STATE, LOCAL, TRIBAL, AND PRIVATE SECTOR POLICY ADVISORY COMMITTEE (SLTPS-PAC)
January 29, 2020

SUMMARY MINUTES OF THE MEETING

The SLTPS-PAC held its seventeenth meeting on Wednesday, January 29 2020, at 10:00 a.m., at the National Archives Building, 700 Pennsylvania Avenue, NW, Washington, DC. Mark Bradley, Director, Information Security Oversight Office (ISOO), chaired the meeting, which was open to the public. The following minutes were finalized and certified on July 1, 2020.

(The meeting minutes, copies of presentations, and the official transcript of the proceedings are available at https://www.archives.gov/isoo/oversight-groups/sltps-pac/committee.html.)

I. Welcome, Introductions, and Administrative Matters (Reference transcript pages 1–7.)

The Chair welcomed the attendees and participants. He introduced four new SLTPS-entity members: Eric Tysarczyk, Director for Preparedness, New Jersey Office of Homeland Security and Preparedness; Tiffany Olson Kleemann, General Manager, Distil Networks, Arlington, Virginia; Meghann Teubner, Director, Counterterrorism Intelligence Analysis, New York City Police Department, and Mary Michelle Schechter, Director, Division of Community and Maternal Child Health, Nassau County Department of Health, New York. He announced that the SLTPS-entity members selected Marc Sachs as their Vice Chair and that he approved the selection. He reported a vacancy in the SLTPS-entity membership, as Dori Koren, a Detective and Supervisory Task Force Officer, Las Vegas Metro Police Department, completed his four-year term at the end of last year. He advised the membership that they would receive a call for nominations to fill this vacancy and asked, in the interest of geographic diversity, they submit nominations for individuals who live west of the Mississippi. On the Federal side, he announced a new member from the Department of Transportation, Dr. Sidonnie Dunham, and reported vacancies in three agencies: the Nuclear Regulatory Commission, the Federal Bureau of Investigation (FBI), and the Department of Defense. Finally, he advised Federal members that it was again time for them to submit their financial disclosure forms. (See Attachment 1 for a list of meeting attendees and participants.)

II. Old Business (Reference transcript pages 7–37 and 54.)

Updates from the DFO
Greg Pannoni, SLTPS-PAC Designated Federal Officer
Associate Director, Operations and Industrial Security, ISOO

Mr. Pannoni reported on the two working groups that met to address the action items from the previous SLTPS-PAC meeting, which was held July 24, 2019. The action items were (A) Convene a working group on the security clearance database for SLTPS personnel, and (B) Convene an ad hoc working group to develop recommendations for improvements to the classification system to better facilitate the sharing of information with SLTPS partners.

A. Report on Action Item 1, Security Clearance Working Group

Mr. Pannoni began his report on the security clearance database working group by noting that the Committee has been discussing the issue of the central database for all SLTPS personnel for at least two years. He indicated that the Central Verification System (CVS) is supposed to be the database according to law, as he pointed to the Intelligence Reform of Terrorism Prevention Act, which established that there will be a central verification database system for all cleared people, not just SLTPS personnel. He reminded everyone that E.O., 13549, "Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities," requires that there be a Central Database Tracking System that the Executive Agent, DHS, shall maintain in coordination with other bodies that are involved with those other databases. He stated that the issue at hand is visibility, the ability for our nonfederal partners to know where their clearance is, the date of the clearance in order to direct someone for example if there's a meeting that they have to attend. They have to provide that information to someone who can then go and validate it; they need to know where to go to see it. Mr. Pannoni stated that there are at least two agencies where this surfaces as an issue: the FBI, which uses Scattered Castles for SLTPS clearances, and the Office of the Director of National Intelligence (ODNI) for the Central Intelligence Agency (CVS), which also uses this space.

Mr. Pannoni reported that the working group meet in early December 2019. The main outcome of the meeting was that the Defense Counterintelligence and Security Agency (DCSA) would furnish what it called a flat file to the FBI, which would allow the FBI to upload SLTPS clearance information into the central database. Mr. Pannoni indicated that the Committee was encouraged by the movement within the FBI and DCSA. The participants in the working group agreed to provide the following information at this meeting: (1) the FBI would report on what it can do with regard to entering its SLTPS clearance data into the CVS; (2) the FBI would provide the number of SLTPS personnel currently holding security clearances who have been cleared by the FBI; and (3) the Office of the Director of National Intelligence would provide the number of SLTPS personnel currently holding security clearances who have been cleared by the intelligence community. Mr. Pannoni then turned to Earl Camp, FBI, for a report on the first two items.

1. FBI SLTPS Security Clearance Data and CVS

Mr. Camp began by stating that the previous representation on this committee was from the technical side of the FBI, from the Office IT Systems. He stated that that office did not engage FBI security personnel in this discussion. Mr. Camp indicated that he is assigned to the FBI Security Division, which handles the issuance, storage, passage and verification of all clearances throughout the FBI. He indicated that, when his office became aware of the issue from the last meeting, they presented it to the FBI Office of General Counsel (OGC). He stated that the FBI OGC has concerns about submitting the information into CVS because they are bound by the Intelligence Community (IC) Policy Guide, which mandates that the FBI continue to use and leverage Scattered Castles. He indicated that uploading the information into the CVS is not only a technical issue for the FBI. They do not integrate with the CVS because they leverage Scattered Castles as required by the Intelligence IC Policy Guide. He stated that this is IC policy not FBI policy. He indicated that the Office of Security is waiting for the OGC, after reviewing the Executive Order, Security Executive Agent Directive (SEAD) 4 or SEAD 7, and the IC Policy Guide, to provide a legal opinion on whether the FBI is barred from sharing that information.

Mr. Camp then turned to what he understands to be the crux of this issue, namely that the FBI's state, local, tribal and private sector partners indicate they do not have the ability to check on their clearances. He stated that from an FBI perspective that is not the case and that the state, local, county, tribal and private sector partners that the FBI sponsors clearances do have a mechanism with which they can check the status of their clearances, the date of the issuance of the clearance, and whether the clearance is in scope or not. They can also check on the status of any SCI by reaching out to the Chief Security Officer and the sponsoring FBI Office and requesting that information. He stated that state, local, county, tribal and private sector can check on the status of their clearances, like every FBI employee does, which is they go through their Chief Security Office, and for those partners it's in the Field Office that sponsored their clearance.

Charlie Rogers, Vice Chair, DHS, provided clarification regarding DHS's responsibilities as the Executive Agent under the Executive Order regarding clearances. The Executive Order says that DHS is responsible for documenting and tracking the final status of security clearances for all SLTPS personnel in consultation with the Office of Personnel Management (OPM), DoD and ODNI. Right after the Executive Order was signed, DHS stood up a working group committee with those players, as well as the FBI, and it was agreed that CVS was going to be the mechanism. So, DHS does not request clearance documentation from agencies. DHS expects agencies to migrate clearance documentation into CVS, which was designated by that working group. Mr. Rogers emphasized that the FBI was represented on that working group and had input into the configuration of how CVS would work. The DoD modified the Joint Personnel Adjudication System (JPAS) to enable JPAS to communicate directly with CVS, and the OPM created a portal for state and local Fusion Centers to access and verify clearances in CVS. The decision was made early that the mechanism was going to be CVS and that the CVS would be the means by which DHS would receive its information and fulfill its responsibilities.

Mr. Camp responded that he understands this but reiterated that the personnel representing the FBI on this issue in the past were not from the Office of Security and did not understand the sensitivity of the information involved. He added that he thinks the technical fix is something they can come to. Computer people can talk to computer people and get that ironed out. The Office of Security just wants to make sure that they are not violating some other policy as laid out by either the ODNI or SEADs 4 or 7, which are primarily their bible. He said that is really the issue here.

The Chair indicated that he understood what Mr. Camp was saying, but expressed that his fear is if something goes wrong, having a congressional hearing on this issue with people wondering why clearances did not get passed. He asked Mr. Camp when he expects the legal review to be complete. Mr. Camp responded by first stating there is no issue with getting the clearances passed. SLTPS personnel can always contact their local FBI office and facilitate that. With regard to when can the FBI get a legal read on whether they can put this data into CVS, he indicated that he cannot provide a timeframe because he is at the behest of the FBI OGC attorneys. The Chair asked if perhaps a letter from him to Director Wray might prompt things along. Mr. Camp responded, yes, he did not think that would hurt anything. The Chair then asked the SLTPS partners for their perspective on this issue.

Marc Sachs, SLTPS-entity Vice Chair, acknowledged that if the individual knows Field Office is, which they should, that shouldn't be a problem. The issue is timeliness when someone gets a phone asking them to come immediately to be briefed on something. If they're in CVS, the location they're going to can immediately determine yes, come on in, join the meeting. Compare this to having to find your FSO, having to hunt that person down, having them go through the formal process of passing clearances which often you need to do a week in advance. That's the typical way if you're doing a scheduled classified briefing at some point in the future. It's the timeliness issue particularly with cyber information. Charlie Rogers added that the original intent of CVS it was to enable federal agencies and state and local partners to verify the final status of clearances in a quick and effective manner.

Mr. Camp responded that if there's an impromptu meeting there's still a mechanism. The Fusion Center could call their local FBI Office and every Fusion Center has a relationship, a very close relationship with their local FBI Office. And say hey, we're holding a meeting this afternoon. Here's our planned list of attendees. If the intent is to allow entities to access their clearance data so they can participate in these meetings, the FBI does have a process in place for that.

Mr. Camp then turned the focus to the risk of sharing information with SLTPS partners. He stated that when the FBI sponsors a state, local, county, tribal or private sector partnership, they do not necessarily have that control. People come to the meetings. They receive classified information. They leave the meetings. But they're not in a controlled government environment. In other words, there's no recourse if those people decide to somehow spill or leak that information; there are no reporting requirements. There are no repercussions for that. So that entails a greater risk especially for the FBI. And that in the Security Division is what they are trying to manage. They are trying to balance the obligation from the result of the 9/11 Report to share information with our state, county, local and tribal officials with the risk that the FBI assumes by sponsoring those clearances and sharing that classified information. And that's where the lawyers come in, right. And they're helping the Office of Security determine the management of that risk. The Chair and a number of members responded that this is a separate issue.

Patrick Hogan, Department of Defense, turned the discussion back to the original issue of passing clearances. He confirmed that there are plenty of IC partners in both JPAS and CVS. There's nothing illegal about it. There is a mandate to put things into Scattered Castles, but that does not prohibit an agency from putting it in another approved system. In terms of OGC across the government, there is plenty of legal precedent from putting IC members' clearances or any of those state, local, tribal partners at the ICs adjudicating into other secure Personnel Security Systems of record to include CVS and JPAS. Mr. Camp indicted that he agreed with Mr. Hogan but reiterated that he needed to get the okay from the FBI OGC first.

Valerie Kerben, ODNI member, provided clarification on security clearance databases and the SEADs. With regard to Scattered Castles, she confirmed that agencies should record their TS/SCI access levels inclusive of all the intelligence agencies. She added that all agencies that have access to Scattered Castles determine who should at their agency can have access and reporting capabilities. ODNI does not determine who gets access specifically. It's up to an agency to sponsor their own people or their own FSOs. And they are to track who they're giving database access to.

Regarding the SEADs, she confirmed they describe the policy for reporting clearances to government-wide databases. However, they do not say specifically who reports where. She added that, as everyone is aware, eventually there may only be two databases, a high side and a low side, sponsored by DoD. At this point, though, there are three databases, and we want to encourage everybody to share what they need to in all the proper databases.

Towards the end of the meeting Mr. Camp interjected that he reached out to his OGC and indicated that the FBI is going to have an answer on this by the next meeting. He added that he was going to have his technical folks go ahead and work on the technical solution, so if they get the green light, they can just basically affect everything. He indicated that they could probably do a quarterly flat file passage as long as they get the green light. He reiterated that he will have some clarity for the next meeting.

ACTION ITEM 1: Mr. Camp and the FBI will report at the next SLTPS-PAC meeting the on whether the FBI will be able to provide data to the CVS on the SLTPS personnel it has cleared.

2. Number of SLTPS Personnel Currently Cleared by the FBI

At the working group meeting, the FBI was asked to provide to this meeting the number of SLTPS personnel currently holding security clearances who have been cleared by the FBI. Mr. Camp reported that currently, the FBI is the sponsor for 892 clearances nationwide that fall into that category.

3. Number of SLTPS Personnel Currently Cleared by the IC

At the working group meeting, the ODNI was asked to provide to this meeting the number of SLTPS personnel currently holding security clearances who have been cleared by the IC. Mr. Pannoni reported that ISOO had been informed by the ODNI prior to the meeting the CIA was unable to extract number for this tasking, as they do not categorize or break down their population by SLTPS categories. Ms. Kerben indicated that the ODNI will engage with CIA again and get more information. She noted, that CIA supports the non-title (NT) 50 agencies for TS/SCI, though she is not sure how they are tracking this information. So, if one agency submits 100 cases, the ODNI does not know how many of those 100 are specifically for state, local, or tribal. She reiterated that ODNI will continue to engage with CIA and determine if there may be another way extract a number or see how they could do future tracking.

ACTION ITEM 2: Ms. Kerben will provide an update at the next SLTPS-PAC meeting on the effort to determine the number of SLTPS personnel currently holding security clearances who have been cleared by the IC.

B. Report on Action Item 2, Classification and Sharing of Cyber Threat Information Working Group

Mr. Pannoni began the report by reminding everyone of the briefing provided at the last SLTPS-PAC by Leo Masciana, SLTPS member, Department of State, which was the impetus for the formation of the working group. The issue he presented was whether the classification system was working to hinder or to help in the cooperation with SLTPS partners to defend the nation's critical infrastructure from cyber threats. The working group, which included Mr. Masciana, Mr. Rogers, Mr. Sachs, and Mr. Pannoni, met in early January. The fundamental issue under discussion was how to desensitize cyber threat information and get it to the right people in an expeditious manner. Cyber threat information, in particular is perishable. If the information is actionable and you don't have it within 24 to 48 hours, generally speaking you've missed on addressing the vulnerability or threat, and if the bad actors wanted to do damage, they would probably have already done it. Mr. Pannoni reported that the working group quickly recognized the need to bring the right subject matter experts into the discussion at a subsequent working group meeting, to include personnel from the following agencies and organizations: the U.S. Cyber Command, the National Security Agency (NSA), the Defense Information Systems Agency, the

ODNI, the Cybersecurity and Infrastructure Security Agency (CISA) of DHS, the FBI, and the National Council of Information Sharing and Analysis Centers (ISACs). Mr. Masciana reported on the progress he has been making in enlisting the appropriate personnel form many of these entities to participate in the next working group meeting.

Mr. Masciana opined that there's considerably more that needs to be done to expedite cyber threat sharing then just classification. But it's a good place to start to ensure that the guidance is effective. And that's at multiple levels. It's at the level of Executive Order itself and whether reform is needed in terms of a secrecy order within agencies, whether their guidance is adequate to accomplish this and whether there is a need for guidance across the government, maybe even a joint classification guidance. Mr. Masciana indicated he was looking forward to learning how these, sort of, fusion centers that are working the sharing as it is, can inform us as to their write to release, their declassification or downgrading, and what they're actually doing in practice to expedite sharing. Possibly, they might consider whether there should be a reform that sets up a whole new approach such as a modified handling procedure for this kind of information within the secrecy order. However, Mr. Masciana observed that these are longer term solutions. To reform the Executive Order would take at least a year, maybe several years. But, procedures within organizations under existing authority could be done relatively quickly to better inform the operational elements of those organizations on how to better comply with the intent of the intelligence format.

Marc Sachs added that one of the pieces that we have to not lose sight of is that this is not just a drill to change the way we declassify information for the sake of declassification. The issue is how do we get timely information to the people who need it. Whether they may be government partners, private sector partners, it doesn't matter. And if that timeliness is blocked because of classification rules, then we need to address that classification. So, that's part of what this group needs to worry about. He offered three examples to illustrate his point. First, he reported on an unclassified briefing hosted by DHS, which had maybe 6,000 people dialed into it. While it was very detailed, there were limitations on what could be discussed at the technical level because the briefing was classified. The second example was an unrelated but very similar private sector engagement. It included some of the leading cybersecurity big companies that people are familiar with. They gave a very technical—here's what we know, here's what we're seeing—briefing. But it's the private sector's view. He expressed confidence that the private sector's view and the government's view are almost identical. The government can't talk about theirs because of classified reasons, but the private sector can. It's the same technical data, but the private sector can talk about it because it's not encumbered by restrictions on classification. Marc’s third example was an announcement made very quickly by the NSA about finding of a vulnerability inside of Windows. They worked with Microsoft and got patches up to address them. That shows you it can be done. So, when this information is picked up in a very sensitive world and you recognize the impact it has, not only to U.S. infrastructure, but globally, you can fast-track it. You can get the technical information out and divorce it from how they learned about it. This shows it can be done. Mark stated that he realizes NSA likely spent a lot of time working with the legal folks to get this done, but it was done. However, that was a very costly effort they went through to get that done, and it shouldn't be that costly. It ought to be more routine to be able to do that.

Tiffany Olson Kleeman, SLTPS member, observed these are the same conversations they had when she was back at the White House in 2001 to 2003. There has been some progress obviously, including the establishment of organizations like this and others to be able to allow for other folks in the private sector, state, local, tribal territories, to have a seat at the table. However, she indicated that it is slightly disappointing to her, that further progress has not been made. Ms. Kleeman added that this isn't just about the government contributing information and intelligence to individuals in state, local, tribal, private sector entities. It's about sharing information both ways. Because as Mr., Sachs indicated, there are many private sector entities that have just as much to contribute. In many cases, though, the government cannot gain access to a lot of the information today because of its limitations and title authorities.

III. New Business

A. Department of Homeland Security (DHS) SLTPS Security Program Overview (Reference transcript pages 37–44.)
Mr. Charlie Rogers, SLTPS Vice-Chair and Chief, Compliance/Standards & Training Division, Office of the Chief Security Officer, DHS

For the benefit of the new SLTPS members Mr. Rogers provided an overview of E.O. 13549 and a summary of DHS activities under the Order. He began by stating that the purpose of the E.O. was to standardize the way in which classified national security information (CNSI) that is shared with SLTPS partners is safeguarded to make it consistent between federal agencies and the state and locals, and to ensure that the safeguarding is done in concurrence with other Executive Orders. The E.O. doesn't create whole new procedures. It connects those procedures together into a single document. The E.O. also directed the creation of an implementing directive, which amplified the content of the Executive Order in more granular detail. The Directive discusses how federal agencies are responsible for sponsoring clearances. The basic operating level of the program is SECRET. It can go higher, but that is an exceptional action based on a case-by-case decision. It formalized the governors having clearances without a background investigation. The E.O. affirms that clearances and room certifications are reciprocally accepted between agencies. It provided that states could have physical custody of classified information at the SECRET level but limited that anything above SECRET would be managed by federal agencies. It reaffirmed the National Industrial Security Program's cognizance over contractors. It established this committee, the SLTPS-PAC. It called for the establishment of a database or for a mechanism to verify clearances, which OPM stood up in the CVS in 2014.

Mr. Rogers then turned to some of the activities that the DHS is involved in with this program. There is the Cyber and Infrastructure Security Agency (CISA), which was previously called the National Protection and Programs Directorate. CISA has multiple committees and multiple interactions with the 16 critical infrastructures, involving security clearances and the sharing of cyber threat and other threat information. Within CISA there is also a new subsector, the Election Infrastructure Subsector, for which DHS is clearing election officials for all 50 states. Also, within CISA is the National Cybersecurity and Communications Integration Center (NCCIC), a 24/7 incident response and management center, for which DHS is clearing a fair number of people at the TS/SCI level. These are state, local, and private sector people who are detailed on a rotational basis to the NCCIC. CISA also has protective security advisors—subject matter experts who go out and do threat assessments-for the infrastructure in the United States. They work closely with fusion centers and also sponsor select private sector personnel for security clearances as they deemed necessary, whether they're managers of dams or electrical grids. So, DHS is involved in providing security clearances on behalf of the other protective security advisors.

The Intelligence and Analysis (I&A) directorate has the responsibility in DHS for the sharing CNSI. They are the primary interactors with the state fusion centers, of which there are like 82 right now. All the fusion centers have classified connectivity through the Homeland Security Data Network (HSDN). The DHS Office of Security has certified 65 rooms, which have HSDN connectivity and are managed by the states. There are another 15 rooms and fusion centers that the FBI manages, which allow interaction with the states, and within which the HSDN is deployed. There are also a couple of DoD facilities that are co-located with the fusion centers. Within the fusion centers, there are security liaisons; these are state and local employees who are trained by the Office of Security and the I&A to manage the classified holdings within the facilities. In July, I&A sponsored a workshop in Ohio, which was attended by 70 federal and state and local personnel who came to receive training. The FBI, the DHS Office of Security, I&A, and some of the state organizations participated in this training event.

Mr. Rogers then turned to some of the activities under the SLTPS program that are performed by his office, the Office of Security. He noted that they do security compliance reviews (SCR) of fusion centers, utilizing a checklist based on federal and DHS policy covering information security, physical security, personnel security, and operations security. When they do the SCRs, they also provide training and listen to and interact with the fusion center personnel. The Office of Security did 14 SCRs last year and expects to do 16 of them this year.

Mr. Rogers ended his SLTPS program summary by providing some basic metrics on SLTPS personnel who currently have been cleared by the DHS: 2,100 private sector personnel, and 6,200 state and local personal. It's a total of about 8,300 people that DHS has cleared in total. They are all in CVS, I will say that. Of that number, there are approximately 475 individuals that have TOP SECRET/SCI. They have that for a variety of reasons: either they sit on a particular Working Group, or they are detailed within DHS, or maybe they are working with a JTTF, or they have some other role or responsibility that requires it.

Mr. Pannoni asked Mr. Rogers how many state, local, tribal, (non NIST private sector) facilities have actual physical custody, authorization at the SECRET level? Mr. Rogers responded that the only storage that the DHS has approved is for state and local facilities. There are the 82 fusion centers. There are also a number of states that - Maryland is one and Florida is another - that have requested and been sponsored by I&A to have minimal storage. Also, there are some regional state police facilities that have a STE, in which case the DHS requires the facility to have a safe. Mr. Pannoni clarified that he was asking the question to try to make the link between an earlier discussion on sharing of cyber threat information and if there's a way to express the information at the SECRET because this program is centered around SECRET not TOP SECRET/SCI. He noted there is the issue of the actual storage requirements when accessing the information. So, if it were possible to be operated at the SECRET level where more of these places could essentially operate the access SECRET information systems like the HSDN. Mr. Rogers affirmed that HSDN is at some locations. He observed that even at the SECRET level, there is a limit to what you can share because we can't clear every executive in every company in every company in the United States. He indicated that he thinks with the cyber being able to get actionable unclassified products is going to be helpful too. Richard McComb, Chief Security Officer, DHS added that, the component heads in DHS—the Administrators, the Directors, the Undersecretaries—do have authority for one-time relations. They do that on a regular basis. He observed that part of this conversation is actually getting the system folks here to explain what they do. They do it on a regular basis through the ISACS - the Information Sharing Analysis Councils and through other venues. He noted that the briefing that Mr. Sachs talked about earlier was obviously was unclassified, with 6,000 people. So, there’s a logistics issue there with regard to how you get that out to that large number of people in that short period of time. Mr. McComb spoke again to emergency authority, reiterating that component heads do exercise that authority. He added that he does agree that there could be a more blanket emergency release type policy that might allow for something like that to happen on a quicker basis, which could be beneficial to the overall process.

B. Controlled Unclassified Information (CUI) Program Update (Reference transcript pages 44–47.)
Devin Casey, Controlled Unclassified Information Staff, ISOO

Devin Casey, Controlled Unclassified Information Staff, ISOO, provided an update on the Controlled Unclassified Information (CUI) Program, noting that it is not related to the CNSI program and that it may help facilitate and standardize the way we protect and share unclassified information. CUI is an information security reform in Executive Branch that is built on standardizing the protections for information agencies are already required to protect in accordance with law, regulation, or government wide policy.

Mr. Casey reported that most agencies are in the final stages of their policy creation phase, which is when the first domino falls for implementation at that agency. Most agencies have reported that policies will be out this fiscal year or by the end of the calendar year. There should be some pretty quick implementation CUI programs at agencies over the next year or two. It will mean that agencies will become a bit more deliberate with what they mark and protect as CUI, but they will also be pushing, perhaps, more onerous requirements to protect unclassified information.

The CUI staff currently has a lot of current engagement with the private sector. They are working on a Federal Acquisition Regulation (FAR) clause that will address CUI through contracts. There is a CUI notice that discusses the sharing of CUI through agreements. The CUI staff has met with representatives from states, including the Chief Data Officers from several states—Virginia, Florida, Texas, New Hampshire. A few CUI Council meetings have had most of the states represented, and there have been some private meetings with Chief Data Officers because a lot of agreements that agencies have will be modified to adjust to these new standards, such as the National Institute of Standards and Technology (NIST) Special Publication 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems."

Mr. Casey indicated that there is a quarterly CUI stakeholder meeting to which he offered an invitation to the SLTPS-PAC meeting participants. He advised, if they join the CUI blog, which can be found by searching for "CUI blog," they would find information of the stakeholder meeting. He encouraged state, local, tribal, private sector personnel to attend. Mr. Casey noted that there is a lot of participation from the private sector and some from state; and a lot of academia is involved as well.

Mr. Casey reported that the focus of the CUI staff is currently helping agencies implement the programs the best they can, with a specific focus on ensuring standardization through these agreements to industry, as well as to other nonfederal entities, working with DoD in particular on their plans for certifying people to work with their unclassified but sensitive information.

Mr. Pannoni added that the method that DoD is utilizing for certifying their contractors that will have access to CUI is the Cybersecurity Maturity Model Certification. DoD is moving relatively quickly, especially for the government, hoping to have a certification body or more than one body, that would then certify entities to would go out and certify the hundred or more thousand of DoD contractors that are accessing CUI. The CUI staff views it as a positive and maybe a model that the rest of the government will adopt. Mr. Casey added that they hope that this reduces confusion about the standard for protecting sensitive information outside of the federal government and it deconflicts system reciprocity when you've actually certified systems to handle this. And the hope is that the that increase in trust to protect this information will provide an avenue for things like declassification of certain things that can be shared in a wider circle, because you can see a little bit more trust in the more real walls around that newer, larger group of CUI.

IV. General Open Forum/Discussion (Reference transcript pages 47–53.)

The Chair began the open forum by discussing the importance of the SLTPS-PAC. He noted that at least once a year he is asked to justify why this committee should continue. There is a move afoot and has been for some to reduce the number of FACA Committees in the government. We always push back saying that this one is absolutely critical because it's the only forum he knows in which government and SLTPS partners to come together like this, where we try to actually not be a debating society, but actually solve problems. He continued, emphasizing that the committee is no better than who sits on it, no better than the interest people take in it, no better than the issues that are brought to it. The Chair implored everyone who sits on the SLTPS-PAC to take this committee as a real opportunity to be of service to, not only to our country, but also to their own areas. He emphasized the things the Committee tries to do and the issues they confront are not easy. They require a lot of shoulder at the wheel. He expressed his belief that with the right people in the room, and the right sensibilities, and the right civility, we can actually get something done. That's the whole point of this FACA.

The Chair reiterated something he said previously: that he would like to figure out a way to work in more of a classified element into the work of the Committee. However, he acknowledged that the SLTPS-PAC is a FACA Committee, which means it has public responsibilities. He said that he does not what that means legally. He stated that, while he is lawyer, he is not a FACA expert; so, it will be necessary to consult with our own people. It may be some sort of informal meeting. He closed by stating that whatever it is, he wants this committee to be real. He wants it to actually do something. He encouraged the new members, especially, to take an interest in this, stating that the Committee is delighted to have fresh blood, particularly such experts as the group that has recently joined. He then turned to the new members to introduce themselves.

Eric Tysarczyk, Director of Preparedness, New Jersey Office of Homeland Security and Preparedness, indicated that he oversees all of the state's infrastructure security work, their training and exercise, and their risk management efforts. His organization also oversees the state and local clearance process throughout the state; so, they are liaising with both DHS and our FBI field office. He noted that the initial discussion in the meeting was very helpful to him He reported that this is his second governor in New Jersey and that he worked for two governors in Pennsylvania, as counsel, noting that he is a recovering attorney as well. In a previous life, he was on the White House Homeland Security Council as Director for National Preparedness, as well as at DHS Headquarters in some of the early days. He spent some time in the private sector doing cybersecurity work back in the '90s. He has had a career path that has handled and dealt with information sharing and the importance of it for some time, which motivated him to come to this body and apply to try to be a part of some of those solutions mentioned by the Chair. He expressed his appreciation to be part of the Committee and stated that he looks forward to adding some value to it.

Tiffany Kleemann is the Chief Executive Officer of Distil Networks, a Bot Mitigation, Cybersecurity Company. She stated that prior to that, she was at FireEye for a couple of years through another acquisition of a company, Eye Sight Partners a cyberthreat intelligence firm. Prior to that, she was at Symantec for 10 years, running government programs and also leading the policy shop for the company. She indicated that she got there by way of a White House stint and that she served with Marc Sachs way back when. She added that she is a former Coast Guard officer as well.

Meghann Teubner introduced herself as the Director of Counter Terrorism Intelligence Analysis with the New York City Police Department (NYPD). She indicated that they are very lucky in New York in that they do not face some of the challenges that some of our other local partners face as far as access to spaces to access classified information. They have the ability to do that right in their headquarters building, which is very convenient for us. The focus in their analytic shop is on information sharing for awareness and prevention of terrorism, not only in New York, but in the surrounding areas and across the U.S. because they see their CT mission as being the CT mission of all of their partners. They do a lot of work with the private sector on terrorism tactics, indicators of mobilization to violence. They also do this now in the cyber realm and have a lot of partnerships within New York City to make sure that they are sharing all new cyber-attack factors that we are getting awareness on. So, it's really important for them to make sure that information is shared in a timely manner, because from their perspective it keeps people safe on the streets of New York City, or globally really. Ms. Teubner has been with NYPD for four years. Before that she was 10 years at the National Counterterrorism Center under the ODNI. She indicated that she excited to be on board.

The fourth new member, Mary Schechter, Director of the Division of Community and Maternal Child Health Nassau County Department of Health New York, was unable to participate in the meeting due to a last-minute meeting with her Commissioner.

The Chair then asked the members if they had anything to discuss in the open forum.

Ms. Teubner asked about how to go about getting access to HSDN. While they have access in their headquarters building, there is a unit in another facility outside of headquarters that is a High Intensity Drug Trafficking Association Space and one floor below it is a DEA Strike Force Space and they have an area in which they can access classified information. Ms. Teubner asked about the process of getting access to an HSDN System at the facility outside of headquarters. Mr. Rogers replied that they would have to work with their I&A partner would evaluate the request. Ms. Teubner indicated that they work closely with I&A, as they manage the secure space at police headquarters. Marc Sachs added that this raises a good question: if Mr. Teubner is and she is already working with I&A, how many other people don't know that's the process, and is there some way to kind of make that more widely known? Mr. Rogers noted that the fusion centers aren't really designed to centralize the classified footprint. There is a limit, and not every police department is not going to get HSDN, hopefully they're close enough to fusion centers.

Mr. Masciana recommend that the Committee share those classified mailing addresses that members already have and then they can start some exchange work that way. Marc Sachs added that having worked with several other FACA groups, he has seen that classified is not a problem. It can be done. The Chair agreed.

V. Closing Remarks and Adjournment (Reference transcript pages 53 and 54.)

After the open forum, the Chair adjourned the meeting.

Attachment 1

State, Local, Tribal, and Private Sector Policy Advisory Committee

Meeting Attendees and Teleconference Participants, January 29, 2020

Bensley, Glenn	Department of Justice Member	Teleconference
Bradley, Mark A.	Chair, Director, Information Security Oversight Office (ISOO)	Attending
Brooks, Mark	Department of Energy Member	Teleconference
Buckley, Steve	Department of Homeland Security (DHS)	Attending
Camp, Earl	FBI Obesrver	Teleconference
Casey, Devon	ISOO	Attending
Davenport, Jessica	SLTPS Member	Teleconference
Dunham, Sidonie	Department of Transportation (DOT)	Teleconference
Earring, Martin	Office of Tribal Justice, Department of Justice	Attending
Hogan, Patrick	Department of Defense Observer	Attending
Jackson, Darrell	DHS	Attending
Kerben, Valerie	Office of the Director of National Intelligence Member	Attending
Kleeman, Tiffany Olson	SLTPS Member	Attending
Masciana, Leo	Department of State Member	Attending
McComb, Richard D.	DHS	Attending
McCurdy, Patrick	Defense Counterintelligence and Security Agency (DSCA)	Teleconference
Pannoni, Greg	Designated Federal Officer, Associate Director, ISOO	Attending
Parsons, Darryl	Nuclear Regulatory Commission Alternate	Teleconference
Prasnikar, Trisha	DSCA	Teleconference
Rogers, Charles	Vice Chair, DHS	Attending
Sachs, Marcus	Vice Chair, SLTPS	Attending
Skwirot, Robert	ISOO	Attending
Stone, Nicole	DHS	Attending
Teubner, Meghann	SLTPS Member	Attending
Tysarczyk, Eric	SLTPS Member	Teleconference
Walker, Adam	DHS	Teleconference
Woolworth, Thomas E.	SLTPS Member	Teleconference
Wright, Natasha	Department of Energy Observer	Teleconference