STATE, LOCAL, TRIBAL, AND PRIVATE SECTOR POLICY ADVISORY COMMITTEE (SLTPS-PAC)
July 25, 2018

SUMMARY MINUTES OF THE MEETING

The SLTPS-PAC held its fifteenth meeting on Wednesday, July 25, 2018, 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 November 16, 2018.

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

I. Welcome, Introductions, and Administrative Matters (Reference transcript pages 1–6.)

The Chair welcomed the attendees and participants, and reminded the assembly that this committee was authorized by Executive Order 13549, "Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities," and that its purpose was to safeguard and govern access to classified national security information shared by the government and SLTPS entities. He noted that the meeting was being recorded and that a copy of the minutes/transcript would be provided to the public via the ISOO website. He introduced five new members who have joined the SLTPS-PAC this calendar year: Tom Carr, Executive Director, Washington/Baltimore High Intensity Drug Trafficking Area Program; Marc Sachs, Chief Security Officer, Pattern Computer; Doug Reynolds, Vice President of Security Operations, Mall of America; Hans Olson, Assistant Secretary for Homeland Security, State of Massachusetts, who joined the meeting via teleconference; and Erik Galow, Information Sharing Lead, Office of Data and Information Sharing, Federal Bureau of Investigation (FBI). The Chair reminded the assembled that the blue folders they received upon arrival at the meeting contain copies of the meeting agenda, the slides for one of the meeting presentations, and the minutes of the last meeting. (See Attachment 1 for a list of the attendees and 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 reminded the committee that as a result of the single action item from the last meeting, a working group of federal SLTPS-PAC members was convened to study the multiple separate and unconnected security clearance databases in the Executive branch and the effect this has on effective clearance reciprocity. (See the SLTPS-PAC's January 24, 2018 meeting minutes, pages 1-2, for a synopsis of this action item.) He then called on Mark Pekrul, National Background Investigations Bureau (NBIB), Office of Personnel Management, to update the committee on any action item-related discussions that the SLTPS-PAC working group or any of its membership had with the FBI. Mr. Pekrul pointed out that many of the individuals in the SLTPS community hold clearances through the FBI, and that it isn't just a matter of the SLTPS community having access, but also the access of their federal sponsors. That is, if a state government employee with a

clearance from the FBI wants to gain access to classified information at another agency, that agency sets about to verify the clearance. Here the agency may become thwarted, as the clearance is not loaded into either the Central Verification System (CVS) or the Joint Personnel Joint Personnel Adjudication System (JPAS), the two clearance databases to which most agencies have ready access. The FBI loads its clearance information into Scattered Castles, which not all agencies have, or know they have, or can access. Doug Reynolds, SLTPS member, shared his experience as a private-sector individual with an FBI-sponsored clearance, indicating that for 12 years he has been coming to DC, and for 12 years, agencies have not been able to find his clearance information.

Mr. Pannoni then called upon Erik Galow, FBI, to provide updates on the FBI's progress towards solving this dilemma. Mr. Galow noted that both the Chief Data Officer and the Chief Information Officer at the FBI have become actively engaged in the issue and that as a result it has been escalated to the higher echelons of the Bureau's national security apparatus. In addition, he is aware of a National Security Council subcommittee that is studying this issue in an attempt to consolidate an effort to place such information into a single location, but that as yet no firm strategy has been established. He also indicated that he was not aware of any specific measures that the FBI security division has taken to independently push FBI-vetted individual data from Scattered Castles to CVS or to JPAS. Charlie Rogers, DHS, stated that fusion center personnel, who often need clearance information quickly, are only certified at the Secret level, and thus cannot access Scattered Castles, and that the DHS has no means to change this condition. Valerie Kerben, Office of the Director of National Intelligence (ODNI), stated that she knows of no ODNI effort to downgrade the required Scattered Castles database information. At the end of the discussion, Mr. Galow indicated he would meet with security division personnel after the meeting to try to formulate a plan moving forward, at least in the short term.

Action Item: Erik Galow, FBI, will meet with FBI security division personnel to formulate a plan to remedy the current situation in which clearance information for SLTPS personnel sponsored by the FBI is often not readily available to agency and SLTPS personnel because it is provided only to Scattered Castles and not to the CVS or JPAS.

III. New Business

A. SLTPS Security Program Update (Reference transcript pages 19-40.)
Mr. Charlie Rogers, SLTPS Vice-Chair and Chief of the DHS's SLTPS Management Division

Mr. Rogers, DHS, provided updates on the SLTPS security program by way of a summary of its implementation as established in Executive Order (E.O.) 13549, "Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities." He discussed classified engagement, which is primarily facilitated through nationally organized Fusion Centers, which facilitate the flow of classified information from federal agencies to state, local, tribal, and private sector entities. He also described the compliance review program, enrichments in security liaison roles and responsibilities, and training program improvements, and provided updates related to DHS's ongoing efforts to encourage robust communication and cooperation between SLTPS and federal personnel security initiatives. He pointed out that at present there are approximately 8,000 Secret-level cleared SLTPS personnel throughout the nation who were sponsored by the DHS, approximately 320 of whom are cleared at the Top Secret/Sensitive Compartmented Information (SCI) level. (See transcript pages 19-32.)

Following Mr. Roger's presentation, the Chair asked the members to reflect on the eight years since E.O. 13549 was issued and consider if there is anything that was missed or needed to be fixed or improved. Marc Sachs, SLTPS member, opened a discussion about the difficulties faced by private-sector individuals trying to navigate the clearance process. They do not understand the process and once cleared, they have no idea of how to pass a clearance. He suggested the FBI and the DHS might have a sort of concierge service wherein SLTPS personnel might speak with live individuals on matters related to security clearances. The Chair commented that it was a good suggestion. Mr. Pekrul added that his organization, NBIB, has a public-facing website (https://nbib.opm.gov) that has a wealth of information about the clearance process.

Leo Masciana, Department of State member, discussed classified information that's being shared and the appropriate levels of it. He also mentioned related issues of tear lines, downgrading, declassification, and write-to-release. He noted that there has been discussion in the press about whether classification, particularly classification level, has become a barrier to what is now a priority of the Trump Administration to deter bad actors in cyber attacks and suggested that this is an area appropriate for this group to be considering.

B. An Overview of the FBI's Information Sharing Mechanisms and Better Cyber Hygiene Practices (Reference transcript pages 40-67.)
Mr. Edward M. Parmelee, Supervisory Special Agent, Mission Critical Engagement Unit, Cyber Division, FBI

Special Agent Parmelee described his unit's main objective as pushing intelligence information to private sector and government agencies in exchange for pulling intelligence from them and subsequently feeding it to other operational units. He noted that this approach is designed to stop, thwart, and/or dismantle national-level inbound cyber threats. In practice, pursuit of this objective often depends on individuals engaging with the local FBI field office. (See transcript pages 40-67.) He explained that the FBI Cyber Division is trying to be as transparent as policy and the law allows, and that their strategy is based on the concept that the world is not as big as we think and that everything is interconnected. The FBI has been designated as the lead federal agency for investigating cyber threats and crimes. It wants to stop people from being victimized and to thwart the constant and pervasive attacks against the nation's national security. He described several initiatives to accomplish these objectives, including the National Cyber Investigative Joint Task Force, which partners with federal agencies to collect and share information and help thwart cyber-attacks against the nation and its infrastructures; the National Cyber-Forensics and Training Alliance, a non-profit group that is comprised of government, private sector, and academia that collects information and helps stop emerging cyber threats; the Cyber Behavioral Analysis Unit, which is the cyber element of the FBI's well-known Behavioral Analysis Unit, charged with building psychological profiles of cyber actors and then assisting in investigations and developing technical support for those investigations; the FBI's Cyber Action Team, a group of highly experienced and technically proficient FBI staff, that travels to investigate major incidents; the FBI Liaison Alert System (FLASH), which produces technical documents meant to make information technology specialists or chief information security officers aware of new threats by providing document compromise indicators and technical information that can utilized to harden information systems; Private Industry Notifications (PIN), which are less technical than the FLASH; and intensive outreach with Information Sharing and Analysis Centers (ISAC). He explained that these are but a few of the resources the FBI can provide to fight and survive cyber-attacks. In addition, Special Agent Parmelee encouraged enterprises at all levels to keep policies up-to-date and to report

infrastructure attacks, as the more that is known the more effective can be the solutions. He urged all entities to be constantly vigilant in looking for ways to improve security, to train employees to recognize and act against cyber-attacks and to question unusual business practices. He encouraged entities and individuals to develop relationships with the local ISAC and other sector-specific organizations, as well as utilizing cross-sector resources like the FBI-managed InfraGard. He advised them to develop and test an incident response plan; to consider using multi-factor authentication; and to consult the National Institute for Science and Technology website for excellent information about preventative maintenance and cyber hygiene best practices. Leo Masciana, Department of State, asked Agent Parmelee if the Cyber Action Team was international in scope. Agent Parmelee indicated that the team could go out and assist an ally. However, much coordination is required, and action must be initiated by a formal request. Finally, he explained that there are cyber-specific assistant legal attaches assigned around the globe and noted that the Cyber Division is trying to expand its presence into every embassy it can, as it is important interact with local governments on a cyber-centric basis and through cyber investigations, much like already is being done on the counterterrorism front.

C. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information (CUI) in Non-federal Information Systems and Organizations"

Mark S. Riddle, Controlled Unclassified Information Staff, ISOO

Mr. Riddle began by presenting a brief historical overview of the CUI program. (See Attachment 2.) He described CUI as information protected due to the existence of a law, regulation, or government-wide policy that calls for its protection against unauthorized access. He spoke at some length about the standards that govern the protection of CUI owned by Executive branch agencies, to include the need to protect that information created and stored on information systems. (See transcript pages 69-76.) He indicated that the NIST SP 800-171, published in June of 2018, established the technical standards for protecting CUI in the non-federal environment, and he noted that this standard is a reflection of the moderate confidentiality impact value that Executive branch agencies have decided is appropriate for the protection of CUI in both the federal and non-federal environment. In addition, ISOO has been working with an interagency group to develop the required Federal Acquisition Regulation (FAR). Once finalized and fully implemented, the FAR will standardize the way the executive branch communicates safeguarding guidance standards to non-federal entities. Mr. Riddle noted that, in the development of the NIST SP 800-171, it was determined that, although the same standard of moderate confidentiality would apply to federal and non-federal systems, requirements that were uniquely federal, such as continuity of operations, continuity of government, and other government documentation, would not be required for non-federal systems. In due course, the NIST SP 800-171 would include lists of both moderate baseline controls as well as the ones excluded from the final document. Another NIST document published later in that same month, the NIST Special Publication (SP) 800-171A, "Assessing Security Requirements for Controlled Unclassified Information," is an assessment guide for the NIST SP 800-171 and is to be used by agencies to assess compliance to these standards. Non-federal entities can also use this publication to conduct their own internal self-assessments, as it contains the answers to fundamental questions regarding systems configuration. Also, both the NIST SP 800-171 and the NIST SP 800-171A were modified to include an expanded explanation of each security requirement.

Mr. Masciana described two situations and inquired if encryption would be required for CUI in such conditions. Mr. Riddle indicated that there are specific requirements for encryption in the moderate baseline in both circumstances. He noted that as implementation is moving forward there are issues with the compatibility of encryption software that need to be addressed. Mr. Masciana asked about deadlines for compliance with the systems requirements. Mr. Riddle replied that there is flexibility in this area. Agencies must report on the status of their implementation efforts. With regard to systems, agencies have been asked to develop a plan for the transition to the CUI standards. There must be a plan in place to get to the point where all of the agency's systems are compliant.

IV. General Open Forum/Discussion (Reference transcript page 89.)

The Chair called for any further matters that a Committee member or guest wished to offer for discussion. Mr. Sachs spoke about tear-lines, noting that a lot of the Cyber intelligence information is issued as Top Secret/Sensitive Compartmented Information and the system administrators who need this sort of information are generally not cleared. He asked if tear-lines could be a topic of future discussions. Mr. Masciana, added this relates to the point he raised earlier about classification as a potential barrier to sharing cyber-threat information and noted that it has already been identified as such in the 2017 National Security Strategy. He suggested that the group should take an initial look at this. The Chair agreed.

V. Closing Remarks and Adjournment (Reference transcript pages 90.)

The Chair reminded everyone that the next SLTPS-PAC meeting would be held on Wednesday, January 30, 2019, 10:00 a.m. to 12:00 noon, at the National Archives, and the one after that would be held on Wednesday, July 24, 2019. The meeting was adjourned at 12:08 p.m.