INFORMATION SECURITY OVERSIGHT OFFICE

Chair: Mark A. Bradley
January 27, 2021
10:00 a.m. EST

Mark Bradley: Good morning, everyone. Mark Bradley, your Chair, and also Director of the Information Security Oversight Office. This is the first State, Local, Tribal, and Private Sector Policy Committee meeting of 2021, and the 19th meeting overall.

This is a public meeting, subject to the Federal Advisory Committee Act. The minutes of the SLTPS-PAC meeting are available through the public. Meeting is being audio recorded. Please identify yourself each time you speak so we have an accurate record of your comments.

This is of particular importance because this meeting is being held by teleconference and the audio recordings will be used to produce a transcript. Also, when you're not speaking, if you can remember, please mute your phones. But obviously when you come back on, unmute the phone.

We’ve had some membership changes since we met last. For the SLTPS entities first, I must announce a vacancy. Jessica Davenport, Deputy Director

Florida Fusion Center, completed her four-year term earlier this month. Thank you, Jessica, for your service on the committee.

My staff will send an email with a call for nominations. To meet the requirements of the SLTPS-PAC Membership Balance Plan, please submit nominees who are not, and I repeat, not from the eastern region of the country. We have five SLTPS entity members from the east. We currently have no one from the Mid-West.

I'm pleased to announce new members on the federal side, Department of Defense, Michael Russo, Chief, Information Security Policy. Also, the Undersecretary of Defense for Intelligence and Security is a new DOD member.

The Department Of Energy has a new member and two new alternates, Mark, Hojnacke, Director, Office of Security Policy, Office of Security, is the member. Tracy Kindle, Personnel Security Policy Program Manager, Office of Departmental Personnel Security, Office of Security is the alternate. Natasha Sumpter, Program Planning and Management Team Lead, Office of Security Policy, Office of Security, is also an alternate.

Now that I asked the members of the committee to identify themselves, let me just do it this way. Charlie Rogers, are you there?

Charlie Rogers: Yes, I'm here, and Rich McComb is not available today. He had a pressing matter he had to deal with.

Mark Bradley: Okay. Thank you, Charlie. Darryl Parsons, NRC, alternate, are you there?

Sabrina Atack: He may join late. This is Sabrina Atack. He has a conflict of time.

Mark Bradley: Okay, Sabrina. Thank you for letting us know that. Mike Russo, DOD, member.

Michael Russo: Yes, sir. Present. Pleased to be here.

Mark Bradley: Good to have you, Mike. Valerie Kerben, ODNI, member.

Valerie Kerben: Hi, good morning. This is Valerie.

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

Leo Masciana: Yes, sir. I'm on. How are you?

Mark Bradley: Hi, Leo. Good to see you, and hear from you. Kate Connor, State, alternate.

Kate Connor: Good morning. I am here as well.

Mark Bradley: Okay. Hi Scott Gerlach, FBI, alternate.

Scott Gerlach: Good morning. Scott Gerlach is here.

Mark Bradley: Hi, Scott. Glenn Bensley, DOJ.

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

Mark Bradley: Hey, Glenn. Sidonie Dunham at Department of Transportation, member.

Sidonie Dunham: Here.

Mark Bradley: Welcome. Brian O'Neil, CIA.

Brian O'Neil: Good morning. I'm here.

Mark Bradley: Hi, Brian. Mark Hojnacke, DOE, member. All right. Don't hear from him. All right. Derrick Bouchard, DCSA, alternate. Okay. All right, Marc Sachs, SLTPS Vice-Chair.

Marc Sachs: Good morning, Mark. I'm here.

Mark Bradley: Hey, Marc. Tom Woolworth, SLTPS member.

Tom Woolworth: Yes. Good morning. I'm here.

Mark Bradley: Hi Tom. Tom Carr. SLTPS member.

Tom Carr: Yes. Good morning. I'm here.

Mark Bradley: Great. Thank you. Tiffany Kleeman, SLTPS member.

Tiffany Kleeman: Good morning. I'm present.

Mark Bradley: All right. We got an email I think from Eric Tysarczyk saying he was not going to be here. Is that right, Bob?

Bob Skwirot: That's correct, Mark. Yes.

Mark Bradley: Okay, great. All right. Mary Michelle Schechter, SLTPS member.

Mary Michelle Schechter: She is here.

Mark Bradley: Great. Welcome. Meghann Teubner, SLTPS member.

Meghann Teubner: Good morning. I'm here.

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

Debra Ann Winsor: Good morning. I am here.

Mark Bradley: All right. Is there any board members - I'm sorry, board members. Any committee members that I missed or alternates that I overlooked?

Angel Catalan: Good morning. This is Angel Catalan with the FBI. Present.

Mark Bradley: Great. Thank you. Anyone else? All right. Hearing no one, I'm going to introduce Greg Pannoni, my deputy, who will take us through some old business. Greg, all yours.

Greg Pannoni: Thank you, Mark. Good morning, everyone, and thank you for attending the meeting. So, a few updates here from our last meeting, which was July 29th, 2020. The FBI clearance data to DCSA was something we had as an action item, and I believe we're going to hear from the FBI this morning on that matter.

Another item was the number of SLTPS personnel cleared by the intelligence community. You may recall that the chair tabled that one. We have to continue to do that until we're back from the pandemic and can have a discussion in a SCIF, in the ISOO SCIF to discuss that matter.

The third item was a briefing by the Cybersecurity and Infrastructure Security

Agency, CISA. We did have that discussion, as you may recall, many of you. Bryan Ware gave an excellent update from DHS CISA agency. So, that's occurred. I think that was in October.

Next item was the identification and review of policies related to discussions about allowing access to classified information at home. I do not have any additional updates per se. We are trying to get more information. ISOO is a little short-handed right now.

We don't have an information assurance specialist, which would tie us in to the Committee on National Security Systems, which we are aware they have at least one document on the use of mobile devices remotely. And so, we tried to reach out to the CNSS. We're not currently - we were an observer, but we're not currently an observer to that committee. So, we have tried, but unfortunately without success to reach out to them to get more information about anything they have with respect to this action item on remote access to classified. So, we'll have to continue on that one.

And then the other item, the last item from the last meeting …

Man 1: I'm a multi-tasker.

Greg Pannoni: I'm sorry, did someone say something? Anyway, Cyber Threat Information Sharing Working Group, we did meet again. We actually met twice. And so, we'll -I'll get to that in a moment. We met in January and December; so, this past December, and January on that one. So, those are the action items.

The minutes are in, or you should have received the minutes from the last committee meeting. And so with that, unless there's any questions on the action items, I'll turn to a little bit more in depth discussion about the Cyber Threat Information Sharing Working Group.

Okay. Well hearing none, we'll move on to a little bit of the discussion about the Cyber Threat Information Sharing Working Group. So, we met - as I mentioned, we met December, December 3rd, and then we met again in early January. And the group has met prior to that back in May, and we briefed it out at the last SLTPS-PAC then.

So, we're still - we're not ready to present recommendations yet to the full PAC because the working group collectively has not had a chance to comment on recommendations that had been drafted. So, we will have to, you know, do that at the next meeting.

We - some of this you've heard before. We’ve had a lot of discussion about - in the space of cyber threat information sharing, what are some of the concerns. And it runs the range of - well, first of all, I think someone made the point at one of the meetings, which is still something is ongoing is, to set the table, so to speak, identify what the problem is.

So, in other words, assess what the current situation is with regard to cyber threat information sharing, what's being done effectively, and what's not. And while we've had, I would call it informal conversations on that, we don't - we haven't reached the maturity level where we have anything concrete, and even whether or not that's something we should do.

But meaning to assess agencies, ask them to come back with, you know, a little bit of formality, say something like a white paper identifying the existing state in terms of the methods and the procedures that are being used, the policies for - and the implementation of cyber threat information sharing.

We - then of course moving on, we've heard things concerning timeliness of sharing this type of information, that the idea that, is the information actionable? Is it relevant? Does it provide the tactics and techniques and procedures? Is it prioritized? We've heard that one too.

So, a number of different points have been raised as far as potential areas for recommendation. And so, that's essentially kind of boiling it off quickly here. That’s kind of where we are. So, I'll stop at that point. And if anyone has any questions to ask, glad to try to answer them. Well, hearing none. I will turn it back to you, Mark.

Mark Bradley: Okay, Greg. Can we go through the action items now?

Greg Pannoni: Well, I think pretty much, I …

Mark Bradley: That's it?

Greg Pannoni: Yes, I think that's pretty much it.

Mark Bradley: Okay, right.

Greg Pannoni: I’m glad to go over that if you want.

Mark Bradley: Hold on. Let me get my key sheet here.

Bob Skwirot: Mark, can I interrupt for a second?

Mark Bradley: Yes, Bob.

Bob Skwirot: I think the FBI was going to provide an update with regard to action item number one.

Mark Bradley: Okay. Got it. All right, the FBI report. Okay. Yes, I got it. Right. So, there are five - all right, yes. The FBI report on the January 2021 SLTPS-PAC meeting on the status, be able to provide SLTPS security claims data to the DCSA. All right. FBI?

Angel Catalan: All right. Good morning. Angel Catalan here for the FBI. I also have Scott Gerlach, alternate member on the line, and we invited Marie Bernoi, who leads our mission support section, who have been instrumental in developing this process.

So, over the summer 2020, the FBI Security Division started collaborating with the FBI's Information Technology Applications Division, to develop a script to download clearance information for State, local, tribal, and private sector personnel whose clearances are held by the FBI, and pretty much download that from our Phoenix platform, which is the FBI’s clearinghouse for clearance information, and again, you know, create a script to feed it into DCSA’s CVS system.

Back in August, they developed a script. It was tested during the month of November. And then they started conducting end-to-end testing with the DCSA, you know, since the beginning of this year. It's currently ongoing. We expect to go live, start feeding of that clearance information into DCSA’s CVS system probably by March of this year.

Everything seems to be on track. Basically, you know, this is going to be a manual process, which is - again, it's going to be downloaded from our

Phoenix platform, push the script over to DCSA on a monthly basis, with the understanding that at some point, we'll develop some sort of automation.

That is still a long ways down the road. I can't comment on any timeline on that at this point. But that is the intent, is to develop some sort of automation where we could download and transfer clearance information directly to DCSA automatically.

As of January 25th, basically last Monday, we identified 9,163 TFOs, task force officers, again, from different organizations, whether they're State, local, tribal, or private sector components, whose clearances and investigation records are held by the FBI.

One action item that is still pending is to identify how many non-task force officers' clearances we have in our systems. I hope to provide an update during the next meeting, but that's something we're still trying to track down. So, again, you know, everything seems to be on track. We should be doing live, you know, by, if not before March of this year. I will turn it over to Marie Bernoi if she has anything else to add on this item. Marie?

Marie Bernoi: Sure. Good morning. Again, this is Marie Bernoi. I'm in charge of the IT portfolio management team that's been working on this effort. And so, really the only other thing to add is, we are looking at that other population, but the original request was to send over the TFO population.

So, that is what we are focusing on. But once we get our connection made with DCSA, where we're doing this on a monthly basis, we'll continue to look at what other populations may - that we may be able to share in this capacity. And the only other thing is, I did get an update from the team right before this meeting, and they feel like we are definitely on track for the March timeframe, and potentially could even be done sooner before they go live.

So, they're very close to being able to provide that feed on a monthly basis. So, all good between the teams as far as getting this project complete.

Angel Catalan: Great. Thank you, Marie. And that concludes our update, pending any questions from the group.

Greg Pannoni: Just a comment. Greg Pannoni. I just want to thank the FBI, especially for, you know, pursuing this and bringing it forward, and moving towards maturity on being able to provide these data. This is more of a core mission, as you know, elements of the executive order for this program and clearances is important that we have a better idea where they are and the volume. So, thank you.

Angel Catalan: Yes, you're welcome. And happy to collaborate with the team here on this.

Mark Bradley: This is the chair, and I want to echo what Greg said. Thank you so much for doing what you've done and moving this forward. As Greg said, it's absolutely critical for the success of this executive order, and given this high threat environment that we’re in and going to stay in, it's absolutely essential that this takes place. So, again, kudos to the FBI.

Marie Bernoi: Thank you.

Angel Catalan: You're welcome. And again, I take no responsibility. This is Marie Bernoi’s team and, you know, so we thank her team for developing this script. So, thank you.

Mark Bradley: You're the man on the phone; so, you get the credit. So, anyway, thanks again. All right. Bob, is that the end of the old business?

Bob Skwirot: Well, we probably should remind a number of the members that they need to submit their financial disclosure forms.

Mark Bradley: Okay. Members, hear that? That's required as part of your responsibilities for sitting on the committee. It's been a longstanding requirement. Let me just make sure that I get this official. NARA is required to ensure that the federal government members' advisory committees and their designated alternates, do not have actual or apparent conflicts of interest with respect to service on such committees.

For that purpose and the subject of the bylaws - I'm sorry, to that purpose and subject to the bylaws of the SLTPS-PAC, NARA's Office of General Counsel was responsible for reviewing member financial disclosure forms. Please send the forms to Ms. Khandekar as soon as possible.

Anybody has any questions about that, please reach out to us. We're not asking you to come up with a new form. The forms that you already filed, you know, in the course of your duties, suffices to this as well.

Marc Sachs: This is Marc Sachs. Is this an annual requirement or just for new members?

Mark Bradley: This is an annual requirement.

Bob Skwirot: It's only for federal members.

Mark Bradley: Yes. Marc - yes. It's federal only.

Marc Sachs: That would explain why those of us in non-federal haven't seen an email. Okay, thank you for that.

Mark Bradley: Yes. Well, you consider yourself fortunate. But no, I mean, this is strictly a…

Marc Sachs: Oh, we have them in plenty for other purposes, so that’s okay.

Mark Bradley: Yes. I don't doubt that. Bob …

Greg Pannoni: And I’m sorry, Mark. Greg Pannoni.

Mark Bradley: Yes.

Greg Pannoni: Just a point of order I overlooked. The charter for the committee was renewed.

Mark Bradley: Yes, I was going to ask about that.

Greg Pannoni: And so, it's still in order through September 30th, and then it'll most likely be renewed again. This is done by way of another executive order. The current order that did this, not just for this committee, but for all socket-type committees that were renewed, was EO 13889, if you care to look that up. So, just wanted to get that in there too.

Mark Bradley: Okay. So, I'm going to embarrassingly have to ask you another question. Are we now done with the old, and can we move to the new or not?

Bob Skwirot: I think so. I think we covered all the points.

Mark Bradley: Okay, great. No, I mean, this is a busy committee and there are a lot of other things here. All right, Greg, thanks. So, Charlie Rogers, DHS, alternate Vice-Chair, will provide an update on the DHS LTVS security program. Charlie?

Charlie Rogers: Yes. Good morning, everyone. For any of you who have gone to these meetings before, I frequently provide a general update about what we're doing with the fusion centers, primarily in the State and local program. So, bear with me. I'll probably repeat myself a little bit to provide some background, but DHS is currently supporting more than 80 fusion centers.

We have, within the office of security, five field security coordinators are - let me put it this way, our allotted of numbers are five field security coordinators, and they are typically assigned 16 fusion centers to directly support. Having said that, our current staffing is at four. So, they are pressed to cover approximately 20 fusion centers each.

I was going to talk a little bit about the security program audits. And in July, I had updated the committee that due to COVID, we have begun to pivot the way in which we did our security program audits from onsite visits to remote virtual, and that is still going on.

A little bit about the fusion centers. Over the past year, or I guess nine or 10 months since COVID has impacted us, the fusion centers are no different than the federal government. They have been seriously impacted by COVID. They're not having their full staffs come into their facilities on a regular basis.

So, I think it's accurate to say that all of them have been impacted in some manner, but none are shut down. They're operating with minimal staffing. And the secure rooms, the collateral secure rooms, secret levels secure rooms that have been certified, are still being used. They're being properly monitored and secured each day. But they are impacted.

A little bit about the security program audits. I mean, even before COVID, I mean, the purpose of these audits, or like any compliance program, is to ensure that the facilities are maintained in accordance with federal standards, that the classified information is being safeguarded, that the secure rooms are being managed appropriately, training and other things are being - the security training and other items are being done.

So, the way in which we're doing these audits now is a virtual remote auditing. It does not include going onsite. And even if we were able to go onsite, well, there would be - still be a challenge because as I mentioned, the fusion centers are not fully staffed.

So, we're reaching out to them to essentially - well, there's three phases. We reach out to them to - well, before we reach out to them, we look at all the previous audits. We look at previous inspections, findings. We look at our documentation, then we reach out to them, discuss the remote virtual audit with them.

We provide them with a checklist, and give them 24 hours to complete it. So, we think it's important to put some timeline on having them perform it, so that there's not a lot of thought, that they can go and they can get back to us. And then there's a validation phase regarding the audits.

We've been doing this now for - well, we didn't start at the beginning of COVID, but we've been doing it for seven or eight months now. And it was still a work in progress. It's valuable to have people onsite. And not having people onsite to do compliance audits, you know, does make it a challenge, but I think we're getting better at it.

We're utilizing technology. We’re considering using iPads that we would ship out to the fusion centers, and they would ship back to us with embedded checklists and instructions. So, we're looking at ways to do it better. Of course, once the vaccine becomes available and we get past the most significant impacts of COVID, then we will return to on-site visits.

But I think we will continue for - going forward, to utilize some of the lessons we've learned from doing virtual remote audits. So, they - it's kind of a new bag of tricks that we're not going to get rid of. We’re going to supplement it as we go forward.

And I will give you a few numbers on the audit - the status of audits. In FY’20, we had scheduled 16 security performance audits at fusion centers. We were able to perform five of those before COVID impacted us. We had a remaining 11 audits that we intended to do in FY’20, but we were only able to complete eight them because we essentially had to build a virtual audit capability, and that took some time.

So, the three audits which were not completed in FY’20 were moved into FY’21. Now we are all - we're in FY’21, we have completed five security program audits this year. We have two that are coming to completion in this month. We have three more that we'll be doing in February. I think we expect to do approximately 17 or more of these virtual audits this year.

And then the other part of the presentation was just to talk a little bit about some of the ongoing support we provide to fusion centers. We are providing monthly clearance rosters based on DHS's clearance database to the States, so that they can use those in validating clearance. It's a supplemental document.

We continue to approve - conduct surveys and approve classified storage locations and rooms for classified discussions. We do an occasional collateral room certification. Most of the fusion centers have HSDN, our secret level network, and they already have a certified room.

But on occasion, they either relocate to another building or they relocate - or they decide to expand the size of the room. And so, we support that activity. We're continuing to meet with - remotely with the liaisons, the security liaisons from the fusion centers to provide training, guidance on a regular basis.

As I mentioned before, we reach out to them weekly to determine what their operating status is regarding COVID. And that's kind of a quick rundown of where we are on the support to the fusion centers and how we're operating under this - the constraints of COVID.

And then I wanted to give you a little bit of an update on our personnel security clearance metrics. I think previously in July, we had approximately 8,800 total State, local, and private sector personnel cleared at the secret level. And we currently have less than that now. We have about 8,700. So, we've actually gone down about 100.

I don't think that's a significant number. I think that's a normal part of attrition and has to do with us being diligent about - and making sure that individuals who no longer require access are debriefed. So, we're in the same ballpark of numbers. We're about 8,700, as opposed to 8,800.

Regarding the total TS clearances, once again we - in July, we were approximately at 325, and now we're at 320. So, we've gone down approximately five, and that's really insignificant. It could go up 10 next month, so.

And then at the TS-SCI level, which is - a limited number of people are cleared at that level, but we - in July, we had about 375, and as of around January 11th, we had 377. So, we're - we seem to be at a steady state at the clearance levels for both private sector in State and local.

And I think that pretty much covers what I wanted to give an overview of. So, I'm available for any questions that anyone might have. I'll answer them as best as I can.

Mark Bradley: All right. Any questions for Charlie? No? Charlie, apparently your presentation was so brilliant that you answered all the possible questions.

Charlie Rogers: Yes. I don't think - they've heard it so many times before.

Mark Bradley: Right. I wasn't going to say that, but no, thank you. That was well done. All right. Moving on from Charlie, we're going to hear from Devin Casey on my staff on the CUI program. Devin.

Devin Casey: All right. Thank you. This is Devin Casey from the CUI team. Not too many updates for you on the CUI program. Some good news, some new dates, and of course, where to find more information will be at the end. The big news in the CUI program currently is, we're still kind of waiting for the publication of NIEM 5.0.

That's the National Information Exchange Model, NIEM. They handle a lot of metadata work for the federal government. The NIEM 5.0 release has the metadata markings and tags for CUI. Now, it's not mandatory that CUI be marked with metadata, and even if you are marking it with metadata, it's not mandatory that you use the NIEM structure.

But it is an example of a CUI-compliant metadata marking that will be released. And NIEM releases their metadata markings publicly. So, they're accessible by anyone, and that will be maintained by our office. So, we'll make sure that when there's changes to the CUI registry, that that NIEM is updated as well.

Next big update that I think most people have been tracking has been the CUI FAR case. GSA projected a new public comment period for the CUI FAR, which is the Federal Acquisition Regulation case for CUI, which will essentially expand NIST 800-171 use, as well as other CUI requirements to the - you know, every - all the agencies covered by the FAR.

The new comment period is projected to begin from March to May 2021. Again, that is an estimated or projected public comment period by GSA. Also of note, once that is posted, we will - you know, our office will host an ad hoc stakeholder meeting to discuss the content of the FAR, and to answer questions about the content or intent of the FAR, in order to receive better comments.

You can find out more information or stay updated on that if you go to the unified agenda, if you search unified agenda, you can get there. It’s on reginfo.gov. And it's under the FAR timeline case there. You can also get to it - learn from our blog for more information about the FAR as well.

A little bit of other notes on that front. The NIST SP 800-172 is still undergoing comment response. The NIST 800-172 is formerly the NIST 800-171b, which is additional requirements or enhanced security requirements for protecting CUI, when the CUI is of a particularly sensitive nature, for instance, part of a high value asset or a critical program at DOD.

So, that's still going through public comment or comment resolution. It already went through public comment and should be issued shortly by NIST. There will also potentially be a 172a, much like the 171a that the step is the evaluative criteria for those controls.

We've issued a few CUI notices, 2020-6 and 2020-7 since my last presentation. CUI notice 2020-6 talks about limited marketing waivers and the best practices. This is, you know, really aimed at agencies who can apply these waivers internally, and discusses the methods and procedures for marketing that information on systems or through the use of splash screens or databases, as opposed to granularly marking.

They're still required to mark or identify the information prior to transferring it outside of their agency, as the marking waiver only applies internal to the agency. CUI notice 2020-7 also covers kind of a unique thing that the government does occasionally, which is alternate designation indicators.

Certain agencies don't always want to put their agency name or have the flexibility to not put their agency name on information, and may claim it's US government information, as opposed to specifically that agency, in situations where they're permitted to do so. They also continue to be able to do that under the CUI program, following a process that has to be reviewed. And the CUI office will review those situations as well.

Big note, DOD has moved significantly forward with their CUI program. So, if you are working with or doing business with DOD, DODCUI.mil is their website for a lot of information and points of contact on their CUI program. We get a lot of questions.

Other big news in the CUI program is, we’re finishing up receiving our annual reports from agencies. We've gotten well over 90% of the - our reports in. We're just missing a few, mostly from very small agencies. The key to this year's annual report was, we're looking at agencies reporting that they will meet the deadlines that have been communicated this past year for issuing policy and starting training.

The majority of agencies will be meeting that deadline or falling within six months of it. So, we're excited to report that significant progress has been made over the past year, even despite responding to COVID and other concerns in that time towards getting those policies out.

And one of the things I always talk about, about implementation is, policy is really the first domino to fall. A lot of work has to go into placing that and the following dominoes once the policy is published. You’re looking at generally six to 12 months before, you know, some degree of marketing starts happening at an agency.

And, you know, by then you start to have most of your CUI program in place within the next six to 12 months from that policy publication. So, very exciting news on that front. A more in-depth review of that will be conducted at both our next stakeholder meeting, which will be announced on our CUI blog, as well as in our annual report to the president, the ISOO annual report to the president.

If you have any questions about the CUI program, please email me at CUI@NARA.gov, or go to archives.gov/CUI, where you can read more about our program and find our blog. Unless there's any questions …

Mark Bradley: Thank you, Devin. Yes. Please. Any questions for Devin on CUI? All right. Hearing none, we're going to move now to general open/form discussion and solicit comments from anyone who wants to say anything about the SLTPS and how a certain matter that falls under it.

Marc Sachs, do you have anything just to say for private? I mean, have we missed anything today or should - is there anything that we should be aware of?

Marc Sachs: This is Marc. I don't believe so. However, with the new administration coming in, do you anticipate anything from them coming to us that we may need to prepare for? And I don't believe we should - or that we need to have a discussion about the working group, and should we meet again to wrap up these comments that we're not - we weren't able to get them done for this meeting. But we probably should wrap them up as soon as we can and get a report out to the larger group.

Mark Bradley: No, let me speak about the first, and I'll turn to Greg for the second. You know, the administration, as you know, is brand new. So, I mean, we're still trying to establish, you know, who our contacts are going to be, especially on the National Security Council. And that's who I take my policy guidance from.

That said, I can only imagine that there's going to be more and more emphasis on robust information sharing, especially on the threat front. That's probably both internationally, and unfortunately now, probably domestically too. So, I expect this committee actually to rise in stature.

I think its work is going to become even more important for our country's security. So, it's - we'll certainly - once we make solid contact with the new administration, to tell them about the committee and its work and how important that we believe it is. It would be nice to actually have somebody from the NSC come in and speak to us about the administration's goals and points of view.

Marc Sachs: Well, and particularly if a …

Mark Bradley: Yes, please. Yes.

Marc Sachs: … new cyber director, whatever they're going to call that position …

Mark Bradley: Yes. Right. Exactly. Right.

((Crosstalk))

Marc Sachs: ... who’s going to be appointed, that's going to be (unintelligible), as well as the new assistant director, once that person is appointed. Hopefully all that takes place in the next 90 days. And then we've got - we'll have a good bit of opportunity there to work with them, you know, shaping where we want to go over the next four years.

Mark Bradley: No, that's true. Exactly right. And it's good to see the administration emphasize that particular vulnerability, I mean. So, you're absolutely right about that. Greg, do you have anything to say about the working groups and finalizing some of these outstanding issues?

Greg Pannoni: Yes, sure. And also, if I'm not mistaken, I think we just heard that they did announce, I want to say a cyber director.

Mark Bradley: I thought that was done this morning. Yes. I mean, I thought - at least I read that. I mean, at least I think I did. But yes, it is …

Greg Pannoni: Same here.

Mark Bradley: Yes.

Greg Pannoni: So, we're - but back to - yes, to the working group. Sure. We - as you've indicated, Mark, we still need to come up with recommendations to the committee. And so, that's the intention that we will meet again to try to get some sort of consensus on what the needs are, you know, for the population I'm referring to, both the private sector in the state and local, tribal, with respect to cyber threat information.

And so, that is the intention, is to meet again. But I will say, I think we need to work within the confines to be realistic with the executive order’s purpose and the committee's purpose, which are both well stated in the order. I don't really need to restate those.

But - so I think we need to be keen on looking at whatever recommendations we make to the committee, that they are in alignment with the order and the purpose of the PAC. So, that's …

Marc Sachs: Thanks, Greg. I fully concur. I just wanted to make sure that we don't - just don't leave the group out there hanging and try and schedule maybe a wrap up in the next 30 to 45 days or so, so we can finalize those recommendations.

And exactly, as you say, making sure they're within the guidelines, but if there are recommendations that are outside those guidelines, maybe we can forward them over to CISA or someplace else where they might have the ability to consider them.

Greg Pannoni: That sounds good recommendation on - in and of itself. So, yes. I agree and welcome anyone else from the group now when we - before we meet to provide any input. I do think, as I mentioned before, which really someone else in the group first brought it forward, that we assess the current situation with regard to cyber threat information sharing.

Essentially, what are we doing now, and what's being done effectively now? It just seems to me that that's the base where we want to make sure we're clear, we have the data on that as a basis for recommendations to the committee.

Mark Bradley: All right.

Greg Pannoni: That's all I have.

Mark Bradley: Thanks, Greg. Yes.

Marc Sachs: Thanks, Greg.

Mark Bradley: Yes. Is there anything else? I mean, looking at the clock, we've done this in record time. I mean, who said teleworking wasn't efficient, right? It's what, 10:49. So, we've got time, if anybody wants to discuss anything else that you think we should be focusing on, you know, neglecting, looking ahead.

I mean, this is a wide-open forum; so, please don't hesitate to speak. Okay.

Well, hearing none, and I don't want to have a meeting for a meeting's sake, so let me see if I can wrap this up. Let's see. The next SLTPS-PAC meeting will be held on Wednesday, July 28, 2021, from 10:00 am to 12 noon.

Let's hope that this will be possible to hold this one in person, back in our confines at the National Archives downtown. So, please mark your calendars for that. Right.

Marc Sachs: Can you say that one more time? You said July 28th? Is that correct?

Mark Bradley: Yes. Sure. I said July 28, 2021, 10:00 am to 12 noon.

Marc Sachs: Thank you.

Mark Bradley: You're most welcome. Please mark your calendars for that.

Operator: Everyone else has left the call.

Mark Bradley: Okay. Having …

Marc Sachs: Some of us are still here.

Mark Bradley: Yes. That's rather peremptory there, but maybe that's a sign, huh? So, anyway, you all stay safe.

Operator: It looks like no one else is going to join this call. Goodbye.

Mark Bradley: Okay. Right. Yes. All right. I'm going to adjourn the meeting and look forward to seeing you all, hopefully in person, in July.

END