STATE, LOCAL, TRIBAL, AND PRIVATE SECTOR POLICY ADVISORY COMMITTEE MEETING
Mark A. Bradley, Chair
July 29, 2020
10:00 a.m. EDT

Mark Bradley: Okay. Let's do it. All right. Good morning, everybody. This is the second State, Local, Tribal and Private Sector Policy Advisory Committee meeting of 2020 and the eighteenth SLTPS-PAC meeting overall. I dare say this is probably our most challenging one yet. Let's hope the technology holds up. We're trying to keep this as basic as we can by just using phone lines.

That said I look forward to what I hope is like all of our other SLTPS-PAC meetings and that means having a robust and very frank discussion. This is a public meeting subject to the Federal Advisory Committee Act. The minutes of the SLTPS-PAC meetings are available to the public.

This meeting is being audio recorded. As always please, and this is particularly important this time, please identify yourself each time you speak so we have an accurate record of your comments. Also, when you're not speaking please mute your phones. Now when you mute them just remember to unmute them when you do speak.

Some administrative business here. We've had some membership changes. I'm pleased to introduce our newest SLTPS member Sergeant Debra Winsor, Deputy Director. Washington State Fusion Center, Seattle Police Department. Debra, I'm going to ask you a little later on to tell us a bit more about yourself. But I can well imagine you've been rather busy lately.

Debra Winsor: I have been. Thank you.

Mark Bradley: Oh, yes, indeed. I also want to introduce a member who joined our committee in January but was unable to participate in our last meeting because she was meeting with her commissioner. And that is Mary Michelle Schechter, Director, Division of Community and Maternal Child Health, Nassau County Department of Health, New York. Welcome, Shelly.

Shelly Schechter: Good morning. Thank you.

Mark Bradley: Yes, sure. And again, a little later on in meeting we'll have a spot for both of you to introduce yourselves and tell us a bit more about you. You both have really interesting backgrounds and we're really pleased that you've decided to join us. It's a big plus for us.

On the federal side, first I'm very pleased to announce that Rich McComb, Director of Security DHS, has been named as the new DHS Vice Chair, our Committee's Vice Chair. I appreciate Rich's commitment to this Committee as always. With that said I want to thank Charlie Rogers for his excellent work that he has done as the Vice Chair. Charlie will remain with the SLTPS as the alternate.

We have a new member from the Nuclear Regulatory Commission, Sabrina Atack, Director. Division of Security Operations Office of Nuclear Security and Incident Response. We also have a new member and alternate from the Federal Bureau of Investigation. Angel Catalan, Section Chief, Security Operations Section, FBI Security Division, is the new member. Scott Gerlach, Unit Chief, Redstone Security Unit, Security Operations Section, FBI Security Division, is the alternate.

I must also report that there are two federal vacancies on the committee. The Department of Energy longtime member Mark Brooks is no longer with the

DOE. So, we need a replacement from DOE. The Department of Defense, the DoD slot has been vacant now for nearly a year. That's not acceptable. I don't know whether Mike Russo is on the phone or not but Mike we need to take care of this.

I mean, DoD, we're the 17th biggest country in the world. We're a nation. So, we need the DOD's participation in this. Again, I'm anxious to have these openings filled as soon as possible.

What I am going to do because we're on the phone, I'm just going to take a quick roll call here. And when I mention your name or speak your name if you would be kind enough just to say yes or here. The first name up is Rich McComb, DHS Vice Chair.

Rich McComb: Yes, Rich McComb is here. Thank you.

Mark Bradley: Hi, Rich. (Charlie Rogers, DHS alternate?

Charlie Rogers: Yes, I'm here.

Mark Bradley: Great. Darrell Parsons, NRC alternate.

Darrell Parsons: Yes, I'm here. I hope you can hear me.

Mark Bradley: I can, Darrell. Thank you. Perfect.

Darrell Parsons: Thank you.

Mark Bradley You're welcome. Mike Russo, DoD observer.

Mike Russo: Yes, I'm here.

Mark Bradley: Thank you, Mike. Valerie Kerben, ODNI, member.

Valerie Kerben: Good morning. I'm here. Thank you.

Mark Bradley: Hi, Valerie. Leo Masciana, State Department, member.

Leo Masciana: Good morning. I'm here.

Bob Skwirot: Hi, Leo. Kate Connor, State alternate.

Kate Connor: Yes, good morning. I'm here.

Mark Bradley: Good morning,(Kate. Glenn Bensley, DOJ.

Glenn Bensley: Yes. Hey, Mark, I'm here.

Mark Bradley: Hey, Glenn. How are you doing?

Glenn Bensley: Good.

Mark Bradley: Sidonie Dunham, Department of Transportation member.

Sidonie Dunham: Good morning. I'm here.

Mark Bradley: All right. Carolyn L., CIA observer. Okay. Mark Hojnacke, DOE observer.

Mark Hojnacke: I'm here. Thank you.

Mark Bradley: You're welcome. (Mark Sachs), SLTPS Vice Chair?

Marc Sachs: Marc Sachs is here. Good morning.

Mark Bradley: Hi, Marc. Jessica Davenport, SLTPS member. Tom Woolworth, SLTPS member. Tom Carr, SLTPS member. We've got a little bit of a shortage here on that side of the fence. Tiffany Kleemann, SLTPS member.

Tiffany Kleemann: Hi. I am here.

Mark Bradley: Thank you, Tiffany. Eric Tysarczyk, SLTPS member.

Eric Tysarczyk: Yes, I'm here. Thank you.

Mark Bradley: Thank you, Eric. Yes. Mary Michelle Schechter, SLTPS member.

Shelly Schechter: She is here.

Mark Bradley: Great. Meghann Teubner, SLTPS member.

Meghann Teubner: Good morning, everybody. I'm here.

Mark Bradley: Great. Debra Ann Winsor, SLTPS member.

Debra Winsor: Good morning. I'm here.

Mark Bradley: Great. Is there anybody that I missed? Any of the participants who would wish to identify themselves before I turn this over to Greg Pannoni? All right. Hearing nobody, I'm going to introduce Greg Pannoni, my Deputy. Greg is the SLTPS Designated Federal Officer. He's Associate Director for Operations

and Industrial Security, Controlled Unclassified Information of ISOO. Greg, you're up.

Greg Pannoni: Good morning. Thank you, Mr. Chair. And I want to go over the old business here. We had precisely six months ago our last meeting, January 29, 2020. And those minutes were finalized and certified. You should be able to access them on the ISOO Web site.

We had two actions from the last meeting. And the one is an issue that we've been discussing, those of you who've been on the committee know, for more than a year.

This concerned the ability to get SLTPS personnel who've been cleared through the FBI the data into the Central Verification System (CVS). And we will hear from the FBI this morning. I've been informed that we may have a breakthrough here in terms of resolving this matter. So that would be a great thing.

The other was related - the other action item concerned a similar thing, not quite the same, but we asked the ODNI to provide an update concerning the number of SLTPS personnel currently holding security clearances who have been cleared through the intelligence community. So, if you want to provide that since that's a shorter thing to cover I would ask Valerie Kerben to provide that update at this point.

Valerie Kerben: Sure. Thanks, Greg. Good morning, everybody. Luckily, I was able to re-engage with our CSO CIA and there was reconfirmation that from the community services group that handles the NT50 agencies for granting the TS/SCI they are unable to track the specific cases that are related to state, local and tribal.

So, for example if DNI submits cases to them because they are also our service provider, they are not tracking nor is it indicated that a particular individual might be a representative from a state or local jurisdiction. So, you know, our answer unfortunately is still the same. I tried to make headway but this is not something that is tracked or highlighted in their database in cases.

It's just according to what agencies, federal agencies, supplies it to them for them to process and grant SCI. And I believe and, of course, Rich can confirm that they all, once the Secret clearance is granted, they have that in their CVS database or if top-secret is granted it's in the CVS database.

But they can also grant the SCI for those who might need it and then they can relay that to Scattered Castles. But there is no specific number, I'm sorry to say, of IC cleared people to be recognized from the intelligence community.

Greg Pannoni: Does anyone have any questions for Valerie on this?

Mark Bradley: This is the Chair. Can you just elaborate a bit more on why it isn't tracked? Is it technically difficult to do? Is it some type of hurdle we could jump over or is this just a bridge too far?

Valerie Kerben: Well, you know, also numbers aren't always given out publicly of how many people are cleared. There's always, you know, sometimes aggregates. But at this point, I don't know if they're able to change the way they are tracking cases that come in from their, you know, agencies who use them to grant the SCI.

Mark Bradley: Okay.

Greg Pannoni: Okay.

Valerie Kerben: And, Greg, I know this has been a question but, you know, there isn't at this time a way to have that capability to reflect how many cleared people through the IC intelligence community for state, local and tribal.

Greg Pannoni: Okay. I understand. Unless there are any other questions with respect to this point, I'll turn back to the first issue and the FBI supplying clearance data on SLTPS personnel to the CVS. And I believe Earl Camp, I heard your voice, would you be able to provide that update, please?

Earl Camp: Yes, absolutely. So Earl Camp with the FBI. So we've consulted with our Office of General Counsel and we've been cleared to share the information. So now it's more of a technical question than anything else. And we are already engaging DCSA to create a bridge so that we can pass that information on a monthly basis. Marie Bernoi, are you on?

Marie Bernoi: Yes, I'm on the line.

Earl Camp: All right. Marie, if you could update the technical piece and maybe give some anticipated dates on when we can facilitate that passage as a result of the meetings between the technical folks on our end and the technical folks at DCSA.

Marie Bernoi: Sure, absolutely. So again, this is Marie Bernoi with the FBI Security Division. I'm in charge of our IT portfolio team. So, since February we've been actively engaged with DCSA on what it would take for us to prepare this data feed with the SLTPS Task Force officer clearance and investigative data.

So, we met twice in February and once in March and then we did have a bit of

a COVID hiatus. We met again recently in June and a follow-up meeting is scheduled in August. So, our team has been actively working for sure that the appropriate data is available in our Phoenix system and our development team is in the process of creating a script that's going to create the file that then will be uploaded to NP2 within the DCSA system.

So, we anticipate that during August and September, more likely September, that testing will occur between FBI and DCSA. And we are prepping for a go live in Q1 of FY21. That concludes my update.

Greg Pannoni: Thank you. Excuse me. Thank you. Anyone have any questions for the FBI?

Mark Bradley: Greg, this is the Chair. I want to thank the FBI for really going to bat for this. This is extraordinarily important. Thank you, Earl. in particular for everything that you've done and your technical folks. I also want to thank DHS, too, for its help in this. So, again, this is, in my view, a good government solution. It's important to the security of the country. So, again, thank you all for what you've done.

Greg Pannoni: Okay. Anyone else questions on that point? I did want to just briefly on that second item with respect to the intelligence community data on security clearances for SLTPS personnel.

I think we're going to still have to revisit this, it is my suggestion because as I understand the executive order there is some language in that 13549 order about the maintenance of a database for this population of cleared people. So, from what I'm hearing, I don't know that we're able to satisfy that requirement at this point. So, I think more work will need to be done.

Valerie Kerben: Greg, this is Valerie. Well I mean we could start thinking of another way to

achieve this. Maybe ask those agencies how many they submit to the IC. But we have to also remember that if there is a way to do it then some of these things would have to be done in a different forum and not a public forum. So, you know, but maybe we can think through other ways of trying to achieve it but it's not achievable at this time through their current database and able to give specific numbers.

Greg Pannoni: I see. So just to be clear on this point, Valerie, am I understanding that the total number of IC cleared SLTPS personnel would be considered classified?

Valerie Kerben: Well I don't think that point is. I mean, we have to go - we have to ask the CIA. And I know someone from the CIA is on the phone, but I'm not sure what group she works with. But from what I established with the community services group there is not always a publication of cleared personnel and, you know, attribute them to where they're working.

Greg Pannoni: Okay. Well...

Mark Bradley: Greg, this is the Chair. Let's do this. Let's just table this for now because again obviously nobody is back where they need to be or at least not there enough. And then what we can do is when we finally do get back we can have a meeting in our SCIF and drill down deeper in this because again I think this is another important issue. I don't want to let it go but I'm also sympathetic to what we're facing now. Som, let's table it.

Greg Pannoni: Sure.

Mark Bradley: Let's sideline it. Let's take a knee for a bit. The game isn't over.

Greg Pannoni: Okay, Very well. Moving on the third item - there were the two action items.

But we also had a meeting of the cyber threat information sharing working group. We had one actually before the last SLTPS-PAC meeting. And then we had one subsequent to the last meeting and that was in May.

So, this is an issue that was brought up by our State Department representative initially, the concern being that there needs to be greater, more robust sharing of cyber threat information with the SLTPS community. So, the interest here - and this falls right in line with the Committee's purpose both to remove undue impediments to sharing information and discussing policy issues related to the classified national security information program. So clearly the first purpose of the Committee is intended on this very point.

We had a discussion. And I'll say that the primary interest of the community is the access to the threat information as opposed to the source or method for obtaining that information. And in particular, information that is actionable. And so we had a robust discussion.

There were a number of subject matter experts, stakeholders that attended this meeting we had in May: DHS, ODNI, NSA, U.S. Cyber Command, Air Force, Army, Navy and the private sector, of course. And in general, we were trying to gain an understanding surrounding the issues of sharing cyber threat information and the needs that the private sector participants outlined and also the concerns the federal government participants discussed and the processes and the challenges.

So, the private sector emphasized the need to get timely information to the asset owner community in an unclassified format whenever possible because it is often shared with technical staff and security staff that have no clearance at all.

Some private-sector participants spoke of their past experiences when they were embedded in the (NCCIC), National Cybersecurity and Communications Integration Center, where representatives of a number of critical infrastructures were able to share information with, and review information, up to the TS/SCI level from intel and law enforcement agencies.

And they looked at that as a model for information sharing as it provided a sector-specific perspective that aided in the identification of information of importance to the sector and fostered the development of relationships that helped to facilitate sharing.

The federal participants indicated that they recognized the information must be relevant and actionable. And they emphasized that to sort through millions of pieces of information is critical for everyone to understand what is important and why in order to work through the classification issues to get the information sanitized down to the appropriate level where sharing is less restrictive.

So there may be a baseline of information that is needed to indicate something is happening that can be shared at either the unclassified level or the controlled unclassified information level. And then additional people with higher clearances may receive added background information if necessary. So ,as I said, our State Department representative (Leo Masciana) was the one who called for this group and he approached the issue from the policy perspective.

And while there - he questioned whether the classification system helped or hindered the sharing of cyber information. He talked about ways to leverage the current policies.

We also heard from our DHS rep during the meeting that suggested was before we engage in complex long term actions like amending executive orders, it's necessary to understand what's causing the situation to exist and search for lower-level solutions. So, the DHS rep emphasized more work was needed to be done in identifying the problems.

And there was additional discussion about the need to more clearly define the problem and identify solutions that aim to better implement existing policy. So, at this point, we will have a briefing coming up here from Miss Alethea Madello, who was at the meeting and I invited her to this meeting. She's from the office -- DHS Office of Intel and Analysis -- who's going to provide an overview of activities related to information sharing.

But before that, I wanted to ask if our State Department Rep., Leo Masciana, our SLTPS rep to the (unintelligible) and Charlie Rogers from DHS if there's anything else they would like to add with respect to the discussions from that cyber threat information sharing working group.

Charlie Rogers: Go ahead, Leo, and then I'll go.

Leo Masciana: Ok. Leo Masciana, State Department. Originally, I pressed for the working group based on several national-level priorities established through the National Security Strategy Cyber Strategy and other important National Security Council related documents that outline that there is a problem and that it needs to be solved urgently in order to protect the nation's cyberinfrastructure and government cyberspace activities.

I was heartened to see that so many of our cyber defenders and agencies that deal primarily and inform us with cyber threat. This discussion and participated -- as you said Greg -- robustly in a dialogue. My concern now is

that that we continue to press forward with continued dialogue, perhaps in this working group format that we've started so that, you know, we can get to a set of recommendations for the chair that may be feasible in the short run as well as perhaps some longer-run policy reform recommendations. So I'll leave it at that. Marc?

Marc Sacks: Yes, Marc Sacks here. Just a bit of a comment from one of our ISAC members who participated I think resonated with many is that we get a lot of great information from the government that has been rapidly declassified. But we still have a problem of figuring out which is the most important because as you can imagine an asset owner is getting not just government info but also private sector info coming from various alerting sources. But the government could help.

Just for example, if you're having a briefing -- say with the FBI or if you're a fusion center or (unintelligible) or wherever you might be -- faced with multiple threats and challenges to look at an indication from the government about which one you need to worry about, whether it's helping with the prioritization and then maybe providing some context as to why this particular incident or this event or this action or activity is more important than something else, which would then help the private sector asset owner prioritize their own investigation or their own reactions to something that's going on.

That does border a bit on classification, of course. But the key thing here is to make things actionable, to provide some context, and to help the private sector prioritize. Because again, they're being overwhelmed with so much information.

.

Greg Pannoni: Charlie? Charlie Rogers?

Charlie Rogers: Yes, I just have a few comments. I don't disagree with anything that anyone has said thus far. I do think, you know, the first meeting there was a fair amount of tension about the problem, but the problem was kind of anomalous and big. And I think there is a lot going on in the government that we may not be aware of to share information.

And I'm not saying that it's - we're entirely effective or ineffective, but I think there is a lot going on. So if this moves forward in meetings, I think we really need to take some time to articulate in some detail the nature of the problem and recognize what is being done effectively before we jump immediately to formulating solutions.

I think there probably needs to be some solutions, but I think they should be informed with a little more detail and granularity about the nature of the problem. And that's really all I have.

Greg Pannoni: Okay. Fair enough. Anyone else have any discussion points on this?

Rich McComb: Hey, Greg, this is Rich McComb, the Vice-Chair and DHS Chief Security Officer. I agree with Charlie. The one thing that I would add, I think an effort to kind of establish what the as-is picture is. All the - in other words, all the current methods by which classified is provided to the private sector.

As you well know, obviously, there's not only the executive order 13549 but also 13691 and any number of other venues. So, I think one of the first things I would recommend is that there's a good handle on exactly what is being done today, to Charlie's point. I think there are a lot of venues. They may be underutilized at this particular time.

Greg Pannoni: I agree.

Mark Sacks: And this is Mark Sacks. I'll be happy to help with that, because from the private sector's perspective while the government may feel that a lot is being made available, the private sector has a different point of view. And so it may just be perspectives in terms of believing that a lot is being shared.

And then those who are looking for the sharing either not knowing where to find it or it's just it's not timely, for example. But I'd be more than happy to help from the private sector side to bring that viewpoint in.

Greg Pannoni: All right. I appreciate that, Marc. I think, though, it would be (unintelligible) as-is foundation of here's the mechanisms that we have. But I recognize like so many things, you know, we have policies, we have mechanisms. But how effectively are those mechanisms being actually carried out? So - but we need to start with the landscape of here's - here's what it looks like in terms of what we already have in place - these mechanisms.

I think that that will be - I don't know if it's going to be enlightening to some, but at least it level sets. And we all can see here's - here's the things we already have established. How well they're being actually carried out is a question mark. I understand. But that would -- I believe -- would be a worthwhile thing. So...

Marc Sachs: That's a necessary starting point. Agreed.

(Greg Pannoni): Yes. Yes.

Mark Bradley: And Marcus, this is the Chair. Is one of the complaints that you're not getting enough finished intelligence? I mean, stuff that's already been analyzed? And then also, too, are you also lacking a prioritization of the threats that you're

facing?

Mark Sacks: Yes, the prioritization is one of the key areas along with timeliness. Processed and fully analyzed, you know, well-written reports it took six months to write is nice to read but doesn't do anybody any good in a timely fashion. And this is what the asset others -- particularly for the critical infrastructures-- are (unintelligible) for. It's something right now.

In the physical world, if the FBI were investigating some, you know, white-collar crime or the local police department were looking at burglars and so forth, those asset owners would be updated almost in real-time as to what to look for. You know, the white Ford truck kind of thing.

Mark Bradley: Right.

Mark Sacks: In cyber we don't do that. And I think that's the piece they're begging for is timely information and actionable, not so much processed and analyzed. But take weeks or months to put together.

Mark Bradley: Okay, thank you.

((Crosstalk)

Greg Pannoni: No, good. I was just going to ask if anyone else had anything they wanted to comment on with respect to (unintelligible).

Eric Tysarczyk: Hey, guys. This is Eric Tysarczyk: in the state of New Jersey. I just wanted to...

Greg Pannoni: Go ahead.

Eric Tysarczyk: Thank you, sir. I just wanted to follow up on the point that I think Charlie made from the state perspective. And I'd be curious if my other contemporaries-- especially from the Fusion Center -- see this. I think it's correct to kind of outlay the problem.

Anecdotally, a challenge we've seen with our private sector partners, the FBI -- especially their field offices -- and DHS have been great partners in sharing information as timely as they can. But if something comes in, let's say, that they have classification wrapped around it and it's an indicator of compromise or something along those lines that our private sector, as well as us as a state, are also doing from bodies like MS-ISAC or the like.

The challenge really is -- and whoever used the Ford Bronco example is exactly right -- the challenge is sometimes when that comes down classified there may be an indicator of compromise with some remedial actions. But some of the technical folks -- both in the private sector and at the state level -- are looking to discuss what those variants may be.

And so sometimes while they don't need sources or methods, they may need a more in-depth discussion about if this is the indicator of compromise. We know that there are variants that could be exploited from say the Windows Exchange server or something along those lines. And having that timely discussion in the regional level that are connecting directly with some of the technical folks at the private sector at the state.

That's kind of where the delay comes in because some of the field reps may just have a classified report and they're following up from the initial alert that went out. So as we're trying to identify the issue, that timeliness of being able to have a discussion where the private sector or the state may not be looking

exactly for sources and methods but may need more information to better secure their system, especially in those critical infrastructure providers in the lifeline sectors to have discussions on variants that sometimes may be precluded because of the classification.

So just - hopefully, that helps kind of outlay the problem because it's something we've seen in New Jersey.

Mark Bradley: Thank you, Eric, that was helpful. And again, this is another one of these important issues. And I think that both sides - (unintelligible) is exactly right. We do need to identify the problem a little better. Then sit down and try to structurally figure out what we can do about it. In my view, this is what the SLTPS-PAC is supposed to be doing. Exactly what it's supposed to be doing.

Mark Bradley: (Unintelligible). Shall we turn to the meeting … ?

Greg Pannoni: Yes. I mean, if we're re-ordering we talk about it would be natural flow if Alethea Madello is on the line to give her update.

(Greg Pannoni): Yes, let's (unintelligible) first. (Alethia), you were a director of state and local partner engagement field operations? Also of intelligence and analysis, DHS, and will give us an overview of your information sharing activities. Okay? The floor is yours.

Alethea Madello: Absolutely. Thank you, sir. Good morning members and other participants on the call. I am the (Alethea Madello) with DHS I&A, Partner Engagement, State and Local Programs. What I heard from a lot of you is to understand there's a keen interest to understanding what information-sharing capabilities are currently in play.

And so I'm glad - I'm going to just take maybe five to seven minutes to really explain to you what opportunities are out there not only important state and local but also supporting private sector. And I'm happy to say for the last - increasing over the last two years, I&A has done a robust job at supporting our external stakeholders within the state and local arena as well as the private sector partners.

I want to start with talking about the branches within field operations division within I&A that are accessible to state and locals and private sector. And so you've met you mentioned in my title Field Operations Division. Typically, we have deployed personnel throughout the country which are your intelligence officers around the country, typically located in your state and local fusion centers.

That is your - that is the private sector as well as the state mobile's first point of contact to support your information needs. If there are any questions about how to actually get in contact with your DHS -- Department of Homeland Security -- Intelligence Officers around the country, please let me know. I can follow up and provide assistance to that.

I heard a few different things. I heard a few different things on this call and I wanted to make sure in addition to talking about the other programs that - or portfolios that exist within I&A, I wanted to highlight that the field operations deploy folks. A few of you mentioned critical infrastructure and timely and actionable information and access to classified information. My portfolio is specifically state and local.

But I do have a good understanding of how our private sector partner engagement branch liaises with the cybersecurity infrastructure and agency within the department. Their acronym is called CISA. And they have the

primary role of working with private sector partners to provide timely intelligence.

I mean, not intelligence but threat information associated with cybersecurity incidents. The great thing is I&A's private sector works in tandem with that agency to host the classified intelligence forum.

And were that - what that is is I&A has worked with the 10 or so - 10 and 12 sectors to bring together those sector partners and provide security clearances so that they can work with I&A and CISA to develop products - actionable intel products - that would support depth and breadth of understanding of issues percolating within the critical infrastructure arena.

And so I think on the previous call I briefed about the classified intelligence forum. And while currently, we've been in this pandemic we have not hosted any classified intelligence forums because it requires that those meetings occur in a – SCIF-ed environment.

I'm happy to say that we re-energized that program and that we've figured out some particular ways to have an unclassified intelligence forum where we bring private sector clear partners together with our analysts to develop products to meet the need that you just mentioned exist.

And so if you need some additional information or you'd like to get some clarification of who your points of contact for the various sectors are. Please feel free again to reach out to me. Tammy Hutchinson of I&A is the Director of the Private Sector Engagement Branch and the Classified Intelligence Forum is run out of that branch.

And we've seen some great success as it relates to updating our state and

locals and our private sector partners about threats that are facing the cybersecurity infrastructure, intrusion alerts, and so on and so forth.

In addition to that, I did want to mention the Homeland Security Information Network HSIN -- as we call it -- is the Department's platform where various communities of interest interests are set up to address and to share information. That's our primary infrastructure.

And so HSIN critical infrastructure -- is called HSIN CI -- is a platform where private sector partners have access to unclassified intelligence and information that comes from I&A and other appropriate entities from the Department, as well. In addition to that, I&A also sponsors - so HSIN is actually HSIN CI is actually sponsored by this CISA, the component I just mentioned. And that is the appropriate community of interest for the private sector partners to access a lot of the products that come out of I&A that support their understanding of time - their need of timely access to intelligence and information associated with cybersecurity issues and a myriad of other issues.

In addition to that, we – I&A - actually hope that HSIN intel community of interest where that actual portal is open to state and local law enforcement intel professionals. That, too, is a community of interest where I&A shares a myriad of different products.

Not only I&A but other federal partners. And the fusion centers as well. And so again, that infrastructure has been in place for several years now. Initially, about five years ago we took a hard look at the metrics of how effective and efficient that system is.

And we've made some significant upgrades to make it user friendly, to make it more accessible, and more to suit the user needs. And so, I would encourage

folks if you have any questions about the HSIN platform, which community of interests best suit you, please reach out to me and I can coordinate your access with the appropriate COI.

In addition to that, you know, I&A has a myriad of different portfolios that at the national level state local organizations and associations, as well as the private sector industry organizations and associations. I'll pause there and kind of see if there are any questions about the existing infrastructure in place, whether it's the field-deployed personnel, the I.T. system -- which is HSIN -- or our office and kind of individual portfolio that we support.

Meghann Teubner: Hi this is Meghann from NYPD. How are you? I am...

((Crosstalk))

Meghann Teubner: Hi. I just wanted to give you guys and CIFA specifically kind of a shout out for these bi-weekly unclassified cyber threat briefings that they're hosting every Friday. We have found them very useful on our end of just kind of getting pointed in the right direction of products that would be of interest either to us or to our information technology bureau with the NYPD or New York City Cyber Command.

And so we've really - we've really appreciated the information that has come out in those phone calls to include in some cases they've been providing data on kind of emerging current threats that the community is looking at, including, you know, foreign influence threats and cyber threats from China.

So I just wanted to give you guys a shout out on that. Those have been really, really helpful and have helped kind of direct my analysts to the right places on HSIN intel into kind of good documents to review and share on this end. So, I

wanted to thank you for that.

And along those lines and kind of the cyberthreat lines, I think both DHS and FBI have been doing a pretty good job of pushing threat actors and kind of the -- what are they -- advanced persistent threats -- the APTs -- and some of the tactics that are being used out in a more timely fashion, to include like compromised IP addresses so that we can ensure that we're protecting our infrastructure here both at the HYDA and the NYPD.

So again, you know, they're baby steps. And I understand that there is, you know, there's always going be a challenge of getting the kind of more detailed classified information out to a wider audience. But over the last couple of months -- especially during the COVID pandemic and the lockdown -- I have been really happy to see the amount of information from both DHS and FBI that's getting pushed out at the unclassified UFO you level. So I just wanted to kind of take a moment to thank you guys for that.

Alethea Madello: Perfect. Thank you. We always love to hear that the mechanisms that we have in place are working and that you're finding them valuable. Just for the group, what she's speaking of is I&A hosts a bi-weekly cyber call that has state local and private sector partners on to provide a threat - a threat brief, if you will, of emerging topics and issues.

We've been doing that for a few months now and I'm glad to hear it being successful. She also mentioned that her state local analysts are getting timely intelligence and information through the infrastructure I mentioned which is HSIN. Specific to state and locals, HSIN intel is a community of interests where that information is made available to them.

HSIN CI is a different portal and it has all the same I&A data, but it doesn't

have some of the other noncyber related intel and products on that - on that COI. However, private sector partners are eligible for HSIN CI community of interest. And again, thank you Meghann, for giving us a shout out. I'll make sure I reach out to the Cyber Mission Center and let them know that they're doing a great job

Meghann Teubner: Great. Thank you.

Alethea Madello: Are there any other questions? Yes? All right, well thank you so much for allowing me to give you an update. If you don't have any other additional questions for me, I'll just turn it back over to you and drop off. Charlie Rogers knows how to get in contact with me if you guys have anything additional for DHS I&A.

Greg Pannoni: Hey, could I just...

Mark Bradley: Go ahead (unintelligible).

Greg Pannoni: Hey, Pannoni, ISOO. Thank you Alethea, for the briefing. I wonder - you did refer to the CISA -- the Cybersecurity Infrastructure Security Agency -- and just trying to get a little bit more insight and more granularity in terms of their interaction.

And as we heard before, in terms of timeliness and priority of actionable information that they have and - now I realize you may not be the person to speak to that. But you did mention interaction between intel and analysis with them. Is there any more that you can say about CISA and their interaction, particularly - you know, with not just state and local but with also with the private sector partners?

Alethea Madello: So hi, how are you? How about this? I think - I believe it's probably pertinent at this point for me to coordinate a speaker from CISA to come to this body and really give a nuts and bolts detailed briefing on how they engage.

Because I do know -- and I don't want to speak out of turn -- but I do know that they have several mechanisms by which they work with the ISAC and they have the NCCIC that kicks out all these different alerts and messages, as well as managing the HSIN CI portal. But I think - it appears that there are a lot more questions you guys had that are geared to what they're doing specifically and it may behoove this group could coordinate a briefing from them. Can I...

Greg Pannoni: And I completely agree. In fact, we may want to not wait six months and have some sort of a special meeting where we invite them to talk about it. But I'll defer to the chair on that.

Mark Bradley: Well, that sounds like an excellent idea, and also one that's important. So we can work on that and try to do something, perhaps the fall.

Mark Bradley: Well thank you again, (Althea).

Altehea Madello: All right thank you, guys. Have a good afternoon and if you need anything, please feel free to reach out.

Mark Bradley: Thank you so much. Next, we're going to turn to Charlie Rogers, Director of Compliance, Standards and Training Division, Office of the Chief Security Office, DHS, to talk about COVID and personal security updates. Charlie, the floor is yours.

Charlie Rogers: Thank you, Mark. Good morning everyone. Regarding getting a speaker from

CISA, we would welcome assistance from Alethea, but also I think Rich McComb will probably be engaging with CISA as well to see if he might be able to identify some key persons. I'll work with him on that and get back with you all. Normally in these meetings, I sort of give an overview of what we're doing with our direct security support to fusion centers.

So, most of you are familiar with what we do. I'll try and summarize briefly without telling the full story. We do have a team that's engaged out of the DHS Office of Security that supports more than 80 fusion centers. We provide direct security support, certified secure rooms that are certified for the deployment of a classified secret network. And we also perform oversight - training and oversight.

So, what I'm going to talk about briefly today is a little bit about how COVID-19 has impacted some of our program. When we first went to basically nearly 100% telework and travel was suspended, we had no idea that the - that it would last this long. So we were, you know, we were innocents thinking that we'd be back to work in four to six weeks.

In any event, what we did initially was just to go through our program, polish our checklist, update our policies, procedures, revalidate what we were doing in anticipation of traveling. Well, that didn't occur. What we've now done is we've begun to implement what we call remote or virtual audits.

We did three last week. We initiated three audits last week. We're doing another two this week. We anticipate doing another five in August. And we hope to complete a total of 11 by the end of this fiscal year. We had already done five in-person audits where we traveled to the fusion centers. So, these virtual audits cannot duplicate the scope or depth of a - of what would, you know - an onsite visit. But we believe they're important because they do

enable us to work directly with the security liaisons.

We review our own internal data when we do this. We engage with the security liaisons. We have them complete a checklist. They provide us data. And then we have a virtual online meeting with them to go through the results of the checklist. So, we're evaluating this process.

As I said, we - we develop checklists. We just implemented it last week, and we're doing it again this week. So, we're not sure we have it right yet. We're - we're - it's a work in progress but we expect to complete a combination of onsite and virtual audits that will meet our previous schedule which was to be 16 for the year.

There's a certain level of excitement in the team in that we now believe that once we get past COVID and travel does get re-instituted that we certainly will move forward with our traditional security audits. But we may end up supplementing those audits with these virtual audits which would enable us to reach more fusion centers within a given year than we had been in the past when we were operating strictly from travel only.

So, there's act - we anticipate there'll be a benefit from - overall benefit from the challenges that COVID placed on us. One of the things that are impacted by doing virtual audits - remote audits is just the ability to meet with people, the ability to go into these secure rooms to identify changes that may have occurred.

And our normal onsite visits usually lasted three to four days and included providing multiple training sessions on security. And so that's really difficult to do to the remote virtual audits but we still believe it's a benefit. And I think I pretty much covered where we're at on that. There may be some - some

questions on it...

((Crosstalk))

Mark Bradley: …Charlie, this is the Chair. When you do your remote audits, what's the level of classification?

(Charlie): It's unclassified. It could be sensitive, but we can - initially we go into our own records and we look at the documentation, past audits, previous inspections, findings and we - we validate that. Then we reach out to the security liaisons which are our primary point of contacts and go over the checklist and the type of data we want them to go through. And then the final phase is the validation phase in which they send back the data and we set up a conference call and go through their findings and discrepancies.

But it's not classified. If we were to reach that threshold then we would end up having to - to go back to using a classified system. But...

Man 1: It is sensitive.

Charlie Rogers: The other thing I wanted to bring to everyone's attention is just those - kind of the status of the fusion centers over the last several months. The team has found that about 90% of the fusion centers are working under a kind of a reduced operational tempo.

And there was a - for a while there, there were five fusion centers that virtually had no one. They had someone in there, but it would be, like, a very small staff once a week would be going in. They were still validating the alarms and checking the secure rooms and that kind of thing.

But they still remain impacted. So, a lot of them are doing exactly what the federal government is doing. They are teleworking or they have a large amount of the staff that is on telework. So that's another impact that we've had with them.

And that pretty much summarizes what we're doing with the - under the COVID impacts. We're still reaching out to them primarily on a weekly basis. At a minimum, it's every two weeks. We try to reach out to them on a weekly basis to get their status -- their operational status -- and they go over any concerns they have about the secure rooms.

And they're impacted the same way the federal government is. They're trying to figure out how to operate effectively in this environment. Are there any questions on our oversight or on how we are operating now?

I'll just go over a few brief, rounded off metrics for you. I normally do for our personnel security metrics. Currently, DHS has about 3,000 of cleared private sector personnel that we have directly cleared, and we have about 5,800 state local tribal personnel that we've cleared. So that's a total of about 8,800 personnel. They're primarily cleared at the Secret level.

At the TS and TS/SCI access we have about a total of 700 people. Not all of those people have TS/SCI, but between TS and TS/SCI is approximately 700 people. And the - those that have access to TS/SCI is roughly about 125 to 150 are in the private sector and about 250 are in the state-local arena. And that pretty much summarizes where we're at on the clearance. Are there any questions -- anything I can answer?

Mark Bradley: Thank you, Charlie. That was a nice summary...

((Crosstalk))

Charlie Rogers: Thank you.

Mark Bradley: Oh, you're welcome. Next, we're going to turn to Devin Casey of my staff to give us an update on the Controlled and Classified Information Program. Devin?

Devin Casey: Thank Mr. Bradley. This is Devin Casey from the Information Security Oversight Office and I work on the Control and Classified Information Program. Thank you all for inviting me to give an update on the CUI program. First, we did issue our 2019 Annual Report.

The CUI program does have a section in that report. Key bullet points from that section - most agencies will be issuing policies by the end of this calendar year which is kind of a big step toward implementing their CUI programs. Most of the other dominoes fall pretty quickly after that one.

As such, we've seen pretty significant progress by agencies to implement due to both this progress but also some varying timelines and concerns about the timeliness of the implementation of the program. We did issue deadlines for implementation of the CUI program that were put out an ISOO notice this year - or CUI notice this year.

Another bullet point in the Annual Report -- and something that we've been working with a couple other committees -- one with the National Insider's - Insider Threat Task Force and another working group at OMB is insider threat considerations for CUI.

In the report we acknowledge that there - there are insider threats to CUI -

many different categories face either similar or differing threats based on the type of information that they are, and that agencies are looking towards policy solutions to help them address those threats. So, it's something our office has been working with both of those entities for.

Another piece of policy that came out as a draft was issued by NIST the National Institute of Standards and Technology. NIST 800-172 -- formally known as NIST 800-171B -- which is additional controls and enhanced security requirements for protecting controlled unclassified information, and can be used as a supplement to NIST Special Publication 800-171.

The regulation is intended to address certain situations where CUI may be associated with critical programs or high-value assets. And that those high-value assets and critical programs are potential targets for advanced persistent threat. The controls in this 800-171 are designed to address differing advanced persistent threat based off of threat reporting from those either critical programs or the high-value assets as identified.

So, it is out for draft public comment. Comments are due by August 21, 2020, and can be found and submitted on the NIST website. So, you can look up the NIST 800-172, or you can go to our CUI blog and you can connect to the place to make comments there.

Another big event in the CUI program is actually kind of just closed for comments. So, if you send them in, they will likely review them. As a work-between, the CUI Advisory Council, the CUI Office, and the National Information Exchange Model, or NEIM to create a CUI metadata standard.

Now it's a standard not the standard. CUI does not require metadata marking, but what we did want to do is work with this entity to create an environment

as well as a reflection of the CUI markings and a metadata standard to facilitate information sharing where possible, and to provide a template for agencies or non-federal entities to use as a marker receiver, or plan to share or receive CUI information in a metadata-required environment.

So, we do imagine that will many agencies will voluntarily apply those standards, or use those standards, or reference them in the creation of similar standards. So, it's not the standard and it is not required. However, it is a good place to start and look for CUI metadata markings.

It did just come out that NIEM released 5.0 Beta 1. It did just closed for public comment. But as mentioned if you do send some comments and it is likely that they will still get to us. NIEM had mentioned that they were going to keep it open for about another week or two.

So please feel free to - to take a look at those. Those are something that's important to you. I know a lot of entities are considered - concerned about or - or thinking about when the CUI FAR case is going to come out. It did get updated in the unified agenda. And the current comment period it's predicted to be from October to December of this year.

Again, that's an estimate and it's subject to change. But based off of GSA's internal predictions for policies, that's when they predicted that this - the CUI FAR case -- which will expand the CUI requirements to the executive - entire executive branch that falls under the FAR -- will come out for comment. Again estimated October 20 to December - October 2020 to December 2020.

For more information about the CUI program or to stay up to date on elements occurring in the CUI program, please join our CUI blog. You can get there from our website which is archives.gov/CUI or you can look up to CUI blog --

it's ISOO.blogs.archives.gov.

There you will see an advertisement for the CUI Stakeholder - Quarterly Stakeholder Meeting which will be August 19 from 1:00 to 3:00, as well as advertisements for things like our CUI training class that we just did July 23, and other elements in training and good information about the CUI program.

Those stakeholder meetings are open to anyone. They're performed over Webex (unintelligible), and all you have to do is be a member of the blog - or follow the blog to call in. And that's it for me, Mark.

Mark Bradley: Thank you, Devin. And any questions for Devin?

Leo Masciana: This is Leo. State Department.

Mark Bradley: Hello, Leo.

Leo Masciana: You mentioned issuing deadlines for implementation earlier.

Devin Casey: Yes.

Leo Masciana: Would you clarify if - particularly any hard deadlines?

Devin Casey: Yes, of course. So, our office issued a CUI notice that updated the formal notice about implementation to CUI program. CUI Notice 2020-01, and it's called CUI Program Implementation Deadlines. And in it you'll see a series of dates for when different activities should be completed by an agency as far as the implementation of their CUI program.

Agencies do have the option - well, agencies that are going to be missing the

deadlines or not meeting the deadlines are required to report in their annual report to our office what their timeline is, what the cause of the missed deadline is, and when they will be meeting those requirements including a plan for how to reach implementation of that part.

((Crosstalk))

Devin Casey: So, the actual dates are in CUI Notice 2020-01.

Leo Masciana: A particular question that keeps arising is when it's permissible to begin using the label - CUI label on documents.

Devin Casey: Yes. So, the CUI marking can be used on a document once an agency has implemented and allowed for the use of the CUI marking -- and generally, that comes after both the policy are completed and training are completed -- is when we generally consider an agency is likely to start marking.

Some agencies have already begun marking. For instance, Department of Interior does have the CUI material that they mark and control as CUI currently under their CUI program. Other agencies have followed suit as well. So, it really depends on the agency.

During that time when some agencies have the CUI program and others do not continue to use your Legacy programs to protect your sensitive information. And if you receive CUI from another agency, use the most equivalent of your Legacy programs to protect that information as you're implementing the CUI program.

Other agencies' CUI programs have been instructed if they receive information from an agency that uses Legacy markings but they've

implemented the CUI program to protect that information under the CUI program for now.

Leo Masciana: Thank you. That's very helpful.

Mark Bradley: Good. All right, Devin, thanks a lot. That was outstanding. Well, we're not going to move into our general open forum discussion. But before we do that, I'm going to ask our new SLTPS-PAC members to talk a little bit about themselves. First, I'm going to turn to Mary Michelle Schechter, Director of the Division of Community and Maternal Child Health, Nassau County Department of Health, New York. Mary, you're up.

Shelly Schechter: Wow, good morning. First of all, I commonly go by the name Shelly. Mary Michelle Schechter...

Mark Bradley: Okay.

Shelly Schechter: ...is a handful.

Mark Bradley: Got it.

Shelly Schechter: I'm Director of Community Health and Maternal Child Health here in Nassau County, Long Island. So, you can imagine how busy that we've been for the past six months or so. I just want to say I'm honored to be on the Committee. A lot of what's going on here has a good connection with the SLTTGCC which is the council that I serve on. And I think that there'll be a lot of value-added to connect those two. That's really all I have.

Mark Bradley: Well we're delighted to have you. And you bring a unique portfolio with you. And I can't say anything other than it's very timely. So anyway we're delighted

to have you. So, welcome. All right, next we're going to do Sergeant Debra Ann Winsor, Deputy Director Washington State Fusion Center, Seattle Police Department -- another very busy place.

Deb Winsor: Good morning. I'm Deb Winsor, and I am the Deputy Director of the Washington State Fusion Center, I'm also a 29+ year veteran of the Seattle Police Department. And we have been very busy. I've been involved with critical infrastructure efforts since the start within the Seattle Police Department post-9/11, and have been and - have - have been instrumental in implementing programs for critical infrastructure -- not only within the city but across - across the state.

And with current events, we have definitely been very busy both - not only with COVID but I've been - we - we deal with a lot of intelligence on the civil unrest side as well as - then the COVID response side, as well. So, it's been a challenging time. But I'm also very honored to be on this committee.

Mark Bradley: Well we're delighted to have you. And again, I mean - the way we kind of run this thing is make it as productive as possible. So, for both our new members, anything that you think that we're missing or that we need raise, please - please help us make this exactly what it should be -- a body that's aimed at protecting the United States. So again, we couldn't be more delighted to have you both. So, please, welcome.

Right now, open forum - Mr. Sachs, I understand that you might want to discuss a topic about access to classified information personnel working at home. Is that right?

Marc Sachs: Yes, Mark Sachs here from the private sector. I - I think it was discussed a little bit by Mr. Rogers from DHS, the - the issue being brought up is for those

who are working from home this is primarily a government policy issue but it does affect the private sector for those who have clearances is -- because of Covid-19 -- ready access to the (unintelligible) is not possible.

Take TS/SCI off the table for a moment, but I am aware that the DOD has been working on some policies for how to handle Secret level information literally in your home. And I'm just curious if other agencies are working on the same thing. And can that be extended to private sector asset owners?

We don't believe the COVID thing is going to disappear overnight. As most people are aware, this - this may be setting a new baseline for - for how we work in the private sector. And so be interested in insights there - for - for the future and this may be, you know, a future briefing item that we could look at for how do we handle Secret in a residential setting since the DOD is already working on that?

Mark Bradley: Anybody have any comments to Marc's point?

Ken Polk: Yes. This is Ken Polk, Office of Intelligence and Analysis of DHS. You know, the leadership within the - the office is looking at exploring the possibility of extending secure capabilities at home. There's going to be a lot of work to do, but I think collectively as a body there needs to be consistent policy or procedures established across the board. So, DOD is not doing one thing, DHS something else, and DNI or whomever doing another thing.

And I think from our exploration so far there's - there's not a whole lot of policy or procedures, or good practices to follow that have been identified. So, if anyone's got some points of contact on folks that are working this, I welcome that.

Darryl Parsons: This is Darryl Parsons with the Nuclear Regulatory Commission. I've read the media reports about DOD perhaps relaxing or finding a way to use some classifications or some information sources that are classified from a home location. The agency - my agency has - has taken a look at that. There are no current plans to do that. Although we are asked - are being asked to stretch our imagination a little bit.

We haven't come up with anything definitive but we do have some categories of information that potentially would lend itself to this and - and - and that it dives more into CUI in a specialized category that we have there. So, we are looking at that. But it - we have nothing definitive as of yet. That's all I have.

Man 2: Anyone else have any comments on this?

Mark Bradley: This is the Chair. I mean, you think this will be the subject of a working group or - or not?

Greg Pannoni: Sorry. Had to unmute my phone there. Greg Pannoni, ISOO. It may - may be. We, as you know, have engaged a little bit with DOD on this.

Darryl Parsons: Right.

Greg Pannoni: The CNSS -- the Committee on National Security Systems -- some of you may know that group -- it's inter-agency government group focusing on the policies for use of information systems. And I have to confess I need to revisit their policies and instructions and directives. But I believe they do already have some policies regarding remote access using mobile devices.

And maybe -- I'm a little bit of a Luddite -- I'll just call them dummy boxes. So there's the sort of two issues we've got the issue of remote access, and then

the issue of - potentially of storage. And those are two really different things. And if we're not talking about storage in terms of the ability to download classified information and stuff like that - but to your question, yes perhaps.

I'm not really certain one way or the other should - if this - I welcome if this group wants to have that discussion. I do - some of the comments. I share their sentiments that, you know, COVID probably isn't going away for quite some time. And so as far as being more - having more options for us to perform national security responsibilities, it's - there's - there is some good reasoning to - to have more discussion about how this could possibly occur and that - including as we're discussing it in this forum - the private sector folks, not just US government folks.

Mark Bradley: No, I - this is Chair. I think that's quite right. The main impact of COVID is going to echo for a long, long time. First of all, we don't even know how it's going to last now, but much less - it's transformed things. I think that's what Charlie was mentioning, too - that, you know, if it - now - if it certainly wouldn't hurt -- it seems to me -- to at least pull policies together and see exactly what they say now, what they permit, and more importantly, what they don't and start looking ahead a bit. I mean, if we don't then who will? So, you know, I think would be a timely and - and useful subject for us to at least begin to probe.

Greg Pannoni: Absolutely. I'm pumped. 100% on board. This is Greg, ISOO. Greg Pannoni.

Mark Bradley: Anybody else have anything they want to raise in our open forum discussion? You got - we're ten minutes ahead of schedule. So anything else we've missed, or should be thinking about, or people want to chime in on?

Rich McComb: Hey, Mr. Chair, Mark, this is Rich McComb. Just a...

((Crosstalk))

Rich McComb: Just as a - as a thought. As we continue in the COVID environment, I suspect that the other departments and agencies are experienced similar issues with regard to - it's really kind of a two-pronged issue with access, you know, with mostly remote staff - with most of your staff working in a remote environment.

We've seen an increase in security incidents and - and folks passing along information to their personal systems. And obviously we've addressed that in, you know, a lot of messaging and communication to our remote workforce. And then there's also the - the issue of unauthorized disclosure of sensitive but unclassified information to the public media, et cetera, that we've been dealing with.

So just thought I'd mentioned that to say maybe others have been experiencing the same thing. But we - we intend to obviously do what we can to educate, you know, all users of information right across all the populations -- not only to the federal government -- not only are DHS federal employees but contractors as well as the state, local, tribal, and private sector partners.

You know, I&A and others do a lot good - do great work getting lot of information out. Unfortunately, some of it has been getting into the public sector where - where it is explicitly caveated not to go. So anyway, just thought I'd mention that and just recommend that all folks start to think about that because as you stated, we're gonna be in this environment for some time. And I suspect that the - unfortunately the opportunities for this to continue to happen will not go away. That's all I have. Thank you.

Mark Bradley: No, Rich, that was quite good. I appreciate that reminder. Yes. Okay, anyone else?

Leo Masciana: Mark, this is Leo.

Mark Bradley: Hey, Leo.

Leo Masciana: An area that's becoming increasingly concerning to me - I sort of followed on the OPM breach, WikiLeaks - the elimination of the third agency rule -- tendency in a pattern and practice of shifting unclassified information to classified security domains.

Yes, I don't know if that really affects our state and local partners that much at this point but I think there is an increasing amount of shifting what should be more accessible information to inaccessible IT domains -- which obviously hinders not only sharing with state and locals but also between and among federal agencies.

Mark Bradley: Right.

Leo Masciana: It's an issue, I think, that if it is isn't acute yet, it will be. And something to keep - keep in mind in terms of ISOO's mission space.

Mark Bradley: Oh no, Leo. Trust me. Oh, indeed. No, I mean, yes. I've got stories that would curl your hair. But yes, we're aware of it. And now we are - we are being constantly reminded that it's an issue.

Leo Masciana: Well it concerns me now that we're so dependent on remote work during an environment where it's a matter of life and death for personnel.

Mark Bradley: Yes. No, that's right.

Leo Masciana: Couldn't agree more.

Mark Bradley: Okay. Anyone else? Anyone else, before I adjourn the meeting, here.

((Crosstalk))

Mark Bradley: Yes, Marc.

Marc Sachs: Do we have due out to follow up with building on the meeting we had in May to build the baseline of what is currently in place from our federal partners? Should we schedule a meeting to do that or...

((Crosstalk))

Greg Pannoni: Yes. This is Greg Pannoni, ISOO. We intend to have a follow-on meeting, taking into account a lot of what I heard this morning. As far as identifying essentially the foundation of the landscape with the various mechanisms that we have in place and any other - or solution-oriented ideas.

So yes, myself and my staff, we will work on getting a date for meeting well before our next actual SLTPS-PAC committee meeting. And then as we talked about perhaps maybe even - I'm not sure yet, but integrating into that meeting or a special separate meeting -- have to consult with the Chair as far as the (unintelligible) - having a CISA representative come and give us, you know, an in-depth overview of how they are operating in particular vis-a-vis their transactions, their interactions with private sector -- and of course state and local -- to get a lot more insight into that process -- the granularity hopefully of what interactions are occurring the timeliness, the speed, the priorities. A

lot of things that many of you mentioned on this call.

Marc Sachs: Okay. Thank you.

((Crosstalk))

Mark Bradley: Okay. Anyone else before I end this today? The next SLTPS-PAC meeting will be held on Wednesday, January 27, 2021, 10:00 a.m. to 12:00 noon. God willing we'll be back in the building by then and be able to do this in person. If not, we'll obviously give you plenty of notice about how we intend to handle that. So, anyway, I mean, that seems like a lifetime away now. The way time is - been going. But again, January 27, 2021.

Right, with that, thanks to everyone for participating today. I think it was another good and useful meeting. You all please stay safe and hopefully we'll be able to meet in person soon. Thank you. Meeting adjourned.

Leo Masciana: Thank you.

Deb Winsor: Thank you.

((Crosstalk))

Man: Take care, everyone.

Man: Thank you, Mark.

END