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

SUMMARY MINUTES OF THE MEETING

The SLTPS-PAC held its tenth meeting on Tuesday, July 22nd, 2015, at 10:00 a.m., at the National Archives Building, 700 Pennsylvania Avenue, NW, Washington, DC. John Fitzpatrick, Director, Information Security Oversight Office (ISOO), chaired the meeting, which was open to the public. The following minutes were finalized and certified on December 9, 2015.

I. Welcome, Introductions, and Administrative Matters

The Chair welcomed the attendees. He reminded them that all SLTPS-PAC meetings are recorded events subject to the Federal Advisory Committee Act and that a transcript of the meeting would be made available through the ISOO website. He also stated that this meeting is the third iteration of a virtual meeting; he noted that the meeting folders included the agenda for this meeting and the minutes from the last meeting.

The Chair introduced the new SLTPS member, Mark Schouten, the Director and Homeland Security Advisor from the Iowa Department of Homeland Security (DHS), and thanked him for his attendance in person. The Chair noted the departure of several members: Will Pelgrin from the Center for Internet Security; Marcus Brown from the Maryland State Police; and Tim Davis from the Department of Defense. The Chair solicited the Committee members for nominations to fill the SLTPS vacancies and reminded the Federal government members to submit their financial disclosure forms. Joan Harris of the Department of Transportation asked what are the criteria and expectations for the SLTPS members. The Chair responded by recalling that the SLTPS-PAC was established to monitor the information security and information sharing aspects related to providing classified information to state, local, tribal, and private sector entities. So, the Committee is interested primarily in the security support functions that enable this, such as security clearances and training and how to support personnel in non-federal environments that have been granted access to classified information. From a mission standpoint, the interest is in the entities that interact and partner between federal and non-federal actors in homeland security, counter-terrorism, and national defense. The Chair advised that the SLTPS-PAC staff would email the SLTPS-PAC members an invitation to provide nominees, which would include information about the criteria for membership and the makeup of the membership. (See Attachment 1 for a list of members and guests in attendance.)

II. Old Business

Updates from the Designated Federal Officer (DFO)

Greg Pannoni, DFO, began by reminding the membership that, due to Federal budget constraints, the reimbursement of travel expenses continues not to be possible and encouraged future Committee participation via teleconference. He stated there were no action items from the previous meeting.

III. New Business

A. SLTPS Security Program Update

Charlie Rogers, Vice-Chair, DHS, opened by giving an overview of the state of the Security Compliance Review (SCR) Program, which was established in 2012 to review locations where DHS has deployed a classified system or has certified a room. He indicated that DHS will have completed a total of 52 SCRs by the end of this fiscal year and will have conducted SCRs in all the locations where the Homeland Secure Data Network is deployed in state government controlled space.

Mr. Rogers then discussed training for security liaisons. The security liaisons are required by E.O. 13549, "Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities," and are essential for the security of classified information at state and local locations. Training is crucial to ensure the liaisons have sufficient expertise. Mr. Rogers explained that there are two short-term mechanisms for training that were developed by his staff and their partners in the DHS Office of Intelligence and Analysis (I&A). One is webinar training, in which newly-appointed security liaisons log on the Homeland Security Information Network to learn about their responsibilities. The second, which is more robust and is funded by I&A, entails bringing security liaisons to DHS headquarters for a two-day training event with sessions by the Office of Security and I&A, and with guest presentations by experts in communications security, operations security, and counter-intelligence. Nine security liaisons attended the two-day training in 2014, and 15 attended, in two sessions, in 2015. Mr. Schouten asked if the liaisons were primarily from fusion centers. Mr. Rogers responded in the affirmative but indicated that DHS would like to expand the training to others.

Mr. Rogers reported on plans for a national fusion center security liaison workshop that would be held in Washington, DC, in November of this year, and sponsored by I&A, provided the funding is approved. The DHS has done several of these workshops over the past few years. The workshop lasts two and a half days and typically attracts about 80 or more security liaisons. The liaisons receive training on their security liaison responsibilities and other government issues such as insider threat and cyber-security. It also gives the liaisons an opportunity to express their concerns. Mr. Schouten asked if the workshop was open to more than just fusion center liaisons. Concerned that an important group of stakeholders might be missed, he noted that the Homeland Security Advisor is not always associated with a fusion center. In his state, his office is associated with emergency management, not with the state police or the Department of Public Safety. Actions such as passing clearances are done through his office rather than through a fusion center. So, by limiting invitations to the fusion center liaisons, the workshops would be missing personnel who would benefit from the training. Mr. Rogers responded that the workshop is currently aimed at fusion centers but there have been discussions about opening it up to the governors' offices. Because the responsibilities of personnel in the governors' offices would not require them to have the full range of training, there was some thought of bringing them to the workshop for one day, but this would depend on the availability of funding.

Mr. Rogers provided a personnel security update, reporting that, since 2003, the DHS has cleared approximately 2000 private sector and 5000 state and local personnel. Currently, about 350

individuals have Top-Secret (TS) or TS-Sensitive Compartmented Information access, many of whom are working with the Joint Terrorism Taskforce (JTTS). This is down from 450 a year ago. He noted there had been an effort on the part of the sponsors to ensure that those who have an active clearance still require it and that accesses are not held beyond what the need is.

Mr. Rogers reported that the DHS is writing a security liaison manual that will consolidate guidance that has been issued in policy and guidance documents. The manual will help the liaisons understand their job requirements, and provide their Federal points of contact. Similarly, a manual will be created for field security coordinators to bring together guidance on how to perform compliance reviews and how to certify rooms. These manuals will be useful to fill the knowledge gaps left by personnel turnover and will serve as a supplement to the training program.

Mr. Rogers then briefly talked about the Insider Threat Program, noting that the DHS has developed protocols to monitor its' classified systems, which eventually will incorporate state and local partners who access classified systems in the field. He reported that the DHS has started the program internally and that once it is fine-tuned it would be migrated out. Mr. Rogers indicated that the DHS would provide its partners training on the program and their responsibilities under it. Mark Pekrul, Department of Energy (DOE), added that there is much emphasis on insider threat in all constituencies of government. National policy requires everyone to get training and understand what their responsibilities are for the protection of classified information systems, what activities are occurring on those systems, how systems are monitored, how consent for monitoring occurs, and what the responsibilities of cleared individuals are for reporting suspicious activity. While these are traditional personnel and information security concepts, they are wrapped in a new package of insider threat policy with an increased emphasis on awareness and training.

B. Central Verification System (CVS) Security Liaison User Role Update

With Trisha Prasnikar and Carol Morehart of the Federal Investigative Services Division, Office of Personnel Management (OPM), on teleconference for support, Mr. Rodgers provided the Committee an update on the security liaison user role, which is now a function within the CVS. E.O. 13459 required the creation of a mechanism to verify clearances to enable states to conduct classified meetings. Early on, the OPM agreed that the CVS would be the best system in which to create this functional area and volunteered to create it. This effort was rolled into a modification of CVS that was already underway. Mr. Rogers emphasized that the OPM did the hard work. A working group, which included private sector, state, local, and Federal Government members, issued a requirements document. There were negotiations with the Department of Defense (DoD) to determine how to interface with the Joint Personnel Adjudication System (JPAS). Mr. Rogers noted that the portal is designed to give specific kinds of information, not wholesale access to the CVS, and, while it has a portal to JPAS, it provides access only to the information that is necessary to verify clearances. A pilot program for testing was started on July 13, 2015, with about a dozen people who will test the new portal for the month of August. After the pilot, the remaining security liaisons would be added in increments. Mr. Rogers estimated that there would be total of approximately 125 or 150 accounts. He added

that the OPM also created a webinar and a manual on how to use the portal. The liaisons must complete the webinar and review the manual before they can gain access.

Mr. Pekrul asked if the capacity was built into the portal to include novel data fields in which agencies can capture specific information for inclusion in the CVS. Ms. Prasnikar responded that fields that had been requested for data had been built in the system; the fields are ready for DOE to populate them.

C. OPM Data Breach

The Chair provided basic information about the OPM data breach and the remediation activities for it. He opened by stating the best source for information on the data breach and the government's on-going efforts was opm.gov/cybersecurity. He explained that there were two distinct data breaches. The first breach was of a repository of current and former Federal employee and retiree personal information affecting 4.2 million distinct identities. For those affected by this first breach, the government had rich and current contact information. So, OPM was able to notify them of the breach and of the identity protection and remediation services.

News of a second breach broke as notifications of the first breach were being made. The second breach affected 21.5 million individuals who completed a Standard Form (SF) 85, SF 86P, or an SF 86 in association with a Federal background investigation. He explained that the second breach included social security numbers as part of the compromised information. He also noted there is a separate population of minor children included in the second breach population.

The Chair reported that notifications had not gone out to those affected by the second breach as of yet. There was an issue in that some of the contact information for these individuals was over 15 years old. He explained that the government was in the process of deciding how it will acquire and pay for the identity protection services and reported that there would be a notification system or series of systems announced.

Mr. Schouten asked if the 7000 individuals with state and local clearances that Mr. Rogers spoke of earlier would have been subject to the breaches. The Chair stated that it would be safe to assume so, even though there is no firm information to confirm that at the moment.

The Chair noted that members of the National Industrial Security Program Advisory Committee (NISPPAC) have been getting ISOO notices that advise them of a government release that relates to their interests and suggested we should try to replicate that for the SLTPS.

Mr. Schouten asked if those that have separated from their employment would have been purged from the system. The Chair stated that he was unaware that current clearance status has any bearing on inclusion in the population. The likely scenario is that once your information is in the system it remains there.

Mr. Schouten inquired about the operational security implications of the second breach. Does the governor's office need to do anything differently about its staff that travel to China or about those who travel from China to the governor's office? The Chair noted that this question allows

us to draw a distinction between what are the Privacy Act and related statutory requirements regarding the government's responsibility to the affected citizens and what are the counter-intelligence implications and the potential damage to national security that are associated with a loss that involves a population of citizens with ties to national security. The National Counter-Intelligence Security Center (NCSC) has created a brochure, which can be accessed via the OPM website that has smart reminders of the ideas that Mr. Schouten is suggesting. When thinking about contacts made with foreigners in ordinary life, consider if the character of that interaction might change or if there is a need to heighten awareness if it does. The brochure includes things to think about, ways that an individual can tune into indicators, and what to do if there is a concern. The "see something, say something" concept applies here. There are financial and counter-intelligence implications for the breach and people are watching for both. The Chair suggested to Mr. Rogers that this topic may be a good one for the security liaison workshops and that outreach to the NCSC might be helpful to bring this subject to this population.

D. Controlled Unclassified Information (CUI) Program

The Chair provided a CUI program update for the group. He noted that the CUI program was instituted in the Bush administration for the SLTPS community and focused primarily on counter-terrorism and homeland security information sets and the problem of dozens or more different markings and many conflicting and inconsistent handling requirements associated with providing information security for unclassified information. The Obama administration broadened the approach by recognizing that the government has many other types of information that share the same problems. The Chair stated that the National Archives and Records Administration, which is the executive agent for the CUI program, through ISOO, is in the process of developing Federal regulations, guidelines, and other types of guidance for agencies on what should be identified as unclassified but requiring safeguarding or dissemination control and what cannot and on how the information should be marked. The intent is to reflect a single approach for all of the government, promote efficiency and effectiveness, and reduce duplication and conflicting guidance. He noted that, for a couple of years, a registry of information types that qualify as CUI has been posted on the CUI website. The registry, which can be viewed at archives.gov/cui, contains 23 broad categories, 82 subcategories, and 315 laws, regulations, and government-wide policies that provide authority for a Federal agency, department, or official to place controls on unclassified information. The line that divides CUI from non-CUI is whether or not there is a law, regulation, or government-wide policy that grants the authority to designate the information.

The Chair explained that 32 CFR Part 2002, which would be the regulation for CUI, had been proposed formally through the Federal Register and Office of Management and Budget processes after extensive Federal Government agency coordination. It went into the Federal Register in May for 60 days of public review and comment. The 60 day public comment had closed a few weeks ago with 245 comments received from the public. The comments came from trade associations related to government contracting, academic organizations that primarily perform research on behalf of Federal agencies and institutions, the legal community that provides support to companies and trade associations performing contract business with the government, and the open-government advocates. The Chair explained the CUI staff was currently working

through the comments and addressing them as required. He stated that they expect the final rule to be issued early in calendar year 2016.

The Chair reported that 32 CFR Part 2002 provides instructions on marking, on designation, on when information should be decontrolled, and on how dissemination controls work. He noted that, as a Federal regulation, the rule will be binding on all Federal agencies. Because the department and agency heads have partnerships with non-Federal entities, there is language in the rule that is pertinent to the discussions in the SLTPS-PAC. The intent of the rule is to eliminate unnecessary or unclear restrictions on information and ensure that sharing happens and that it happens in a secure way. One of the expected outcomes is that less unclassified information will bear control markings at all.

The Chair reported that the rule also specifies the responsibilities of Federal agencies. He explained that when information is shared with non-Federal partners the burden is on the Federal agency to manage expectations of protection when the information is shared at the other end. Compared to classified information, for which the rules are clear-cut and well defined, CUI is less rigid and the standards for protection are less onerous. Nevertheless, the issues are the same: with whom can the information be shared, what must be done to protect it, and when can it be provided to someone else. Currently, when Federal agencies share CUI with non-Federal partners, it may be through formalized, regimented contractual requirements or in a less rigid arrangement. The rule has been written to reflect the discretion that exists today that allows the Federal agencies to engage different characters of non-Federal partners in different sharing arrangements.

The chair noted that there is much concern about how CUI will be handled on information systems. He reported that the National Institute of Standards and Technology has published, in partnership with the ISOO CUI office and the DoD, a set of standards for the protection of CUI in non-Federal information systems and organizations. This matches the Federal Information Security Management Act and other requirements that the government has for itself and puts in place for non-Federal partners, when relevant.

The Chair requested that Bob Skwirot send a copy of the current proposed rules to the members of the SLTPS-PAC to view the comments and follow up with questions if they had them. With that he concluded the CUI brief and opened the floor to questions.

IV. General Open Forum/Discussion

Clyde Miller asked if there were findings from the security compliance reviews that Mr. Rogers discussed. Mr. Rogers explained there have been findings, which are based on whether the facility is in or out of compliance with national policy. Reports are sent to fusion center directors, with copies to I&A. The centers are given 60 days to address the issues. The findings and their remediation are tracked in a database. Mr. Rogers explained that while the SCRs had found minor issues they had not thus far found a vulnerability to the protection of classified information. The Chair then solicited final questions and comments from all in attendance. The SLTPS-PAC attendees did not pose any additional questions or raise any points for discussion.

IV. Closing Remarks and Adjournment

The Chair thanked everyone for attending the meeting and for their contributions. He announced that the next SLPTS-PAC meeting would be held on Wednesday, January 27, 2016, followed by a meeting on July 27, 2016. He closed by reminding the members that they would be receiving a request for nominations and getting information about the CUI program and that the Federal members would get a reminder about submitting their ethics forms. The meeting was adjourned at 11:16 a.m.

Attachment 1

SLTPS-PAC MEETING ATTENDEES/PARTICIPANTS

The following individuals were present at the July 22, 2015, SLTPS meeting:

• John Fitzpatrick	Information Security Oversight Office (ISOO)	Chairman
• Greg Pannoni	Designated Federal Officer (DFO) (ISOO)	DFO
• Clyde Miller	SLTPS Entity Representative	Vice-Chair
• Charles Rogers	Department of Homeland Security (DHS)	Presenter
• Mark Pekrul	Department of Energy	Alternate Member
• Michael Layton	Nuclear Regulatory Commission (NRC)	Member
• Joan Harris	Department of Transportation (DOT)	Alternate Member*
• Richard Hohman	Office of the Director National Intelligence (ODNI)	Member
• Elaine Cummins	Federal Bureau of Investigation (FBI)	Member
• Joseph Lambert	Central Intelligence Agency (CIA)	Member
• Leo Masciana	Department of State (DOS)	Member
• Elizabeth Hanley	DOS	Alternate Member
• Booker Bland Jr.	Defense Security Services (DSS)	Member
• Kathleen Branch	DSS (Attending for the Department of Defense)	Alternate Member
• Benjamin Leingang	SLTPS Entity Representative	Member*
• Mark Schouten	SLTPS Entity Representative	Member
• Jeffery Friedland	SLTPS Entity Representative	Member*
• Alaina Clark	DHS	Observer
• Sarah Cole	DHS	Observer
• Nicole Stone	DHS	Observer
• Carol Morehart	Office of Personnel Management (OPM)	Observer*
• Trisha Prasnikar	OPM	Observer*
• Michael Manning	ISOO	Staff
• Robert Skwirot	ISOO	Staff
• Rosemary Hilton	DoD (Undersecretary of Defense for Intelligence)	Observer*

* Participated via teleconference