we have to get buy in from. Oversight - we actually have an insider threat oversight group that we work with; programmatic - working with data owners as well as the components and subcomponents as well as internal offices at DHS such as our human capital office, CI, our information security and just the security office as well. Operational - working with our partners, so the state and local group for example. And technical - making sure we have the right players involved to get the best engineering solution. Next slide.

So once we identify who we need to work with we need to find out what they're going to be able to do and how they'll be able to best service. So strategic - they're going to provide resources and give us that buy in that we need and their support. Oversight - making sure we're in compliance and have that check and balance in place. So we work with civil rights, civil liberties and privacy option and our OGC. Programmatic - making sure our program is running efficiently and consistently across the department. Operational - coordination across the department and making sure we work with everyone who is a stakeholder, so they can help us define what bad looks like; that everybody has a different insider that they're looking at. And technical - making sure we have requirements and everyone has a clear understanding of what those requirements are. Next slide. Thank you.

So the core mission areas - this is another unique thing for the department. As I mentioned before this is - we're on the classified network but looking beyond just the protection of classified. So our seven areas here are workplace violence, espionage, terrorism, sabotage, unauthorized disclosure, investigative support and transnational criminal organizations. So it's beyond that executive order mandate for the protection of classified.

And we want to also ensure - my boss sees this as an example. We're not just trying to be the time card police out there. So we're looking at that bigger picture and what is the significant threat from the insider. So once we define that core mission area we have to look at identifying our critical assets. I listed all of these before. So making sure we know what we want to protect. So we work with the components and the various stakeholders and their subject matter experts, to identify their mission critical assets and needs. And we have to prioritize them as well. Next slide.

So a very short briefing but I think the big takeaways with this is to know that each agency is unique with their insider threat programs and DHS specifically has that big umbrella set up to where we have to do constant collaboration, communication information sharing. So when we need information to better detect the term mitigate, identifying those core mission areas which you saw these seven are definitely outside of that basic scope. And then work to identify critical assets. So it's important that we're bringing the right players to the table constantly so we can ensure that our ITP at DHS is properly protecting our agency's needs.

And that's all I have for you. I figured there'd be more questions so I wanted to keep it short.

Charles Rogers: (Unintelligible) classified networks now but the plan is to move into unclassified networks.

Megan Davey: Yes. There is a plan for the strategic framework to move forward with that. but for right now we're at full operating capability on the classified.

Greg Pannoni: And Greg Pannoni - and just again to follow up on that point. So when it comes to the external supporters operationally speaking, is DHS at the point where you're formalizing these requirements in contracts? Where classified is not involved but controlled unclassified is. In other words, writing into the contract requirement for an insider threat program for these external sources or we're not quite yet there?

Megan Davey: So we're not there yet. It's not a requirement on our end. it would be a requirement of their agency but it's a mandate that if they have a classified network that we are the coverage for that. But if they have an insider threat program we could work with them. Chris do you have any - I'm sorry. My co-worker Chris Dzurilla is here today. He's in charge of our operations. So he's here for questions as well for all the things I may not know all the details on. Is that - was I correct in saying that?

Mark A. Bradley: Chris why don't you…

Megan Davey: Come on over.

Mark A. Bradley: Come over.

Chris Dzurilla: Yes. I'm Chris Dzurilla with operations, Branch Chief for the Insider Threat Program. I believe there are industrial security standards for cleared contractors being mandated to have their own insider threat detection capabilities locally.

Greg Pannoni: Yes. That's correct. But I'm referring to the - I understood early in this briefing that DHS has taken the insider threat program beyond just classified. So I was specifically referring to your unclassified contracts that would fall under the realm of controlled unclassified information. So there's no doubt that the classified there is a requirement.

Chris Dzurilla: Sure. Just from a detection and monitoring standpoint our capability extends to the unclassified networks. Based on our policy it is still limited to clearance holders until we can update the definition in our (unintelligible) our other privacy documentation. So that's still catching up with the expansion of the program. Eventually we will get to a point where we're monitoring all employees on all of the networks. We have a phased approach as Megan alluded to. We're working with the operational components so your TSAs, your CVPs and your ICE operational components to develop a phased approach to deploy the monitoring capability to their unclassified networks.

That plan extends - I think we're budgeting and planning for another potentially three to four years out looking at full coverage and the full expansion of the scope the program (fit).

Greg Pannoni: Thank you.

Megan Davey: Yes. So when I say beyond the protection of classified it's looking at the core mission but only currently monitoring those cleared employees.

Greg Pannoni: Okay.

Charlie Rogers: This is Charlie. Chris but if we down the road when we do monitor the unclassified networks any contractors who have access to those networks would fall under…

Chris Dzurilla: Correct.

Megan Davey: It's a part of that user agreement when you create your account and you have that warning banner that you see every morning when you log in. Yes?

Leo Masciana: Leo Masciana. I have a questions about organization - three distinct questions. One about your direct organization - I think you mentioned an office level. The other would be the decision process; if it formalizes direct input from other organizational elements. You mentioned IT or the CIO counterintelligence office, security office beyond the civil rights, civil liberties folks. And then the third one would be if you're speaking to and working with programs and other agencies directly, to see how they're implementing their EO mandate.

Megan Davey: Yes. I can speak to all three. So one, the insider threat program falls under the Office of Chief Security Officer. So we are security based with varied personnel from CI and investigative support and security as well. We work with all offices at DHS as far as the Exec. Sec. goes. So any policy we're going to be putting out we have to get comments, feedback, buy in from all of those stakeholders. So outside of that oversight group that I mentioned. So we're currently working on our second instruction and it's out for comments and feedback and for the components as well. So secret service is providing input as well as TSA.

And then yes we meet with other agencies. I actually am coordinating a visit to the FBI here soon for myself, my director and Chris. We're going to the DIPMAC to visit as well. So we're trying to see best practices, lessons learned and try to see what would best apply for the approach we're looking for in our insider threat program. Does that answer your question?

Leo Masciana: So the one question about formalizing input - do you engage them beyond policy into incidents by insiders and what's to the - to be done about an individual's career prospects if they are found to be an adverse element?

Megan Davey: So we serve as the hub. So tips will come into us through various means whether it's phone calls, emails, supervisors reaching out to us. We are not the actors per se. We provide support if they need it. And we would refer them to the appropriate entity who is able to act under their authority. So we do have a wonderful relationship with our CHCO and our personal security division to where we freely exchange information and very quickly as needed.

And this instruction we're actually putting out has an attachment or an addendum to it that is specific to information sharing so we can better communicate and respond quickly and address things to prevent we're looking for that detection; deterring; getting ahead of the game especially when it comes to workplace violence and things of that nature. Does that answer anymore…

Leo Masciana: Leo again. So your HR department probably takes the actions…

Megan Davey: Yes.

Leo Masciana: …unless it has to do with clearance suspension. That'd be security.

Megan Davey: Yes. And that's PSD.

Leo Masciana: And if it's a criminal matter it would be refer to your law enforcement.

Megan Davey: Yes. So we're very fortunate that the insider threat program falls under the security group because our investigative group is actually in our division and then we also have PSD which is just right around the corner in security as well. But, we've been able to build relationships and establish POCs that we can quickly get that real time response as needed and make sure it's referred to the appropriate group. Is that good now? Do you think you've got it all?

Leo Masciana: So it is an office level?

Megan Davey: So we - yes we are - our security office has three different directors. We call them our threat, our headquarters and our enterprise. So the insider threat program falls under the threat group for the Office of the Chief Security Officer. And we are under the management directive for the Department of Homeland Security.

Man: But if the headquarters office…

Megan Davey: Yes.

Man: …is security for all of DHS…

Megan Davey: We're the hub for all of DHS.

Leo Masciana: So insider threat would be at division level function or…

Megan Davey: We're a division…

Leo Masciana: I'm sorry to keep hammering.

Megan Davey: No, no, it's fine. No. We're a division but we represent the Chief Security Officer who is a senior insider threat official. Yes. He…

Charlie Rogeers: He's the Chief Security Officer for all of DHS. I mean FEMA has a security office, TSA has a security office but the Chief Security Officer hosts the CSO Council and he is responsible to the Undersecretary of Management for that program.

Megan Davey: Yes. He's been appointed to be the lead for that.

Charlie Rogers: But there's a lot of cooperation. The IG could be involved, I guess counterintelligence could be. It depends on - there are - I don't work the program but there are lines that connect to other key stakeholders.

Megan Davey: Yes. We've recently moved into a new space. We've had issues with finding a location to house all of our staff and we have spaces for if different components want to come sit with us. OIG, CI, our CIO. So we're making sure to start to take on that hub like atmosphere and to have all the players in house as often as we can. Do you have anything you want to add to that Chris? No? All right. Thanks.

Mark A. Bradley: This is the Chair. ISOO has been asked recently to begin to think about expanding the CUI program to the insider threat program. And one of the legal issues we've confronted though is the insider threat program, the executive order that governs can find the classified information only. What authority are you using to expand your insider threat program to cover unclassified. Yes. I'm just curious.

Megan Davey: The Secretary expanded the definition with the 2018, '17?

Mark A. Bradley: (Unintelligible).

Megan Davey: There you go. So he expanded the definition and we've taken on the responsibility of the expansion. So as far as we've just taken it one step further past that minimum standard that was mandated.

Charlie Rogers: And you correct me if I'm wrong but I believe since they looked at the program and the value of the - of doing it for clearance folders in classified and they said well the threat is much larger; the potential threat and this effort is taking a significant amount of resources. It would make sense to expand it to address the overarching threat and just focus on clearance holders and classified information. So that's…

Megan Davey: Yes. That's the uniqueness of DHS.

Greg Pannoni: I think it's the process of the decision. And if I'm not mistaken, Greg Pannoni (unintelligible) the EO, the order itself gives the agency head the authority to expand. I think that's how it's constructed. The 13587.

Megan Davey: Based off of your mission needs. Yes. Exactly.

((Crosstalk))

Mark A. Bradley: …language in there. All right good. Thank you. Any questions for (Melissa) or Chris?

Megan Davey: No? All right. Well thank you for having us today.

Mark A. Bradley: Oh thank you. We appreciate it.

Megan Davey: And if you have anything else Charlie can hopefully link us up.

Mark A. Bradley: Sure he can. All right. We're now going to turn to Devin Casey on my staff to give a briefing on controlled unclassified information; where it stands as of today.

Devin Casey: Good morning. I'm Devin Casey from the CUI staff at ISOO. I work for the controlled unclassified information program which is an information security reform addressing the protection, handling and minimum standards for all controlled unclassified information handled by, collected by or stored by the Executive Branch. It's probably one of the largest information security reform since the creation of the classified program. It covers all types of controlled unclassified information from privacy information to unclassified enabled nuclear. There are about 100 categories of controlled unclassified information which can be found on our Web site, which is something I'm going to hit right now because I can't do a full overview of the CUI program in ten to 15 minutes.

So Archives.gov/CUI. That's Archives.gov/CUI. It's something we'll send out to you. It has all of the training and information policies, notices concerning the CUI program and its implementation. We have hours of videos that are downloadable that you can watch online. We have all of our CUI notices that explain the different aspects of the program; we of course have the 32 CFR 2002. It's our implementing directive as well. Many of you may already be or started becoming familiar with parts of the CUI program.

One of the most prolific parts of the CUI program that's spread rather rapidly is the minimum standard for nonfederal information systems that was created and enforced through the NIST SP 800-171. It was a joint - it was published by NIST with our help as well, to define the minimum standard for protections on nonfederal information systems that process federal information that qualifies as a CUI. And it was an intent to standardize how the government requires or asks nonfederal entities - state, local, tribal, as well as academia and industry, to configure their information systems when they're not being operated on behalf of the government to protect controlled unclassified information.

We found a lot of agencies were doing this in very different ways - some of them relying on, you know, kind of ad hoc partial implementation of 853, others on unique controls that they've invented themselves and some just relying on the recipients to protect the information based off of an agreement and no real defined standards. So this 800-171 is already in use by DoD. It's already in use throughout the (DIB) through DFAR 7012 contracting. So it's filtered its way into industry already. A lot of academia has also begun implementing this 800-171 at the direction of the Department of Education as well as contracts with DoD.

Some states already have begun referencing the SP 800-171 in laws, regulations and policies at the state level. For example, Ohio has the Ohio Data Protection Act which actually is a new law that they passed that provides some level of liability protection if a company in the state - if their cybersecurity systems meet the NIST 800-171 compliance requirements. They have limited liability in case of a data breach for the - an interesting implementation.

Other states have also started initiatives to help small businesses and companies and agencies within their state to implement the controls of NIST 800-171. For example, Maryland and Virginia have already begun offering either grants or tax based incentives to meet the requirements there. An important note on the NIST 800-171 is that there is an attachment for it. There's a NIST 800-171(A) which is an assessment guideline, which helps standardize the way that these systems are audited by federal entities and also provides a way for industry or the nonfederal entities to audit their own systems and they're doing so in a way that the government will then use a similar compatible method to audit those systems as well.

It is currently on Revision 2 which is actually out for public draft. There are minor changes to the Revision 2. The main reason that Revision 2 came out is because it came out at the same time as NIST 800-171 (B) which is additional controls that can be levied by the government to address things like high value assets for particularly sensitive types of CUI that face advanced persistent threats.

So these are more advanced controls for the protection of information and that can be found in (NIST) 800171(b). Now both Revision 2 and 171(b) are out for public comment. It was extended to August 2, 2019. And you can find a link to that through our blog which is on our Web site and we can provide information for a follow up to this email - to this meeting as well. On that note we do have a quarterly update to stakeholders. And when we say stakeholders we mean everybody from agencies to industries to any nonfederal entities that would like to join us. We advertise this through our CUI blog which can be found on a link right at the top right of our Web site.

Again we do them quarterly. They're about two hours long. We spend about 30 minutes to an hour giving an update on any changes in the CUI program, anything new that's come out. And then we spend about an hour doing question and answer for any questions from industry - frequently from industry but also agencies and nonfederal entities. We've done a lot of work in our office on implementing the program. It's still a rather new program. The government as a whole is still implementing. Agencies implement it kind of at their own pace although, you know, generally in lockstep.

The biggest thing that we had reported to us because we do get annual reports on the CUI implementation at agencies, is that most agencies will have policy out sometime this year. Policy was kind of the biggest hurdle. So we saw a lot of delay in getting the policy ready. There was a lot more work that had to go into identifying how agencies were currently protecting this information than maybe we thought.

And so it's taken a lot longer to create policies to address current practices, to roll on those information. Once the policies come out we usually see about 12 to 18 months before full implementation of the CUI program after that. We are conducting another annual report. We're just - we're working on the form this year - this week. It should be going out shortly to agencies so we can get new information about where they are and the implementation of their CUI programs.

One of the biggest projects that our office has been working on to support this implementation is a creation of a FAR case. And this is a new federal acquisition regulation set of clauses to address and standardize the communication of cybersecurity requirements as part of the CUI program to industry as a whole. As mentioned, DoD has already moved out. They already actually have a DFAR 7012 that addresses a lot of the same topics our clause will. That can - we look at that as kind of a template for our clause though we do go a bit further and wider in our requirements for both the government and industry.

So we require a little bit more work on the government's half. We have a pretty hard line in the sand that says if you're going to share information with a nonfederal entity it must be marked or identified if you expect them to protect it. A few other requirements there as well. And then on the industry side we expanded from just cybersecurity and incident reporting to things like physical security to structure and training. So that will come out for public comment hopefully this fall. It's been a long time coming and we've been working on that quite diligently in this office.

So public comment sometime in the fall. If you're - if that's something you'd like to read or look at we'll of course post an update on our blog about when that comes out for public comment. So if you're not one of the people that reads the federal register twice a week like I do, you can get a blog notification that it comes out. We'll also be doing an ad hoc stakeholder meeting to address questions and concerns about the FAR to help inform on quality comments.

It always bothers me when we get comments back that ask what this means because we've missed an opportunity to get a constructive comment back if we didn't, you know, provide the context of the FAR or the information that's being presented there to the people who could be proposing those good comments. So we will be doing an ad hoc stakeholder meeting. If there are a lot of people or if our phone lines get too big we'll throw another one, but we're happy to do that to get that information out, and we're looking forward to the public comment period of getting that expertise from industry and nonfederal entities back from that.

Our office is the oversight office for CUI so we're the ones responsible for its successful implementation and for making sure that agencies successfully implement it. It aligns with a lot of the goals that have already been talked about in this meeting. In fact it was born of one of the incidents - the 9/11 incident and a failure to share unclassified counterterrorism information between agencies. So CUI is very much an information security program. I know we spend a lot of time focusing on the security part of an information security program, but the CUI program also spends a lot of time focusing on the information program part of an information program, which is ensuring that individuals who have a lawful government purpose or authorized to receive information, don't have to jump through unnecessary barriers to access it.

And we achieve a lot of that ability of cost savings and increased security through standardization of requirements for both the executive branch as well as industry. And of course through the standardization of marketing and security practices. That's the goal and purpose of the CUI program. I'm going to hit it one more time - Archives.gov/CUI. We'll send it out. Please join our blog for updates. We'll post - point to new things. We have coversheets and stickers that came out. We point it to the (NIST) Web site for public comments on the (NIST) documents. So we try to keep one stop shop to be appraised of new developments in the CUI program is right through our Web site.

If there are any questions about the CUI program, I'm happy to answer them now.

Mark A. Bradley: Leo?

Leo Masciana: If I understand - my question will follow this. My understanding of the FAR clause is that it will implement requirements of the SP 171 into a contract acquisitions requirements for the industry and contractors - contract organizations and operations. If that's the case then does it become incumbent upon the agencies with industrial security programs to then also implement those with security clauses in the facilities and the systems that they are authorizing to process CUI information?

Devin Casey: So the FAR clause - there will be a universal FAR clause included in all contracts. And it'll have - and I know this is bad contracting (unintelligible); it will have a self-delete in it if CUI Is not being shared. And the only contract that's exclusive from our comps exclusive contracts. So if it's commercially off the shelf exclusively then the CUI clause won't apply. For any and all other agreements the 32 CFR 2002 and a CUI notice address that when entering into these agreements with nonfederal entities or when having the opportunity to revise existing agreements with nonfederal entities the new standard of the CUI program should be referenced and used and the standard should focus on the minimum standards of the CUI program and not agency specific implementation of that program in order to take advantage of the standardization of the program whenever possible.

Leo Masciana: Leo again. So you're anticipating that the industrial security program will incorporate that in their security clauses?

Devin Casey: It's very likely that they will use very similar language. So there is no restriction on using the new FAR clauses if you are not covered by the FAR and other contracts and agreements that you enter into. So a lot of people do take that language. Specifically - I was just talking to FHFA who plans on using a significant amount of the FAR language and content that we'll be putting out even though they're not actually covered by the FAR. So that is language that can be used. We do have a draft template and notice to discuss the content of agreements that aren't covered by the FAR, to ensure that they meet the same (topics). But the NIST 800-171 standard is for anywhere where you're sharing CUI onto a nonfederal information system. The NIST 800-171 standard should kick in at the minimum baseline of protection.

Mark A. Bradley: Any other questions for Devin on CUI?

Devin Casey: I will note for the 171 standards oversight is based off of a risk management model as employed by the agency. So the types of oversight that they conduct, how they conduct oversight and how frequently (unintelligible) their internal risk assessments at the agency. Our goal is to ensure that when oversight is conducted the results are shareable between agencies to reduce multiple (visits).

Greg Pannoni: This is Greg Pannoni, ISOO. And Devin you can help me out on this but it's also true that the draft of the FAR clause right now for the CUI will have a companion sort of something akin to a contract security classification specification. But this will be a contract security control specification. So wherein the identification of what CUI is required in order to fulfill this contract it's identified. Is that correct?

Devin Casey: Correct. So there is an accompanying standard form that's going through the FAR process from the FAR that includes a lot of information. And this is where I was talking about the government will have requirements to enter into these contracts as well. And one of the requirements is to ensure that this form is appropriately and properly filled out. So one of the things that the form does is it requires that any and all information security requirements pertinent to unclassified information must be included in this form or referenced in it, to create a one stop shop for industry and the nonfederal entities to go to that form to understand, you know, where all of the stuff is.

So it's not - so hopefully they have the privacy stuff from the privacy section; the cyber stuff from the cyber section; the incident reporting stuff from the incident reporting section; the insider threat reporting stuff. If it's related to the CUI information and access to it, it has to be referenced there in that part. Another big part of it is - and I talk about this when I talk about CUI a lot - the government has to become a lot more deliberate with what we're protecting and why. And so part of the form requires the government to identify the types of information that will be shared in this contract and whether or not they have special security or handling or dissemination requirements on them.

So there's a type of CUI called CUI specified that requires additional or separate handling from CUI Basic. That would have to be identified on that form as well. So these practices are echoed in our requirements for nonfederal agreements that are exempt to the FAR. But you may - once the FAR comes out - you may see that language used more in those agreements as well. Agencies will be able to, you know, as part of their own phase of implementation address their existing agreements in accordance with their timeline to do so.

So if they have an agreement that's coming up for renegotiation they may, you know, implement the CUI program there earlier as opposed to, you know, reopening ones that have just closed, in order to implement the CUI standards because they do have a requirement to get to full operational capability through agreements as well.

Mark A. Bradley: All right. Any other questions for Devin on CUI. Thank you Devin.

Devin Casey: I hope to see you at the stakeholder meeting.

Mark A. Bradley: All right. Now we're going to turn to the last part which is our open forum discussion. It means we're in the Wild West. Anybody wants to say anything at all say it.

((Crosstalk))

Marc Sachs: You have them in front of you so we can just work through them.

Greg Pannoni: Oh. I can do that too. Sure. So Greg Pannoni, ISOO. Mr. Sachs provided us with an email with a number of items for consideration. The one was a need for a single point of contact in the government for SLTPS personnel to track clearances. So we sort of heard about that; we talked about a concierge type of service at DHS. So we can start right there if you want to expand on that.

Marc Sachs: This is Marc Sachs. Yes. And I say DHS only because you're the holder of most of the private sector's clearances. But you would include cooperation from the Bureau of Energy. Others who have it - the general idea and I've heard this suggestion or request for years from my peers as well as others, is that it would be very handy if kind of look working with the IRS. You know, there's only one place you file your taxes. It would be nice if there was just one place if you're not in the government - in the federal government, where you could go to find out the status of your clearance. And that one place could also serve as the conduit to alert you if there are changes or things ongoing.

Where this comes to light is if there - let's say the Department of Energy picks up on some threat to the power grid and they quickly need to assemble a group of people or get the word out - go to your local fusion center, go to the FBI where there's something for you to read. First you have to pass your clearance. Well the private sector doesn't always know how to pass that clearance. So if there was an 800 number to call, an email to send it in, or something with the concierge service to say okay I've got it for you Mr. Jones. We'll take care of it. That's a general feeling. Plus the, you know, how do I know if my clearance is about to expire; who is my SSO; those general kinds of questions.

Whether it's the DHS is immaterial. It just kind of makes sense that you hold most of the private sector clearances.

Charlie Rogers: (Unintelligible) DHS. I think the key element is that you can't have a concierge service - do you have the database figured out?

Marc Sachs: Correct.

Charlie Rogers: And then if the database gets figured out there may be a way to create a portal that, you know, because we did try to create a portal for CVS for fusions that didn't address private sector. But fusion centers were given accounts to CVS for the purpose of verifying clearances. But if you don't have the data in CVS it doesn't work. So the private sector doesn't have a similar portal but I think the key element is - I mean I'm not trying to talk out of a (concierge), but you can't be a concierge service until there's a database.

Marc Sachs: Correct.

Charlie Rogers: You know, until we solve the database or get - because DHS is unable to go, you know, we could have an 800 number but we're not going to be able to…

Marc Sachs: Well unless we had an office that did have access to JPAS - did have access to (unintelligible), you know, all of the different systems and you had an authorized person there who may be a rep from that agency that owns that system but sits in that office, to handle that request.

Charlie Rogers: Yes. It's twofold I think.

Marc Sachs: Yes. I'd say so.

Devin Casey: Is that information already included in their indoctrination briefings or their user refresher training?

Marc Sachs: It's quite possible but these folks don't deal with classified on a day to day basis so they're not surrounded by the institutional knowledge. And they may only get their classified briefing once a year in order to check the block that says I'm keeping my clearance "active." But in a crisis situation where we're trying to get people together quickly they often just don't know where to go. That's something that a single point would be better.

Devin Casey: I'm concerned that they don't know who to pass their clearance - how to get their clearance passed that they also might not know how to report security incidents or things of that nature.

Marc Sachs: It's quite likely. I mean we're talking a big problem…

Devin Casey: Because that should definitely be…

Marc Sachs: …where we're looking at a piece of the solution.

((Crosstalk))

Charlie Rogers: …working on the Web site too that I'll send out, is that, you know, people are granted clearances; they do get emails; we debrief people who don't respond to emails but it's a big challenge when you have people nationwide who are cleared and a lot of times the program offices are working directly with them and we work with the program offices but…

Yes. So there are multiple issues. I mean the concierge thing is one; the database is another; trying to get information out to the end users so I'm not trying to say this isn't a real issue by any means. I just think the answer is complicated.

Marc Sachs: If it wasn't an issue we wouldn't be talking about it. So it…

Man: Yes. Right.

Man: Yes. Right.

Marc Sachs: But like with everything else we can talk about it all day. What's the right thing for this policy group to do? Is it a recommendation or is it a…

Charlie Rogers: (Unintelligible) we're going to have a working group shortly. So we'll start with that one piece and then we'll…

And maybe as part of the database find out how can people get - is it available to get access or how could agencies get access or…

Greg Pannoni: So this is Greg Pannoni. I agree we need to start with the database to try to have something where the consolidation of all of the clearance data for SLTPS is available in one place. It could be in different places but where you can get to it. But then as far as you mentioned trying to give people access on those systems - that to this day is a challenge for some non - for some federal non-DOD agencies. I know we just had a meeting. We chaired this thing called the NISPPAC which is for - it's the National Industrial Security Program for Classified. And agencies like the State Department has - waste many times to us the ability to get JPAS accounts and now their DISS accounts.

So I think the two go hand in hand; the discussion about getting the database to where we have identified all of the SLTPS people that have clearances and then start that discussion about well how can they then go in and see - or what is the mechanism to access the clearance level of these folks the date of their prior investigation and things like that?

Marc Sachs: Well and also - Marc Sachs, for the individual to see that, for example as retired military I can log into (TriCare), I can log into all of the retired services.

Greg Pannoni: Yes.

Marc Sachs: I have to click past the banner that says you're entering a federal system. But once I'm there and properly authenticated I can find out what benefits I have; what, you know, things that have dates, expirations. I can do a Social Security, you know, to find out what my benefit - I mean there are lots of federal programs already in place. The thing that's missing here is I have no place to go as an individual that says here is when your clearance expires or here is who to call to have your clearance passed.

Greg Pannoni: Yes.

Charlie Rogers: Yes. Well I'd have to get a personnel security officer - different people involved in that. But I know that even within the federal government the ability of the federal employee or even a federal employee in the Office of Security to access that data is greatly limited.

Marc Sachs: Yes. We're not asking to see their file.

Man: Yes.

Charlie Rogers: No. I know. But even just…

((Crosstalk))

Charlie Rogers: Yes. But even that - and so I'm not…

I'm not a subject matter expert at all but well it's all worth discussing.

Mark A. Bradley: (Unintelligible) evaluation program coming online. That's a whole different…

Man: Yes.

Leo Masciana: Greg, I have to ask you a question.

Greg Pannoni: Yes.

Leo Masciana: Leo here. The JPAS and CVS - my understanding is those two databases were to become full merged so it would not matter which one you went through. (Unintelligible) the answer?

Greg Pannoni: I don't - that question about the full merger of JPAS and CVS that's - I'm not understanding it that way. JPAS is being overtaken by DISS. That's a new system for defense but since they have all of the clearances you may be onto something - or just about all of the clearances now with the transition from OPM/(NBIB) to DOD.

Leo Masciana: I mean that would be a good solution.

Greg Pannoni: Well there is - but now I think Charlie alluded to it earlier. There's a way to get to JPAS data or let's call it now DISS, through CVS. It's a little bit complicated but there is - that capability exists right now. I've seen it demonstrated. So if you have access to CVS you can get to JPAS/DISS…

Leo Masciana: Is that going to satisfy (Kim Balger)? Because I hear from her…

Greg Pannoni: It's probably not.

Leo Masciana: …every week about the JPAS access problems.

Charlie Rogers: And this is Charlie. I can't speak to JPAS but JPAS was - when I was hearing about it, it was also the way DOD does it is it's based on the person's investigation but you don't know whether they're currently authorized to have access because they sort of - DOD has a unique way of dealing with it. People are debriefed and then re-briefed and then debriefed so you could verify that somebody has a legitimate investigation but you can't necessarily verify that you can share classified with them unless they sign a 312 and if you don't…

Man: (Unintelligible).

Charlie Rogers: I don't know. So there are some unique configurations of these databases.

Greg Pannoni: It was a joint person adjudication system.

Charlie Rogers: Yews. Yes.

Greg Pannoni: Meaning they should have been adjudicated.

Charlie Rogers: Yes. But for example if DOD frequently debriefs somebody they come on - they're in the National Guard; they have their two week activation - they're briefed in and then they're briefed out. They're - you look the up in JPAS and I may have this somewhat wrong - you look them up and it says their investigation is good; they have a secret clearance. That doesn't mean you can turn around and give them secret information because they've just been debriefed. You know, so there are some unique - I mean - all I'm able to say is there are some unique configurations of JPAS that don't necessarily say go/no go; yes/no. Like some of it says yes/if. And…

Man: (Unintelligible).

Marvin Mackey: This is Marvin Mackey from the Department of Transportation. Basically you…

((Crosstalk))

Man: (Unintelligible) how do I get the (re-sidebar)?

Man: Can you guys let…

Marvin Mackey: I'm sorry Marvin.

Man: I'm sorry.

Marvin Mackey: I just wanted to pipe in a little bit because I spent a lot of time at the DOD working JPAS, adjudications and things of that nature. But what - I think what we're - kind of got a little bit (sidetracked) on is not the person who clears because you've got to remember we do it as eligibility and then access. Access is determined at the local level with their owner organization. That's kind of I think what we're missing is that you don't have an owner organization to manage and process your clearances. So when it's time to pass it who is your owner organization; who is your parent?

So that's what that JPAS system was designed for is to have the overarching jams with adjudications JPAS that has the clearance information in there. And so you have the eligibility which is granted from an adjudication and now access locally from commanders and parents who own that clearance information for you, the individual. So we kind of - it's a little bit different for us here but that's what the whole JPAS system was designed for. So that's kind of my 2 cents worth.

Charlie Rogers: That's what I was trying - I knew there was something like that but…

Marvin Mackey: What he said.

Man: So I think we do have to start with that working group that addresses the database and then figure out the next steps for addressing that concern.

Greg Pannoni: So in the interest of time the next item was - you mentioned Marc the need for rapid declassification of time sensitive cyber information. So Mr. Masciana talked a lot about that too and he mentioned the value of most cyber alerts decrease significantly within 24 to 48 hours of the government discovering the issue. Often it takes days or weeks to declassify and provide a warning. By then the threat has already done damage. So…

Marc Sachs: Correct. And I don't know - this is Marc Sachs, if I need to amplify. I think everybody understands it's cyber information - and we're talking the technical data. You know, the bad actor is coming from this site he addressed doing these things. It may not be doing that three hours from now. That bad actor may still be there and how we determine that bad actor is bad it all stays nice and classified. But what they're doing is the key piece.

Think of it in a physical sense. If law enforcement is chasing, you know, some crazy who is about to blow up Walmart, they'll call Walmart and tell them to lock down; crazy guy is coming your way. In cyber if we're picking up on crazy guy trying to launch an attack against a private entity we frequently won't call the private entity because their hands are tied. Or our sources and methods won't allow us to tip the private sector. That's the piece we have to get in front of. And that's the if we're creating products at the SCI level an analyst is creating it; thinking ahead of how do I do an unclassified tear-line of just tactical technical stuff?

And it has to be on class because the system administrator who is going to do something about it - a firewall or whatever, does not have a clearance; doesn't need a clearance. You're just - it's just admin. They need to be able to take action quickly and I can't be briefing the CISSO who might have a TS/SCI clearance that's great. He can't or she can't then swivel to a sys admin and say do the following things.

Right? So we're talking again actionable information. It's technically actionable. Not who is doing it; why are they doing it; that can all stay locked up in a classified world and not go out there at all. Right? Or Law Enforcement Sensitive.

Greg Pannoni: So that's a challenge. Greg Pannoni, ISOO. You've got the information itself and, you know, distill it to just what's actionable but then how do we quickly within a couple of hours, get it to the asset owner?

Marc Sachs: Well this was the intention behind the various EOs, behind all of the policy that we talked about over the last 20, 25 years is to do that and we're doing very well on the unclassified stuff, things that industry picks up on and shares with the government. It's turned right around and the problem is when we're picking up on stuff that's come into classified channels and how to quickly get that down to where we can action on it.

Greg Pannoni: I'm not sure I have the answer. Where do we take this to…

Charlie Rogers: The intelligence committee?

Pam Miles: Pam Miles. It's really difficult because in order to turn that information around you are giving up sources and methods. You know, you're talking about various ways of getting that information. It's not like, you know, it's coming from a bulletin, I think from Walmart. Do you know what I mean? Or the local police department. So because - and various agencies and mission needs are different. They have their own classification guides; they put out, you know, their own products. So it's not - it's hard to say a one size fits all. You know, it's hard to say okay here is this shoe; everybody needs to have the right foot to fit in that shoe.

And because the various mission needs and the various agencies involved it's really hard to say okay here is a policy and everybody has to follow it in order to get that information is a challenge. And we know that.

Man: (Unintelligible).

Pam Miles: Exactly.

Greg Pannoni: This is Greg Pannoni. Is there some room to consider - if not - it's kind of like a middle ground? It's not unclassified. You have the fusion - you have 80 plus fusion centers throughout the country and perhaps other locations that operate at the secret level. If there were a way to at least break it down, the actionable information to that level then it would be incumbent upon the state and local travel folks or private sector, to get to that fusion center I guess, to get the information. But…

Marc Sachs: Well this is Marc Sachs. It's good to get the info but if you can't do something about it. There have been cases like phishing. This is a great example. We're all very familiar with it. You'll get - some company gets targeted and it's maybe going to their HR department and it's got an attached Word document for somebody who is trying to apply for a job. The Word document is poisoned and introduced malware.

Okay. The fact that the government knows that's going on may have started in some classified role but telling an asset owner that his particular Word document that you're receiving via email contains malware in it, that's the kind of thinking process has to go through. Would that really have some impact on national security? And - but oftentimes you don't get to that conversation because it's still locked up inside the SCI analyst world. And it's - how do we break through that where at least the question is asked can this piece of information be shared quickly and how do we do it in a review process that doesn't take days, weeks, months, years like we normally do for downgrading classified information?

Greg Pannoni: Charlie did the fusion - this is Greg Pannoni, ISOO. Do the fusion centers keep some sort of an inventory of, I'll just as it this way, of - in their geographical area all the cleared SLTPS people that let's just say are within a 50 mile range of that fusion center? Because what I'm thinking of - they could put an unclassified alert if they were to get something at the secret level. I'm saying we've got something - you need to come and, you know, as quickly as possible to get over here.

Charlie Rogers: Well there are a couple - they have distribution lists and they get threat information so they have distribution lists for hospitals; they have distribution lists for ports or whatever is their regional and geographical area of interesting. In Wyoming it might be transportation because of nuclear waste transiting their interstate highway. So they have distribution lists. But when you get to cyber and this is just a personal thing - when you get to cyber you're talking about federal information and they - and if it's classified I think there needs to be some federal decisions about who's getting - not that the states will then say well here is this secret information; you guys figure out who you want to give it to.

I think that - and that's, you know, I mean we'd have to get some other people in the conversation. We have, you know the new CISSO within DHS might have some opinions on…

Marc Sachs: And cyber command…

Charlie Rogers: Yes.

Marc Sachs: …needs to be involved.

Charlie Rogers: Cyber command and some other - because I do think we don't want to delegate, you know, our own - it's the mission owners want to delegate the distribution of federal classified through the fusion center. We do a lot of threat information on classified, you know…

Greg Pannoni: Well there are two steps there. So the one would be providing it to people that are actually have been vetted with a clearance

Charlie Rogers: Right. Yes.

Greg Pannoni: And then the next step perhaps rolls into your other suggestion about the use of a one day read on for briefing private sector folks that don't have a clearance when something urgent is developing. And so we actually have a mechanism in the executive order for classified, for emergency authority wherein, you know, it even takes into account the third agency rule so that the agency that has the information in defense of the homeland, that's part of the emergency situation.

Charlie Rogers Imminent.

Greg Pannoni: Right. Imminent threat.

Charlie Rogers: Imminent threat to life.

Greg Pannoni: Could share with an uncleared in this case, private sector and then there are some provisions for - within the 30 day period, follow up notification to the information owner what just happened and why it happened too.

Charlie Rogers: Yes. You've got the provisions under the executive order which have a pretty high threshold.

Greg Pannoni: Right

Charlie Rogers: DHS has done, you know, one day read in, (pay fund), what is it 12968 I think and - but that requires a certain level of paperwork.

Marc Sachs: A little background check.

Charlie Rogers: It does.

Greg Pannoni: Yes.

Charlie Rogers: And a couple of minimum checks. But then I believe back to (ODNI) they're writing C data I believe it is and I know I'm not involved in that but there are people in my office who have seen draft copies of it. So I think this is being looked at and revised.

Marc Sachs: Marc Sachs. The one day read on actually is better when you're doing awareness and broader kind of education. But doesn't require the rigor of going through a full secret background check and the cost to the federal government of doing that. An FBI wants a (warrant) like you do for the (Infoguard) program where you just check out there's really nothing wrong with this person but they don't need a full blown security clearance but we do need to inform them; educate them; show them what's going on, on a need to know basis.

So if you're working something like that that's going to help as well but we don't have to go to through the (expensive) program of giving clearance to everybody. We don't need to do that.

((Crosstalk))

Pam Miles: …hopefully the end of the year SEAD 8 will be published.

Marc Sachs: Great. Thank you.

Pam Miles: Don't hold me to that date but we're hoping.

Marc Sachs: Right. Okay.

Pam Miles: And it addresses temporary eligibility.

Leo Masciana: This is Leo for Pam. In terms of the nexus within the DNI for deconflicting and resolving the complex problem, is the program manager for the information sharing environment, Steve Mabeus, a good touchpoint for working with the EO policy advisory committee?

Pam Miles: That I don't know. I don't - I will have to get back to you on that.

Leo Masciana: Because I've been persistently raising these issues with them was well, with the information sharing council and asking that they collaborate with this group. If there is a better way to tame it in trying to resolve the - that issue from the TS disconnect I'd appreciate your follow up on it.

Pam Miles: Yes. I don't know him. I work in NCSC, the National Counterintelligence and Security Center so I don't know where he's located.

Charlie Rogers: Yes. This is Charlie. I've reached out to him too and invited him to this meeting and have yet to hear back from him. (Unintelligible).

Leo Masciana: Well there's a council meeting coming up so I'll mention it again.

Mark A. Bradley: Please. Tell him the Chair is looking for him.

Leo Masciana: Will do.

Greg Pannoni: Okay. So I think we made it. Let's see if there were any other - I think that was your last one.

Mark A. Bradley: This was good.

Greg Pannoni: Yes. Thank you.

Mark A. Bradley: Anyone else has anything they'd like to raise in the open session? Anyone still on the phone like to raise anything?

Greg Pannoni: I'm sorry. There was one more. You actually had the question of maintaining automatic access if a person's separated. Let me just read it. As an alternative to the one day read on automatically maintain secret security clearances for government employees and contractors after they depart the government or after the contract ends. So I assume when you're saying contract you're talking about private sector folks like yourself?

Man: (Unintelligible).

Marc Sachs: Oh (NIS)? Okay.

Marc Sachs: So two things - if you're an ex-fed which is what we like to call it…

Greg Pannoni: Right.

Marc Sachs: …you're (read) off. Your clearance indication is still there but you're (unintelligible) not current. And at some point that times out. That person, unless they do something wrong, is really nothing in their background that precludes them from being, you know, brought back on quickly, except for policies that say no we've got to go (re go) through the entire adjudication process.

Greg Pannoni: And so - this I Greg Pannoni. This is something I know that Trusted Workforce 2.0 is definitely looking at. The ability to bring the person back - I forget the terminology; the way they're using it now. When someone separates but still has a current investigation…

Marc Sachs: And the same thing for cleared contractors.

((Crosstalk))

Woman: (Unintelligible).

Marc Sachs: That's addressed in that…

((Crosstalk))

Mark A. Bradley: All right? I am going to adjourn this meeting in a moment. I'll - the next SLTPS PAC will be January 29, 2020 here in the National Archives from 12:00 - 12:00 Noon. We'll have a room at that time. All right. Thank you. It was a good meeting today. Again the goal is to make this body into something that actually does something instead of (debating) society. So anyway I think we're on our way to doing that. So without further ado I will adjourn. Thank you all for coming.

Man: Thank you.

Woman: Thank you.

END