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

SUMMARY MINUTES OF THE MEETING

The SLTPS-PAC held its eighteenth meeting on Wednesday, July 29 2020, at 10:00 a.m., by teleconference, because of access restrictions due to the COVID-19 situation. Mark A. Bradley, Director, Information Security Oversight Office (ISOO), chaired the meeting, which was open to the public. The following minutes were finalized and certified on October 28, 2020.

(The meeting minutes 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 1–6.)

The Chair welcomed the attendees and participants. He introduced a new SLTPS-entity member: Sergeant Debra Ann Winsor, Deputy Director, Washington State Fusion Center, Seattle Police Department. On the Federal side, he announced that Rich McComb, Chief Security Officer, Department of Homeland Security (DHS), has been named as the new DHS Vice Chair. The Chair thanked Charlie Rogers for the excellent work that he has done as the DHS Vice Chair and reported that Charlie will remain with the SLTPS as the DHS alternate. In addition, the Chair announced a new member from the Nuclear Regulatory Commission: Sabrina Atack, Director, Division of Security Operations, Office of Nuclear Security and Incident Response. He also announced a new member and alternate from the Federal Bureau of Investigation: Angel Catalan, Section Chief, Security Operations Section, FBI Security Division (member) and Scott Gerlach, Unit Chief, Redstone Security Unit, Security Operations Section, FBI Security Division (alternate). Lastly, the Chair reported there are two Federal vacancies on the Committee, one from the Department of Energy, as long-time member Marc Brooks, who is no longer with the DOE, and the other from the Department of Defense, a slot that has been vacant for nearly a year. (See Attachment 1 for a list of meeting participants.)

II. Old Business (Reference transcript pages 6–19.)

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

Mr. Pannoni called on meeting participants to respond to the action items from the last SLTPS-PAC meeting, which was held January 29, 2020. The action items were (1) the Federal Bureau of Investigation (FBI) will report at the next SLTPS-PAC meeting the on whether the FBI will be able to provide data to the Central Verification System (CVS) on the SLTPS personnel it has cleared; and (2) the Office of the Director of National Intelligence (ODNI) 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 Intelligence Community (IC). Mr. Pannoni also reported and led a discussion about the May 18, 2020, meeting of the Cyber-Threat Information Sharing Working Group.

A. Report on Action Item 1 from 1/29/ 2020: FBI SLTPS Security Clearances and CVS. (Reference transcript pages 8–9.)

Earl Camp, Section Chief, Suitability and Clearance Section, Security Division, FBI, reported that his office consulted with the FBI Office of General Counsel and has been cleared to share the SLTPS clearance information. He indicated that it is now a technical matter and that the FBI has been working with the Defense Counterintelligence and Security Agency (DCSA) to create a bridge so that the FBI can pass the information on a monthly basis. Mr. Camp turned to Marie Bernoi from the FBI Security Division, who is in charge of the IT portfolio team. Ms. Bernoi indicated the FBI has been actively engaged with DCSA since February to identify what is needed to prepare the data feed with the SLTPS clearance and investigative data. She reported that FBI personnel have been actively working to ensure that the appropriate data is available and that a development team is in the process of creating a script that will generate the file that will be uploaded to NP2 within the DCSA system. Ms. Bernoi indicated she anticipates that, during August and September, testing will occur between FBI and DCSA. She stated that they are preparing to go live in the first quarter of fiscal year 2021.

ACTION ITEM 1: The FBI will report at the January 2021, SLTPS-PAC meeting on the status of the effort to provide its SLTPS security clearance data to the DSCA.

B. Report on Action Item 2 from 1/29/2020: Number of SLTPS Personnel Currently Cleared by the IC. (Reference transcript pages 6–10.)

Valerie Kerben, ODNI member, reported that she re-engaged with the Chief Security Officer at the Central Intelligence Agency and confirmed with the community services group that handles the granting of Top Secret/SCI clearances for the Non-Title (NT) 50 agencies that they are unable to identify specific cases that are related to state, local, and tribal clearances. This specific information is not tracked, nor is there anything to indicate that a particular individual might be a representative from a state or local jurisdiction. Mr. Pannoni indicated that it will be necessary to revisit this issue because of the language in that E.O. 13549 order requiring the maintenance of a database for this population of cleared people. Ms. Kerben responded that they could start thinking of another way to achieve this, maybe ask those agencies how many they submit to the IC. She cautioned that the discussion of a means to achieve this would have to be discussed in a different, non-public, forum. The Chair decided to table the issue until COVID-19 restrictions were lifted sufficiently to allow ISOO to host a meeting in its SCIF to examine the issue in depth.

ACTION ITEM 2: When COVID-19 restrictions have eased, ISOO will host a meeting in its SCIF with the ODNI, and other entities as appropriate, to examine why the Intelligence Community is unable to determine the current number of SLTPS personnel that it has cleared and to seek a means obtain this information. Until then, the issue is tabled.

C. Report on the May 18, 2020, Meeting of the Cyber Threat Information Working Group (Reference transcript pages 10–19.)

Mr. Pannoni provided a summary of the discussion at the working group meeting. He noted that there were a number of subject matter experts and stakeholders in attendance from DHS, ODNI, National Security Agency, U.S. Cyber Command, Air Force, Army, Navy and the private sector. In general, the group was trying to gain a shared understanding of the issues surrounding the sharing cyber threat information, the needs of the private sector, and the processes in place in the federal government. 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. The federal participants indicated that they recognized the information must be relevant and actionable. 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. They noted that 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. There was also discussion about the need to more clearly define the problem and identify solutions that aim to better implement existing policy.

Mr. Pannoni then turned to the members to discuss the issue. Leo Masciana, Member, Department of State, noted that he pressed for the formation of 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 that needs to be solved urgently in order to protect the nation's cyberinfrastructure and government cyberspace activities. He expressed his hope that perhaps in this working group 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.

Marc Sachs, the SLTPS-entity Vice Chair, observed that the private sector gets a lot of great information from the federal government that has been rapidly declassified. However, they have a problem of figuring out which is the most important because the asset owners are also getting private sector info from various alerting sources in addition to the information they get from the federal government. Faced with multiple threats and challenges, they look at an indication from the government about which one you need to worry about—whether it's helping with prioritization or providing some context as to why a particular incident, a particular event, or a particular action or activity is more important than something else. This would help the private sector asset owner to prioritize their own investigations or their own reactions to something that's going on. Mr. Sachs observed that this does border a bit on classification, of course. However, the key 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.

Charlie Rogers, DHS alternate Vice Chair, noted that there was a fair amount of tension about the problem at the working group meeting, but the problem was anomalous and big. He opined that there is a lot of information-sharing activity in the government that we may not be aware of. He added that as the working group meetings continue, the participants need to take some time to articulate in some detail the nature of the problem and recognize what is being done effectively before they jump immediately to formulating solutions. He stated that, while there probably need to be some solutions, they should be informed with a little more detail and granularity about the nature of the problem. Rich McComb, the DHS Vice-Chair, agreed with Mr. Rogers and added there should be an effort to establish what is the as-is picture, in other words, all the current methods by which classified is provided to the private sector. He noted that in addition to the SLTPS executive order—13549—there is also E.O. 13691, "Promoting Private Sector Cybersecurity Information Sharing," and a number of other venues. He recommended getting a good handle on exactly what is being done currently as there are a lot of venues that may be underutilized at this particular time. Mr. Sachs responded that he would be happy to help with that.

The Chair asked Mr. Sachs if one of his concerns was that he was not getting enough finished intelligence product that has already been analyzed and if another concern is that there is a lack of prioritization of the threats that are indemnified. Mr. Sachs replied that prioritization is one of the key areas, along with timeless. Processed and fully analyzed, well-written, reports take too long to produce and thus are not timely enough.

Eric Tysarczyk, SLTPS member, from the New Jersey Office of Homeland Security and Preparedness, added that the challenge is that sometimes there may be an indicator of compromise with some remedial actions in the classified product and some of the technical personnel in the private sector and at the state level who are looking to discuss what the variants may be. While they do not need the sources and methods, they may need a more in-depth discussion about the indicator of compromise. They may need more information to better secure their system.

III. New Business

A. Overview of DHS Office of Intelligence and Analysis State and Local Partner Engagement

(Reference transcript pages 19–26.)

Alethea Madello, Director, State and Local Partner Engagement, Field Operations Division, Office of Intelligence and Analysis, DHS

Alethea Madello provided an overview of the information sharing activities and platforms of the Office of Intelligence and Analysis (I&A) and touched on those of other DHS offices as well. She began by noting I&A's Field Operations Division deploys intelligence officers throughout the country, typically in state and local fusion centers, which are often the first point of contact to support the information needs of the state, local, and private sectors. Ms. Madello noted that I&A's private sector partner engagement branch liaises with the Cybersecurity and Infrastructure Security Agency (CISA) at DHS, which has the primary role of working with private sector partners to provide timely intelligence. I&A's private sector branch works in tandem with CISA to host the

classified intelligence forum. I&A has also worked with 10 or 12 critical infrastructure sectors to bring those sector partners together and to provide security clearances so that they can work with I&A and CISA to develop actionable intelligence products. Ms. Madello reported that the classified intelligence forum had been on hold because of the pandemic because those meetings must occur in a classified environment but the program has been re-energized and has been able to host an unclassified intelligence forum. Ms. Madello also mentioned the Homeland Security Information Network (HSIN), which is DHS's platform where various communities of interest have been established to address these interest areas and share information. There is HSIN Critical Infrastructure (CI), which is sponsored by CISA for private sector partners, and HSIN Intel, which is I&A's intelligence portal for state and local law enforcement professionals.

Meghann Teubner, SLTPS-entity member from the New York City Police Department, complemented I&A and CISA for the bi-weekly unclassified cyber threat briefings, observing that they have been very useful help identify products that would be of interest in a number of critical areas of interest. Ms. Teubner stated the both DHS and the FBI have been doing a good job of pushing out timely information on advanced persistent threats and some of the tactics that are being used.

At the end of Ms. Madello's briefing it was determined that it would be helpful for the SLTPS-PAC to have a briefing from CISA to learn more about their information sharing activities.

ACTION ITEM 3: The DHS will arrange a briefing by the Cybersecurity and Infrastructure Security Agency (CISA) for the SLTPS-PAC membership at the SLTPS-PAC meeting in January 2021, or earlier, possibly in the fall of 2020. Charlie Rogers, DHS alternate, in consultation with Rich McComb, DHS Vice Chair, will identify the appropriate CISA personnel and help arrange the briefing.

B. Department of Homeland Security (DHS) SLTPS Security Program Overview (Reference transcript pages 26–30.)

Charles Rogers, SLTPS Vice-Chair and Chief, Compliance/Standards & Training Division, Office of the Chief Security Officer, DHS

Mr. Rogers provided a summary of the COVID-19 impacts on the SLTPS security program and a personnel security update. He noted that his division supports more than 80 fusion centers, providing direct security support, certifying secure rooms for the deployment of a classified Secret network, and performing training and oversight. Under the COVID restrictions, his office went to 100 percent telework, and travel was suspended. Initially, the staff reviewed their program, polished their checklists, updated their policies and procedures, and revalidated their processes in anticipation of travelling. When they realized they would not be able travel for some time, they began to implement remote—or virtual—audits. They anticipate performing 11 by the end of the fiscal year. While the virtual audit cannot duplicate the scope or depth of an on-site visit, Mr. Rogers believes they are important because they allow his group to work directly with the security liaisons. The liaisons complete a checklist and provide data. Then, they have a virtual meeting in which his team discusses the results of the checklist with the security liaison. While Mr. Roger's team is looking forward to getting past COVID so traditional on-site security audits can resume, they are considering supplementing the traditional audits with virtual audits which would enable them to reach more fusion centers within a given year than they could with just the traditional

audits. The Chair asked Mr. Rogers what is the level of classification of the remote audits, and he responded the they are unclassified.

Mr. Rogers also reported on the status of the fusion centers over the previous several months. His team found that about 90% of the fusion centers are working under a kind of a reduced operational tempo. A few had very limited staff and limited openings, though they were still validating alarms and checking secure rooms. 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.

Mr. Rogers closed his presentation with some personnel security metrics. DHS has directly cleared about 3,000 private sector personnel and about 5,800 state, local, tribal sector personnel, which is a total of about 8,800 personnel. They are primarily cleared at the Secret level. At the Top Secret and TS/SCI access there are about 700 people. Not all of them have TS/SCI. For TS/SCI there are roughly 125 to 150 private sector and 250 are state & local personnel.

C. Controlled Unclassified Information (CUI) Program Update (Reference transcript pages 31–36.)

Devin Casey, Controlled Unclassified Information Staff, ISOO

Devin Casey, Controlled Unclassified Information Staff, ISOO, provided an update on the Controlled Unclassified Information (CUI) Program. He began by providing some key points on the CUI program from ISOO's 2019 Annual Report to the President. The report indicated that most agencies will be issuing CUI policies by the end of this calendar year, which is a key step toward implementing their CUI programs. He noted that agencies have made significant progress but also that there have been varying timelines, which have raised some concerns about the timeliness of the implementation of the program. In response, ISOO issued deadlines for implementation in a CUI notice this year. Another key point from the Annual Report it that it acknowledged that there are insider threats to CUI and agencies are looking for policy solutions to help them address those threats. The CUI staff has been working on this issue with the Insider Threat Task Force and a working group at the Office of Management and Budget.

Mr. Casey reported that the National Institute of Standards and Technology has issued a draft of the NIST 800-172, formerly known as the NIST 800-171B, which is an additional set of controls and enhanced security requirements for protecting controlled unclassified information that can be used as a supplement to the 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 that are potential targets for advanced persistent threat. The controls in this 800-171 are designed to address differing advanced persistent threat based on threat reporting from those critical programs or the high-value assets as identified. He announced that the draft was out for public comments, which were due by August 21, 2020.

Mr. Casey also reported that the CUI Office and the CUI Advisory Council have been working with the National Information Exchange Model (NEIM) to create a CUI metadata standard. He noted that CUI does not require metadata marking, but they wanted to work with NEIM on 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. The expectation is that many agencies will voluntarily apply those standards, use those standards, or reference them in the creation of similar standards.

Mr. Casey reported that the CUI FAR case has been updated in the unified agenda and that the comment period is expected to be from October to December of this year. He noted that the CUI FAR will expand the CUI requirements to the entire executive branch that falls under the FAR. Mr. Casey closed his presentation with an invitation to join the CUI blog which can be reached via https://www.archives.gov/cui or at https://isoo.blogs.archives.gov/.

Mr. Masciana asked about deadlines for implementation of the CUI program. Mr. Casey responded that the CUI office issued CUI Notice 2020-10, "CUI Program Implementation Deadlines," which establishes dates when CUI program implementation activities should be completed by an agency. If agencies do not meet the deadlines, they are required to indicate in their annual report to the CUI office the cause of the missed deadline and when they will meet the deadline with a plan for how to accomplish the implementation.

Mr. Masciana inquired as to when it is permissible to begin using the CUI marking on documents. Mr. Casey responded that the CUI markings can be used once an agency has implemented the program and allowed for the use of the CUI marking, which generally comes after both the policy has been issued and training is completed. He noted that some agencies, such as the Department of the Interior, have already begun marking. He advised that during the time when some agencies have the CUI program and others do not, agencies should continue to use their legacy programs to protect their sensitive information. If such agencies receive CUI from another agency, they use the most equivalent of their legacy programs to protect that information. Agencies that have implemented their CUI programs have been instructed that, if they receive information from an agency that uses legacy markings, they should protect that information under the CUI program for now.

IV. General Open Forum/Discussion (Reference transcript pages 36–44.)

The Chair began the open forum by asking two new members to introduce themselves to the membership: Mary Michelle Schechter, Director of the Division of Community and Maternal Child Health, Nassau County Department of Health, New York; and Sergeant Debra Ann Winsor, Deputy Director Washington State Fusion Center, Seattle Police Department. They spoke about their backgrounds and indicated that they are honored to be on the Committee.

Mr. Sachs began the open forum discussion by raising the topic of access to classified information by personnel working at home. While noting that he recognizes this is primarily a government policy issue, he stated that it does affect the private sector because the COVID-19 situation makes ready access to classified information impossible. He indicated that he was aware that the DoD has been working on policies on how to handle Secret level information from home. Because the expectation is that COVID would not be going away soon, he expressed curiosity about whether other agencies are exploring the same issue.

Ken Polk, I&A, DHS, indicated that leadership within his office is exploring the issue. He counseled that a lot of work would need to done to make this happen. He indicated that he thinks that there needs to be consistent policy or procedures established across the board, so, the DoD is

not doing one thing, DHS something else, and DNI or whomever doing another thing. He observed that there are not a whole lot of policies, procedures, or good practices to follow that have been identified. Darryl Parsons, alternate member from the Nuclear Regulatory Commission indicated that his agency has taken a look at the issue but has no current plans. Mr. Pannoni added that he believes that the Committee on National Security Systems, which is an inter-agency government group focusing on the policies for use of information systems, already has some policies on remote access using mobile devices. The Chair noted that the impact of COVID is going to echo for a long, long time. He concluded that it would be beneficial to pull policies together and see exactly what they say now, what they permit, and more importantly, what they do not permit. He indicated that this is a timely and useful subject to begin to probe.

ACTION ITEM 4: ISOO will seek to identify and review policies relevant to discussions about allowing access to classified information at home to ascertain what the policies permit and what they do not permit.

Several other issues were briefly discussed near the end of the open forum discussion. Mr. McComb noted that as staff has been working remotely during the pandemic there has been an increase in security incidents and unauthorized disclosure of sensitive but unclassified information to the public media and advised agencies to be aware of this trend. Mr. Masciana drew attention to an increasingly common pattern and practice of shifting unclassified information to classified security domains, which hinders sharing with state and local partners and between and among federal agencies. Mr. Sachs inquired regarding the scheduling of a follow up meeting of the Cyber Threat Information Sharing Working Group, which last met in May. Mr. Pannoni replied that yes, a meeting would be scheduled prior to the next SLTPS-PAC meeting.

ACTION ITEM 5: ISOO will schedule and hold the next meeting of the Cyber Threat Information Sharing Working Group prior to the next SLTPS-PAC meeting.

V. Closing Remarks and Adjournment (Reference transcript page 44.)

The Chair announced that the next SLTPS-PAC meeting will be held on Wednesday, January 27, 2021, 10:00 a.m. to 12:00 noon and adjourned the meeting.

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

Teleconference Participants, July 29, 2020

Glenn Bensley	Member, Department of Justice
Marie Bernoi	Participant, Federal Bureau of Investigation (FBI)
Mark Bradley	Chair, Director, Information Security Oversight Office (ISOO)
Earl Camp	Participant, FBI
Devin Casey	Presenter, ISOO
Angel Catalan	Alternate, FBI
Kate Connor	Alternate, Department of State (State)
Jessica Davenport	SLTPS Member
Sidonie Dunham	Member, Department of Transportation
Ricardo Duron	Observer, Department of Homeland Security (DHS)
Christopher Fagan	Observer, DHS
Scott Gerlach	Alternate, FBI
Mark Hojnacke	Observer, Department of Energy
DeRinda Johnson	Observer, DHS
Valerie Kerben	Member, Office of the Director of National Intelligence
Tiffany Kleemann	SLTPS Member
Carolyn L.	Observer, Central Intelligence Agency
Natasha Lewis	General Dynamics Information Technology
Alethea Madello	Presenter, DHS
Leo Masciana	Member, State
Rich McComb	Vice Chair, DHS
Keith Minard	Member, Defense Counterintelligence and Security Agency
Greg Pannoni	Designated Federal Officer, Associate Director, ISOO
Kenneth Polk	Observer, DHS
Charlie Rogers	Alternate, DHS
Michael Russo	Observer, Department of Defense
Marc Sachs	SLTPS Member
Mary Michelle Schechter	SLTPS Member

Robert Skwirot	ISOO
Rowdy Spuesens	Observer, DHS
Nicole Stone	Observer, DHS
Meghann Teubner	SLTPS Member
Eric Tysarczyk	SLTPS Member
Antoine Washington	Observer, DHS
Aaron Weidner	Observer, DHS
Debra Winsor	Observer, DHS
Tom Woolworth	SLTPS Member