

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

SUMMARY MINUTES OF THE MEETING

The SLTPS-PAC held its fourth meeting, on Wednesday, July 25, 2012, at 10:00 a.m., at the National Archives Building, 700 Pennsylvania Avenue, NW, Washington, DC. Mr. John P. Fitzpatrick, Director, Information Security Oversight Office, chaired the meeting, which was open to the public. The following minutes were finalized and certified on October 23, 2012.

The following individuals were present:

- John P. Fitzpatrick (Information Security Oversight Office, Chair)
- Greg Pannoni (Information Security Oversight Office, Designated Federal Officer)
- John J. Young (Department of Homeland Security, Vice Chair)
- Terrie Suit (SLTPS, Vice Chair)
- Harry Cooper (Central Intelligence Agency, Alternate-Member)
- Stephen F. Lewis (Department of Defense, Alternate-Member)
- Richard L. Hohman (Office of Director of National Intelligence, Member)
- Richard L. Donovan (Department of Energy, Member)
- Leo Masciana (Department of State, Member)
- Elizabeth Hanley (Department of State, Alternate-Member)
- Robert Maher (Office of the Director of National Intelligence, Alternate-Member)
- Clyde Miller (SLTPS, Member)
- Robert M. Maloney (SLTPS, Member)
- Colonel Marcus L. Brown (SLTPS, Member)
- Gerald A. (Jerry) Wheeler (SLTPS, Member)
- Lindsey Johnson (SLTPS, Member, via teleconference)
- Kevin P. Donovan (SLTPS, Member, via teleconference)
- Thomas Allen (Department of Transportation, Observer)
- Don Brittenham (Federal Bureau of Investigation, Observer)
- Emily David (Department of Homeland Security, Observer)
- Alaina Duggan (Department of Homeland Security, Observer)
- Barbara Forrest (Department of Homeland Security, Observer)
- John Haberkern (Defense Security Services, Observer)
- Emily R. Hickey (Department of Homeland Security, Presenter)
- Janice Cornwell (Department of Homeland Security, Observer)
- Rich Moreta (Department of Homeland Security, Presenter)
- Robert L. Norman (Nuclear Regulatory Commission, Observer)
- Jeffery Powers (Department of Homeland Security, Observer)
- Charlie Rogers (Department of Homeland Security, Presenter)
- Nicholas Sims (Federal Bureau of Investigation, Observer)
- Garnett R. Stowe, Jr. (INSA¹ Homeland Security Intelligence Council, Presenter)
- Ashley Andrews (INSA Homeland Security Intelligence Council, Presenter)

¹ Due to column formatting and spacing, the acronym for Intelligence and National Security Alliance (INSA) was utilized.

- Jamie Crelos (INSA Homeland Security Intelligence Council, Observer)
- Mary Cradlin Williams (Department of Justice, Observer)
- Patrick Viscuso (Information Security Oversight Office, Observer)
- Alegra Woodard (Information Security Oversight Office, Staff)
- Robert Skwirot (Information Security Oversight Office, Staff)
- Homero Navarro (Information Security Oversight Office, Staff)

I. Welcome, Introductions, and Administrative Matters

The Chair called the meeting to order at 10:00 a.m., and welcomed the membership to the fourth SLTPS-PAC meeting. He informed the attendees that the meeting was open to the public and subject to the Federal Advisory Committee Act. He also stated the meeting was being recorded and minutes of the meeting were going to be made available through the Information Security Oversight Office (ISOO) website. He noted Mr. Gary Ledford, Director of Public Safety for the Eastern Band of the Cherokee Indians, who had served as the nonfederal Vice Chair of the SLTPS-PAC resigned. He introduced Ms. Terrie Suit, Secretary of Veterans Affairs and Homeland Security, Virginia Office of the Governor, Commonwealth of Virginia, as the new nonfederal Vice Chair of the SLTPS-PAC. The Chair, then, acknowledged Mr. John Young, Chief, Administrative Security Division, Office of the Chief Security Officer, Department of Homeland Security (DHS), the federal Vice Chair of the SLTPS-PAC.

The Chair stated that newly appointed SLTPS-PAC members Ms. Lindsey Johnson, Intelligence Analyst/Fusion Center Security Liaison, Tennessee Fusion Center and Mr. Kevin P. Donovan, Vice President Global Security, Johnson & Johnson, were attending via teleconference.² The Chair, then, welcomed the other two new SLTPS-PAC members Colonel Marcus L. Brown, Superintendent of Maryland State Police, and Mr. Gerald A. “Jerry” Wheeler, Executive Director, Office of Public Safety, Seminole Tribe of Florida. The Chair noted there were no SLTPS-PAC membership vacancies; however, not all members were in attendance. Those SLTPS Members not in attendance were Mr. Ronald Brooks and Mr. Frank Taylor. The federal agency members not in attendance were: Dr. Elaine Cummins, Federal Bureau of Investigation (FBI), for whom Mr. Don Brittenham and Mr. Nicholas Sims were attending as observers; Dr. Patricia Holahan, Nuclear Regulatory Commission (NRC), for whom Mr. Robert L. Norman was attending as an observer; Mr. James Dunlap, Department of Justice (DOJ), for whom Ms. Mary Cradlin Williams was attending as an observer; Mr. Louis Widawski, Department of Transportation, for whom Mr. Thomas Allen was attending as an observer; Mr. Drew Winneberger, Defense Security Service (DSS), for whom Mr. John Haberkern was attending as an observer; Mr. Tim Davis, Department of Defense (DoD), for whom Mr. Stephen F. Lewis was attending as the designated alternate; Mr. Joseph W. Lambert, Central Intelligence Agency (CIA), for whom Mr. Harry Cooper was attending as designated alternate; and Mr. Richard L. Hohman, Office of the Director of National Intelligence (ODNI), for whom Mr. Robert Maher was attending as designated alternate. The Chair concluded the opening remarks by asking the Vice Chairs if they had any comments.

² Ms. Johnson had previously attended the January 18, 2012, SLTPS-PAC meeting via teleconference; however, at the time she was not a formally appointed SLTPS Member.

Mr. Young welcomed all the members and congratulated Ms. Suit on becoming the new SLTPS-PAC Vice Chair. He noted that this was the first meeting convened after the issuance of the Committee's Implementing Directive under the authority of Executive Order (E.O.) 13549, "Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities." He acknowledged that it was a lengthy process to get the Directive issued, which required the signature of the Secretary of Homeland Security. He anticipates the Directive will produce various forms and processes to implement the tenants of E.O. 13549 in an efficient and efficacious manner. Mr. Young stated that DHS invites membership comments moving forward in creating new forms, processes, and products.

Mr. Young mentioned that any member who did not receive a copy of the Directive should inform him or Mr. Charlie Rogers, DHS. He stated that the Directive is available for download on the DHS and ISOO websites. He noted that it is also available, for those registered members, on the Homeland Security Information Network (HSIN). He stated that for those members not registered on HSIN, they should contact Ms. Janice Cornwell, DHS, who is administering the program.

Mr. Young stated that there is still much to be done to bring the SLTPS program to maturity, as such, DHS is cooperating with other agencies. DHS is working with DoD, who administers the operations security program under National Security Decision Directive (NSDD) 298. He stated that NSDD 298 has been in existence since 1988, and under DoD's leadership, DHS is seeking to revise NSDD 298. As part of the revision process, DHS is seeking the active participation of the SLTPS community. It is the vision of DHS for SLTPS Members to play a prominent role in the finality of the project. The Chair, then, called on Mr. Greg Pannoni, Designated Federal Official (DFO), for updates on business since the previous SLTPS-PAC meeting.

II. Old Business

Updates from the DFO

Mr. Pannoni addressed three points. First, he stated that the minutes of the January 18, 2012, SLTPS-PAC meeting were finalized and certified on March 26, 2012, and the minutes were included in the SLTPS-PAC meeting folders. Second, he discussed the SLTPS-PAC bylaws. Mr. Pannoni explained that the bylaws were finalized; all the concerns that were raised by members and agencies have been addressed. He stated that the bylaws had been emailed to the membership a week prior to the meeting. He noted that the bylaws require federal members to file annual financial disclosure reports with the National Archives Office of General Counsel (NGC). At present, the requirement has not been implemented. NGC is working to finalize the procedures, and once that is accomplished, ISOO will provide the membership with the procedure details and the implementation time frame. Third and finally, he reminded the membership that E.O. 13549 allows for the reimbursement of travel expenses and per diem for representatives of SLTPS entities. In order to be reimbursed, SLTPS Members must use the same system federal employees' use for their government travel. The first step is for SLTPS Members to establish a government travel account through ISOO. SLTPS Members must then submit travel plans to ISOO at least 30 days prior to an SLTPS-PAC meeting so reservations and other travel arrangements are properly submitted and ISOO travel administrators can ensure that all government requirements are met. Travel vouchers are to be submitted to ISOO within five

days of the meeting. Mr. Pannoni reiterated that this is simply a reminder as the reimbursement information is emailed to all new incoming SLTPS members.

III. New Business

Mr. Charlie Rogers, DHS

A). Status of State, Local, and Tribal (SLT) Compliance Review Program

Mr. Rogers addressed the status of the SLT compliance review program which is in the process of being formed. He reiterated that the signing of the Implementing Directive granted DHS the authority to move forward with the SLT compliance review program. He stated that most compliance review programs have checklists; accordingly, DHS has created checklists covering administrative security, physical security, personnel security, and information security. These checklists were developed based on national policy and on the content of the Implementing Directive. In addition, Mr. Rogers stated that DHS has questionnaires associated with the SLT compliance review program which DHS will utilize for discussions with derivative classifiers and holders of classified information.

Mr. Rogers stated that, at present, DHS is prepared to start a couple of pilot initiatives. DHS is seeking to test and evaluate the aforementioned checklists and the inspection process in order to determine whether these initiatives meet the needs of the SLTPS community. He stated that DHS has spoken with Ms. Suit and the Virginia Fusion Center, who have agreed to be participants in the initial SLT compliance review program pilot. Next, Mr. Rogers mentioned that DHS hopes to do another pilot locally in order to refrain from staff members having to fly across the country to receive training. This presents one less logistical obstacle and allows DHS to utilize a greater number of individuals to implement the initial reviews. He acknowledged once these pilot initiatives are assessed to be suitable and effective, the SLT compliance review program will be implemented nationwide. The primary customers for these compliance reviews are the state and local locations possessing information systems that store and process classified information. He acknowledged these locations are generally the state and local fusion centers: there are 52 primary fusion centers and 25 secondary fusion centers.

Mr. Rogers stated that his office is working with the DHS Office of Intelligence and Analysis (I&A), which coordinates the program between fusion centers and DHS. He stated that a list is being developed in collaboration with I&A that prioritizes the order of fusion centers to be visited. The criteria for prioritization is based upon how long the fusion center has been in existence, the size and magnitude of its respective operation, and whether it manages a secure room (which houses a classified system) or whether it is located with another federal agency that is managing that room. He acknowledged that if a fusion center is managing its own secure room it is given higher visitation priority. If a federal agency is holding a fusion center's systems and managing the secure room, it has a lower visitation priority. Mr. Rogers stated the next immediate step DHS is taking involves training internal personnel followed by working with Virginian personnel to schedule the first compliance review to work through the process.

B) Update on E.O. 13549 Implementing Directive Products

Mr. Rogers gave an update on Implementing Directive products. He stated that the Implementing Directive was staffed through the SLTPS and federal community. However, there

were two documents which were not included in the original staffing of the Implementing Directive, because these documents will eventually become official forms. He noted that there is a separate staffing sequence to get an official form approved; therefore, the decision was made to withhold the two documents. One document is a statement of understanding relative to the protection of classified national security information (CNSI) by private sector personnel. The private sector agreement or understanding document is to supplement the Standard Form (SF) 312 not to replace the SF 312. It is a document which reemphasizes to private sector personnel, who are cleared under this program, that they have an obligation to protect the information and not divulge information to uncleared personnel. The other document is a security agreement between the U. S. government and non-U.S. government entities for safeguarding CNSI. He acknowledged that DHS and other federal agencies have already given CNSI to a large number of state and local facilities, but DHS has yet to initiate an agreement which articulates the mutual obligations between the federal government and state and local entities. He stated that the document refers to the Implementing Directive and delineates specific obligations. Mr. Rogers noted that the document had been sent to the SLTPS-PAC for comment and three members responded. DHS either reconciled or incorporated those comments. He stated that the next step is to work through the DHS forms process to transform the documents into official forms. After this is accomplished, DHS will begin utilizing the forms with those facilities DHS has already shared CNSI with and private sector personnel already given clearances by DHS. He stated that DHS is going to retroactively initiate this implementation.

Mr. Rogers noted that another post-Implementing Directive initiative has been to establish a self-inspection program. He stated that DHS is utilizing existing DHS self-inspection documents to create this self-inspection program. DHS has also sought documentation and guidance from ISOO, as ISOO manages a self-inspection program implementing E.O. 13526, "Classified National Security Information." DHS has created some self-inspection forms based on the Implementing Directive. He noted that the forms will differ from those used by federal agencies, as there is no original classification and declassification authority for state and local governments. Mr. Rogers stated that, on June 21, 2012, DHS went to the Washington Regional Threat Analysis and Fusion Center in Washington, D.C., and undertook a pilot run on the self-inspection checklist. He noted that the pilot run went well and expects to do a couple more locally. He stated the draft has been posted to the HSIN website for reference. Once the document goes from draft to final product, DHS expects to send it out to the fusion center security liaisons. The intent is to have the security liaisons begin to work through the checklist.

C) Update on Security Liaison Workshop and Training Package

Mr. Rogers gave an update on the security liaison workshop and training package. He noted that most fusion centers have appointed security liaisons and DHS has been working with these liaisons for a couple of years. However, he acknowledged that these security liaisons have not been formally appointed under the requirements of the Implementing Directive. The Directive mandates security liaisons to be appointed in writing – there are certain requirements associated with this process. Mr. Rogers stated that his office, in collaboration with I&A, has already drafted a letter to meet this Directive criterion. DHS will send this letter out to initiate the process to formally appoint security liaisons. He noted that this requirement ties into the security agreement between the facilities which cites that they have to officially appoint a cleared employee to assume this role.

Ms. Suit posed a question regarding what is the process for formally appointing a security liaison. In response, Mr. Rogers stated that first, the fusion center director identifies an employee who holds a security clearance, who is able to assume the duties delineated in the Directive, and then, he writes a letter nominating the employee as the security liaison. He noted that the individual does not necessarily have to be a full-time employee. He stated that DHS is attempting to draft a nomination template letter to promote program consistency and uniformity. Once the template is finalized, his office will work with the I&A State and Local Program Office to disseminate the template to all the fusion centers.

Next, Mr. Rogers stated that DHS has provided training for security liaisons over the past couple of years. During that time, DHS has had two multi-day workshop conferences. In July 2010, a security liaison workshop was held in Oklahoma, and the National Security Fusion Center Security Liaison Workshop was held November 14–16, 2011, in San Antonio, Texas. This workshop built upon the first security liaison workshop with presenters from multiple agencies, to include DHS, FBI, DOJ, and the National Security Agency. In attendance were 70 security liaisons and/or fusion center directors representing more than 50 fusion centers. Mr. Rogers acknowledged that the Implementing Directive requires that state and local security liaisons need to be trained within 60 to 90 days. He noted there is annual training being conducted, but this may not meet the 60 to 90 days training requirement for newly appointed security liaisons. Therefore, there is ongoing internal collaboration with I&A to develop a reference booklet for newly appointed security liaisons. Also, he noted that video training and/or video teleconferencing was being developed through collaboration with the DHS Office of Security Training Branch. He stated this is an interim solution to the training requirements of the Directive until newly appointed security liaisons can attend a more formal, in-residence workshop. Mr. Rogers stated that I&A has been funding the workshops, and it appears that the next workshop will be in the early months of 2013.

D) Update on Administration Governor's Staff Support

Mr. Rogers gave an update on the administrative staff support to the governors' offices. He noted that DHS manages the clearances for the governors and adjudicated the clearances of a select number of staff members in the governors' offices. DHS also provides the governors' offices with secure telephone equipment (STE). Mr. Rogers stated that his office works with the DHS Office of Intergovernmental Affairs (IGA) which coordinates periodic STE testing of governors' offices to ensure all the equipment is operable. DHS has concluded that there is an insufficient number of permanent staff in governors' offices to manage STE devices. Mr. Rogers noted that there probably is a lack of knowledge and understanding among the administrative staff of the governors. He stated that, as a result, DHS is in the process of inviting 28 or so cleared staffers/points of contact (POC) from different governors' offices to be part of the HSIN website. DHS has developed a PowerPoint reference on the website. He noted that the intention is to work with IGA after the next STE test and have more staff of governors cleared. DHS is seeking to identify and clear permanent staff or state employees rather than gubernatorial political appointees who change every few years.

Ms. Suit contended that by its very nature the governor's office is a political office; therefore, DHS will be hard pressed to find permanent employees. She stated that DHS may find agency personnel assigned to support the governor's office; however, personnel tend to leave prior to the inauguration of a new governor. She noted that the clearance issue could be resolved or targeted

during the transitional period of changing gubernatorial administrations, as it is a several-month-long process. This issue could be instituted as part of the transition protocols.

Mr. Rogers noted that it is a challenging undertaking to find permanent personnel to clear. He acknowledged that DHS has to actively work with the governors' offices and the IGA. He acknowledged the impetus behind getting permanent personnel cleared is to have someone to manage the training, be a subject matter expert (SME), and train the next group of uncleared staff members when a new gubernatorial administration takes office. It is not that DHS is averse to clearing nonpermanent personnel just that DHS seeks to have long-term security managers in place to manage the security for the governor's office.

E) Update on DHS SLTPS Security Management Division Personnel

Next, Mr. Rogers discussed the staffing of the DHS SLTPS security management division. He noted that the Division has received some funds in the last couple of years to increase its staff. The Division is in the process of augmenting its staff with three new positions that will be advertised within a week. Mr. Rogers stated that two information technology systems analysts have been hired with the intent of having them involved in the process to identify and modify the security clearance database tracking mechanism that is required under E.O. 13549. Also, this will help DHS to build a more robust tracking mechanism for security facilities. He noted that these initiatives will improve the practical functionality of the HSIN website. In addition, Mr. Rogers stated that these two positions will fill a technical expertise gap within the Division. Further, DHS wants to expand HSIN's capacities by posting training, tracking training, and increasing its interactivity capabilities. The Division is also filling a policy position which will help the Division work with other federal agencies as DHS expands the program. The policy employee will work with other agencies' policies and procedures in an effort to collect data to fill and create DHS databases. Also, he noted that DHS may need to write policy documents, and the policy analyst will be involved with that.

F) Update on Homeland Security Advisors/Staff Support

Finally, Mr. Rogers stated that Homeland Security Advisors (HSA) have varying roles in states, with some deeply embedded into the fusion centers and the classification process. He stated that the HSAs are all involved in the clearance process, serve as advisors to governors, and have clearances. He stated that DHS would like to have the HSAs play a greater participatory role in the program. To accomplish this, Mr. Rogers stated that his office would like to work with Ms. Suit and the IGA to invite the HSAs to be a part of the HSIN website community of interest or have them identify some of their staff members who can participate in the website. He stated that this is an effort to enhance the HSAs' knowledge of the program and keep them apprised of what DHS is doing. Also, he noted to identify other ways DHS can engage in community outreach to have the HSAs more involved in the classification program. Mr. Rogers concluded his presentations by asking if there were any questions.

Ms. Suit asked a question regarding the compliance checklists and how they applied or would apply to safes located outside the fusion centers. She stated that she was unsure about whether the governor's office had safes approved for storage of CNSI, but in her office there were several safes approved for storage of CNSI, not located within the fusion center.

Mr. Rogers acknowledged the question and stated that it is partially the reason DHS would like to work with her office. He stated that the initial step is to finalize the self-inspection checklist, followed by having her office complete it. The list will probably be sent out before DHS sends a compliance review team. The checklist will contain multiple items dealing with the protection of CNSI. Mr. Rogers stressed that it is not because her office is not a priority, but DHS's immediate concern are the 50 fusion centers which have classified systems and significant operations. DHS wants to send teams to these particular fusion centers to assess their functionality and aid in the incremental build up of their programs. He stated that DHS definitely wants to interact with any location that is storing CNSI and to his knowledge there are a number locations storing CNSI, such as, the state police barracks of Maryland and the state of Florida having multiple locations.

Ms. Suit mentioned that the Directive's requirements have implications on the location of where the briefing of the governor's chief of staff and the governor on classified information may occur. She clarified that it seems like the Directive has instituted some changes to the location that briefings can take place or the certification of the location, whether or not it is a facility that has been previously reviewed and surveyed. She noted that the governor cannot always be briefed at a fusion center or secured approved locations, as the governor is operating on real time and it is imperative there are no delays in the dissemination of information. Ms. Suit stated that for example sometimes briefings occur inside a vehicle, to which Colonel Brown concurred. She stated that it would be helpful if DHS provided specific guidance to the governors' offices on this issue. She opined that it would be helpful if the agency that is sponsoring access to the classified information would provide guidance as to what procedure or rules to follow to avoid any legal ramifications.

Mr. Rogers stated that this is an issue that DHS will work on with the HSAs. He stated that conducting a briefing inside a vehicle is not the preferable location; however, there is an established process by which DHS can approve rooms that are not necessarily secure rooms, but where documents can be discussed or reviewed on a temporary basis.

Mr. Clyde Miller, SLTPS, stated that he is the Chairman of the Chemical Sector Coordinating Council and raised certain points of concern. He raised the issue of how do individuals outside the Beltway get a CNSI briefing without having to come inside the Beltway. Mr. Miller noted that one of the elements of the National Level Exercise 2010 required that owner/operators needed to come to the Washington, D.C. for a classified briefing. He asserted that this action was not practical given that participants may have been engaged in local projects requiring their presence. Mr. Miller stated that he recognized that DHS may not have as much influence on fusion center operations; however, his concern is that most fusion centers are law enforcement focused and not focused on sharing information with the private sector. He stated that his last classified briefing was conducted at a local Secret Service office through coordination with DHS. Mr. Miller strongly encouraged DHS to attempt to incorporate fusion centers with secure rooms as locations for sharing classified information with cleared private sector representatives.

Mr. Rogers acknowledged Mr. Miller's concerns and stated that his role is limited, because his office's responsibilities are to ensure that the appropriate security environment is in place, people are trained, and they are made knowledgeable. However, he stated that he would inform the DHS State, Local, and Tribal Program Office, which manages the information sharing environment, about Mr. Miller's concerns and will furnish him with names of POCs in that

office. He noted that there are fusion centers in California that are actively inviting private sector personnel to attend conferences; however, he acknowledged that it varies from state to state and among regional locations.

Ms. Alain Duggan, DHS, stated that DHS had just had a meeting with the private sector a week prior, which, Mr. Miller attended. She stated that the meeting included discussions involving the Coordinating Council Chairs, who were present. The discussions noted the importance of information sharing when an event(s) or issue(s) occurred overseas or domestically. Questions that arose were: What are DHS, FBI, and other agencies doing with regard to that specific issue(s)? How and when is this information going to be disseminated to the private sector? Ms. Duggan stated that there was going to be another meeting, which was going to be larger in scope; however, she did not give specifics as to the date and time.

Ms. Suit pointed out that perhaps the concerns raised by Mr. Miller were valid points that Colonel Brown could apply to Maryland. She noted that fusion centers are extremely chain-of-command oriented. Therefore, Colonel Brown, being Superintendent of Maryland State Police, could give the Maryland fusion center directors certain priorities on how the fusion centers are going to operate. He could reach out to other state superintendents who have fusion centers under their command to suggest that they expand their relationships with the private sector. Ms. Suit, also, noted that it takes time for fusion centers to conceptualize beyond being simply law enforcement entities. She stated that Virginia is progressing along the continuum, by expanding its spectrum of focus and hiring personnel with specific skills sets. She stated that Virginia is looking at critical infrastructure and employing cyber and transportation security analysts.

Colonel Brown stated that Maryland is probably in a better situation than other states given Maryland's relative size. He stated that Maryland has a fusion center just outside Baltimore City that has created categorized lists of private sector security leadership and business leadership to maximize its information sharing potential. If an incident occurs, the list provides the names of personnel to brief immediately, and the fusion center's location near Baltimore City makes it readily accessible.

Mr. John Haberkern, DSS, addressed two issues that had been raised in the previous conversation: fusion center priorities and sites to access information. Fusion center priorities are going to be based on the environment and the training of the fusion center employees. He noted that fusion center personnel possess varied specialized skills sets and professional backgrounds and suggested that fusion center management should expand these to broaden fusion center capabilities. He spoke to the second issue by referring to an idea that he said this group discussed over a year and a half ago: creating a list of designated alternate sites where personnel can access classified and sensitive information. He suggested that the publication of this type of list could be reconsidered. Mr. Miller and the Chair concurred with this statement and agreed that it is an issue that SLTPS-PAC should take under consideration.

Mr. Young responded that this is still under consideration. He stated that DHS maintains a list of cleared facilities it has been involved with, but it does not include facilities other agencies utilize and thus is not all inclusive. Compiling a more comprehensive facilities profiles list, under the direction of Mr. Roger's office, will be part of the program's evolution. Mr. Young stated that such a list could be accessed to advise an SLTPS community member of the secure facility closest to him or her.

Ms. Suit then stated that the next challenge is passing clearances. She noted that the FBI has been very accommodating and has permanently certified her at some of its facilities that she visits frequently in Virginia. She stated it would be useful if certain facilities could be designated as customer friendly where individuals can be permanently certified. Furthermore, she noted that if the system for checking clearances electronically became more widely utilized by more agencies it would be extremely helpful.

Mr. Young admitted that there are still many concerns which have yet to be addressed but assured the members that DHS understands the magnitude of those concerns. He acknowledged that some fusion centers do allow use by the private sector while others do not. He recognizes the inconsistencies, noting that this is an issue that his office will bring to the attention of pertinent DHS offices. He noted the importance of the SLTPS-PAC highlighting any potential impediments to information sharing. The Chair concurred and stated that once members concerns are raised, it is up to DHS and the appropriate federal personnel to follow-up on those concerns and develop implementable solutions through cooperation.

Finally, Mr. Miller commented that some centers actually have seats available for private sector personnel, but that fusion center personnel sometimes have too narrow a focus to understand the needs of the private sector. Then, the Chair directed the membership to Ms. Emily R. Hickey, DHS.

Ms. Emily R. Hickey, DHS
Overview of the Protected Critical Infrastructure Information Program (PCII) and
Discussion on Possible Amendments to the Rule that Governs PCII

Ms. Hickey provided an overview of the PCII program and discussed possible amendments to the rule that governs PCII in a presentation that covered the following: what is PCII; why is there a PCII program; how does information become PCII; what are the benefits of PCII; and what happens once information becomes PCII. She also introduced Ms. Barbara Forrest, DHS, PCII Deputy Program Manager. Ms. Hickey stated that PCII is a statutory form of controlled unclassified information (CUI) that was established by the Homeland Security Act (HSA) of 2002 and the Critical Infrastructure Information (CII) Act of 2002 within the HSA. The CII Act gives DHS the responsibility to implement the PCII program, which is designed to encourage and facilitate information sharing between the government and private sector for the protection of all 18 sectors of infrastructure, among which are energy, chemical, transportation, telecommunications, food, and agriculture.

Ms. Hickey stated that not all infrastructure information is PCII. The CII Act is very specific and outlines the criteria that information must meet to be PCII. She indicated that information regarding infrastructure operations and vulnerabilities known by a private owner or operator can become PCII, but it must be submitted voluntarily, as it is proprietary information. The federal government cannot mandate that information be provided. She stated that once information is submitted, the submitter has to expressly request PCII protections for the information. She stated that information must be validated and marked PCII in order to be protected. The CII Act protects information from release under the Freedom of Information Act (FOIA) through FOIA exemption B3. It is also protected from release under state and local sunshine laws, disclosure

laws, or public records act. This information is also protected from civil litigation, and it is protected from regulatory use.

Continuing with her presentation, Ms. Hickey addressed what happens to information once it becomes PCII. Once information has been validated by the PCII program office, it is marked and protected by a cover sheet. PCII can, then, only be accessed by federal, state, or local government employees or their contractors. Individuals must undergo training to become PCII authorized users and have homeland security duties, along with a need-to-know. She stated that there are penalties for misuse of PCII. A federal employee who misuses PCII can be fined, imprisoned, terminated, or all three. A contractor can be terminated, since he or she has to sign a nondisclosure agreement to access PCII.

Next, Ms. Hickey covered how PCII information is used by DHS. It is used for analysis and studies that consider the interdependence of the infrastructure sectors. DHS uses the information to issue alerts and warnings. The information is also used for recovery plans and to mitigate vulnerabilities in the infrastructure. She stated that the PCII program had been incorporated into the CUI framework and it is in the CUI registry. She noted that the PCII marking will be consistent with CUI marking requirements.

Ms. Hickey stated that the PCII program has been in operation for seven years and there has not been an unauthorized disclosure of information. There has been an increase in the amount and quality of infrastructure information being received from the private sector creating a larger database for intelligence analysts to detect patterns and trends. She stated that there has been a strengthening in the information-sharing partnerships among the federal, state, and local government and the private sector. Ms. Hickey enthusiastically expressed that the cost of protecting PCII is relatively minimal to other information security programs. The protection requirements of PCII are basic lock and key with use of a cover sheet. PCII is stored and safeguarded only by the PCII Program Office, accredited entities, and authorized users.

Ms. Hickey stated that when the PCII program was initiated seven years ago it was primarily focused on physical documents, while simultaneously recognizing the electronic environment. She acknowledged that the PCII program needs to be updated to accommodate current and future information technology advancements. DHS wants to update the PCII program due to the lessons learned through operational experience. She stated that two primary updates concern portion marking and international sharing. Ms. Hickey stated that currently, when PCII is in even just a single section of a document, the entire document is protected from unauthorized disclosure. If portion marking could be applied to PCII, it could be easier to obtain and share. Ms. Hickey acknowledged that portion marking of PCII is a contentious topic within the federal government and that the private sector may have its own concerns. Nonetheless, she stated that portion marking is a priority and that once this issue is posted to the Federal Register all stakeholders will have an opportunity to comment. She asked the membership to notify the PCII Program Office, her, or Ms. Forrest of any concerns, comments, or suggestions.

Finally, Ms. Hickey stated that the rules are presently silent about the international sharing of PCII information. However, private sector submitters can request information be shared with a foreign nation. In some cases, state and local government submitters can also request the same action. She noted the main reason that international sharing of PCII is permissible is that the federal government does not own the information. The submitted information is simply under

the custodial care of the federal government. She acknowledged that there are opponents to the international sharing of information; however, such sharing offers considerable advantages to the protection of infrastructure. Ms. Hickey concluded her presentation by stating that the PCII Program Office's website is www.dhs.gov/pcii and that the PCII office can be contacted on 202-360-3023 or via email at pcii-info@dhs.gov. She, then, solicited questions from the membership.

Mr. Rob L. Norman, NRC, asked whether international recipients of PCII are also required to protect the information in the same manner and subject to the same punitive consequences. Ms. Hickey replied that her office is working with the Homeland Security Office of General Counsel to work through agreements to address the question. An agreement would have to be negotiated with each country or international organization, and U.S. legal authority would be based on those agreements. Since the PCII program is about information sharing, there is a reciprocal component where domestic and foreign entities should abide by each other's protection and punitive requirements. Mr. Norman also asked if PCII cannot be used in civil litigation, does that protection extend to the information that is still held by the submitter. Ms. Hickey replied that this is an amendment that is being examined. Any information that is marked and validated as PCII is clearly annotated on the document. She stated that submitters keep copies of submitted information – even though the information is the same, it is not marked as PCII. Currently, there are no protections for unmarked information held by the submitter.

Ms. Suit asked how PCII and the Automated Critical Asset Management System (ACAMS) are coordinated or work together.³ Ms. Hickey referred the question to Ms. Forrest, who stated that once information meets submission criteria, is submitted, and is approved as PCII upon arrival into ACAMS there is no question that it is protected as PCII. Ms. Suit made follow-up comments regarding the use of ACAMS. She stated that Virginia is seeking to increase the number of ACAMS users within the first responder community so that first responders can access PCII critical infrastructure quickly and coordinate with the fusion center to adequately respond to an infrastructure crisis. Ms. Forrest reaffirmed Ms. Suit's praise of ACAMS and stated that it is a very successful state and local partnership where first responders were crucial for data collection. Simultaneously, Ms. Hickey stated that ACAMS stakeholders were the first to identify the need for portion marking.

Ms. Suit continued with a separate comment and stated that each year Virginia does a data call with DHS. She stated that the data call involves the Commonwealth of Virginia nominating critical infrastructures and key resources (CIKR) in order to have those CIKRs in the database for the purpose of determining the size of Urban Area Security Initiative (UASI) grants. Ms. Suit expressed that the amount of CIKR information the private sector contributes to the nomination correlates to how much UASI grant monies are received. To illustrate this point, she noted that Hampton Roads, Virginia lost its UASI funding this year and reiterated the need for the private sector to provide CIKR information.

Mr. Norman asked, in respect to Virginia having ACAMS, is the information housed on a DHS server allowing users to link in or do states have their own databases of information. Ms. Hickey

³ ACAMS is a Web-enabled information services portal that helps state, local, tribal, and territorial governments build critical infrastructure protection programs. ACAMS accounts are granted by the DHS.

and Ms. Forrest responded that it is a federal program operating out of a federal server. He, also, asked if DHS prescribes the type of system, and Ms. Forrest replied that it is certified and accredited to meet all federal standards. Then, Mr. Miller asked if private sector information was submitted for PCII designation and the information was received back with the proper markings and cover letter, is the information protected against discovery or does the private sector assume responsibility during civil litigation. Ms. Hickey stated that in the event of this question the PCII Program office would consult its assigned attorney advisor.

Mr. Haberkern asked a question regarding access to information derived from site vulnerability assessments. Ms. Hickey responded that DHS protective security advisors (PSA) perform vulnerability assessments. Information stemming for those assessments becomes PCII and assessment results are provided to the owner or operator of the facility. He asked if any of the information would be classified or what percentage of the assessment would be classified. She stated that classification of assessment results would be contingent upon the type of facility. If an assessment contains both classified information and PCII, all assessment information would be protected to its appropriate level of classification. Then, Mr. Haberkern asked if classified information is uploaded along with PCII information to an accessible database. Ms. Suit stated that classified information would not be uploaded to an accessible database. Mr. Haberkern agreed with Ms. Suit's comment and voiced his thought that there should be a central location where assessments containing PCII, CUI, and classified can be provided in their entirety to various analysts. Ms. Hickey stated that she has not conducted this type of analysis; however, it is her understanding that intelligence analysts are privy to all information whether it is open source, PCII, or classified. Mr. Haberkern asked how the information is tracked. Ms. Hickey stated that the PCII Program Office is not involved with that issue. Then, Ms. Suit offered her comments mentioning that her office conducts vulnerability studies or assessments in partnership with PSAs, who handle classified information. She noted that no classified information is uploaded into ACAMS and suggested that a PSA program representative attend the next meeting and explain how the program operates. Ms. Hickey added that if more information was needed about ACAMS, the ACAMS program manager could give a presentation at a future meeting.

Mr. Cooper commented that from a classified intelligence analyst point of view, classified analysis may contain some PCII, but unprocessed PCII is unlikely to contain any classified information. A PCII submitter is providing information on the infrastructure, an intelligence analyst is adding classified value. Mr. Cooper noted that access to classified analysis is done through classified databases. Then, Mr. Haberkern pointed out that the challenge is in the timely dissemination of relevant information to the appropriate personnel. Mr. Cooper responded that theoretically if classified analysis is available to fusion centers, then the fusion centers are able to access classified intelligence and brief the appropriate personnel on critical infrastructure threats. Ms. Hickey added that PCII submitters can inform DHS as to who can have access to the submitted information and DHS will facilitate the sharing process.

Ms. Suit stated that not all fusion centers are focused on critical infrastructure. In Virginia, the critical infrastructure program is operated out of the governor's office. She noted that funding was procured recently to allocate critical infrastructure focused analysts in the fusion center. She expressed that fusion centers differ in priorities and analytical expertise. Then, Mr. Robert M. Maloney, SLTPS, commented that lack of federal funding in the foreseeable future poses an obstacle to hiring the appropriate level and variation of analytical expertise. As a result, there is only immediate focus on short-term priorities and locations are losing a great deal of federal

funding. To exemplify this point, Mr. Maloney stated that UASI grant money for Baltimore City has declined, only having received \$600,000. He noted that this monetary amount is not sufficient to maintain an effective cadre of analytical expertise. Mr. Maloney stated that he is encouraged that DHS is developing more extensive homeland security programs at a time when local funds are being cut. As all questions for Ms. Hickey had been answered and all comments made, the Chair introduced Mr. Rich Moreta, DHS.

Rich Moreta, DHS

Foreign National Vetting: The DHS Process for Vetting Foreign Nationals Who Officially Interact with DHS and Select SLT Entities

Mr. Moreta introduced himself as Branch Chief for the Foreign Access Management Branch of the Office of Security, which is within the Internal Security and Investigations Division of DHS. He stated that his office concentrates on vetting foreign visitors and individuals who have access to DHS facilities and programs. He noted that this service is provided to some state, local, and tribal entities. Mr. Moreta reported that every year DHS has approximately 9,000 visitors and 2,000 other types of foreign nationals that officially interact with DHS in other capacities. He stated that some are Foreign Service nationals and others are foreign nationals with authorized access to HSIN international. He mentioned that the Federal Emergency Management Agency provides foreign nationals with access to online training; however, the primary focus of his office is the 9,000 yearly visitors to DHS.

He stated that there is a system that all customers can access and there are about 200 system users throughout all 22 DHS departmental components. These users upload the names of foreign nationals and all required information. Then, Mr. Moreta stated a check of the information is conducted and an investigation is initiated. He noted that part of the process involves indirectly partnering with other federal agencies. DHS will transfer the information of the foreign nationals being vetting to certain agencies, then those agencies conduct their own investigations.

Mr. Moreta stated that while this is transpiring DHS tries to validate the identities of the foreign nationals. The names of foreign nationals are inputted into a traditional name check system. When all the aggregate information is received a risk assessment is conducted and the results are provided to the customer. Then, the customer makes the decision as to whether to allow these foreign nationals to visit or be program participants. Mr. Moreta stated that his office performs this action approximately 300 times a week. The service is provided to several fusion centers and other locations throughout the U.S. He reiterated that his office works with several other agencies, and presently, it is working with ODNI on the issue of interconnecting all U.S. foreign visitor programs so that any visitors DHS might have, another agency such as DOE is aware of them and vice versa. He stated that his office is also working internally within DHS with I&A and other offices. Mr. Moreta concluded by asking if there were any questions. No questions were asked, and the Chair introduced Mr. Garnett R. Stowe, Jr., Chairman of the Homeland Security Intelligence Council (HSIC), Intelligence and National Security Alliance (INSA).

Garnett R. Stowe, Jr., Chair, HSIC, INSA
The Role of INSA Working with Homeland Defense Stakeholders

Mr. Stowe addressed INSA's role in collaboration with homeland security stakeholders. He mentioned that the partnerships between the SLTPS community and federal agencies need to be continually nurtured to grow and find solutions. He stated that there are 18,000 law enforcement organizations in the U.S. and noted that there used to be approximately 840,000 men and women exclusively devoted to homeland security protection. He acknowledged that homeland security is a constant endeavor to counter the continual rise of domestic and transnational threats. Then, Mr. Stowe stated that INSA is an organization which provides a forum for SLTPS entities, academia, and the federal government to discuss threats. It is a neutral forum where representatives from across these entities can voice comments, suggestions, and/or concerns. The forums are unclassified and open to the public. INSA provides the opportunity to collaborate and network with a diverse body of professionals to formulate homeland security solutions. He acknowledged that the largest group of members are from the intelligence community (IC) and the next largest is from private industry. There are a number of members from academia. The membership collaborates to formulate timely, innovative solutions to national security issues.

Mr. Stowe expressed that INSA is a public/private organization that works to recognize and promote the highest standards within the IC. As evidence, he stated that retired U.S. Navy Admiral William O. Studeman, the Honorable Stephen A. Cambone (former Under Secretary of Defense for Intelligence), and retired U.S. Air Force General Michael V. Hayden have volunteered time to work with INSA. INSA draws on the expertise of its members who possess extensive practical national security experience. In talking about membership, Mr. Stowe stated that there is a fairly good representation from FBI, but none from the Department of State. He urged the membership to inform their colleagues about INSA membership opportunities. He stated that among their corporate participants are General Dynamics, Boeing, Lockheed Martin, Raytheon, Booz Allen Hamilton, and the Science Applications International Corporation. He noted that there are 150 corporate members and several hundred private members. Mr. Stowe stated that two INSA interns were in attendance, Ms. Ashley Andrews and Ms. Jamie Crelos, who would be providing copies of two recent reports and other informative material at the end of the meeting.

Mr. Stowe stated that the HSIC is primarily focused on the topic of intelligence activities and information sharing. Members of HSIC include the Deputy Director of the National Geospatial-Intelligence Agency and Mr. Michael J. Morell, Deputy Director, CIA. He stated that Mr. Bart Johnson, Executive Director, International Association of Chiefs of Police, is the HSIC Vice Chair and also serves as a law enforcement SME. He noted that several lawyers are HSIC members

Mr. Stowe stated that in September 2011, the HSIC completed an extensive homeland security study, 10 years after 9/11, that examines both the present state and future of homeland security. He noted that the report advocates 16 specific recommendations and advised that the report could be obtained through the INSA website or from Ms. Andrews and Ms. Cerlos. Mr. Stowe stated that the report was being updated and the revised report would be made public in September 2012. Then, he explained that the HSIC is also conducting a series of roundtables focusing on capturing ideas from outside the Beltway, an approach that will allow the general public to

acquire a broader perspective on homeland security issues and implications. Also, policy makers and Beltway outsiders will have the opportunity to interact. He elaborated that INSA's objective is to have policy makers and federal personnel interact with individuals from across the U.S. to develop homeland security programs and policy based on mutual cooperation and understanding.

Mr. Stowe stated that INSA has formed partnerships with the National Governors Association, Association of Fusion Centers, and has collaborated with the Center for Strategic and International Studies (CSIS). The outcome of these partnerships and collaborative efforts is a series of roundtables. He noted that the first roundtable was held on June 26, 2012, and it covered the recommendations from the September 2011 report. The roundtable's impetus was to raise the visibility of the report's 16 recommendations and set the basis for the report's revision. Mr. Stowe stated that in subsequent roundtables INSA would be seeking academics' perspectives on the report's revision.

Mr. Stowe concluded with discussing the creation of two INSA task forces. The first task force will develop a fusion center standard template of operations by surveying some of the 72 DHS recognized fusion centers. The task force's objective is to create a minimum operational standard in collaboration with a wide range of homeland security personnel. He stressed that the task force's final product will be for reference purposes only and not a mandate. Next, he stated that the other task force will deal with the issue of privacy. The task force will investigate how to effectively protect privacy in the wake of evolving homeland security programs. He noted that this task force is a continuation of a 2011 INSA privacy report. Finally, Mr. Stowe mentioned to the membership that if they were interested in contributing to the initiatives they should contact INSA, and he asked if there were any questions.

Ms. Suit inquired about the size of the HSIC membership. Mr. Stowe responded that the HSIC varies in size; however, there are 12 core members. Depending on the needs of the council, the HSIC invites other individuals to participate. The HSIC meets once a month as a general group and several sub-groups meet as required. The Chair mentioned that the HSIC had recently hosted a public forum in partnership with CSIS and asked whether the HSIC was going to host another similar event. Mr. Stowe responded yes another event was going to be hosted with Mr. Kshemendra Paul, Program Manager, Information Sharing Environment, ODNI, serving as the key speaker. Mr. Stowe stated that another roundtable was going to be held after two or more HSIC meetings, and it would mostly like focus on discussing the fusion center templates. With no more questions or comments, Mr. Stowe thanked the membership for their work and reiterated that hard copies of two INSA reports were available after the meeting.

IV. General Open Forum/Discussion

The Chair indicated that he had reached the end of the planned agenda and solicited final questions and comments from the membership and all in attendance.

The Chair expressed his gratitude for the services INSA provides and encouraged the membership to learn more about INSA. He noted how this group is important as it provides the opportunity for public forums to discuss homeland security issues relevant to the membership. Then, the Chair directed the membership to Ms. Suit and Mr. Young for their final comments. Mr. Young thanked the members for their continued support and contributions. He stressed to the membership to register with HSIN and encourage all their constituencies to register as well.

He emphasized that there were many valuable products and resources available on the HSIN website. Ms. Suit thanked the membership for their time and continued support. Next, the Chair asked Ms. Johnson and Mr. Donovan if they had any comments. Mr. Donovan did not, and Ms. Johnson reported on the establishment of a nationwide conference call initiative in partnership with DHS. She stated that her objective for this initiative was to connect all state and local fusion security liaisons for the purpose of discussing any security practices and/or concerns at the state level. Then, any concerns identified in the conference call are to be forwarded to DHS and highlighted at the SLTPS-PAC meeting succeeding the conference call. The plan is to have conference calls scheduled a month prior to SLTPS-PAC meetings. The first conference call occurred on May 23, 2012, and suggestions from that call have already been presented to DHS. Ms. Johnson stated to the membership that one of the suggestions concerns the Central Verification System (CVS) and requests that security liaisons be given the ability to access clearance information in CVS for the personnel that they are responsible for in their fusion centers.

Mr. Young acknowledged Ms. Johnson's comments and explained that Mr. Rogers' office has created a document reflecting DHS desired modifications to CVS, such as incorporating SLTPS clearance information into CVS. He stated that sometime in the near future the document will be presented to and coordinated with OPM, along all the other agencies required under E.O. 13549. Mr. Young noted it will be a lengthy process, but stressed DHS is addressing the concern.

In summation, the Chair emphatically motioned to the membership that the Committee is a venue to voice any and all suggestions, comments, and/or concerns. The Committee is a vehicle to promote progress. He stated, in light of the CVS comment, OPM could be brought to a future Committee meeting to give a CVS presentation. The Chair encouraged the membership to contact SLTPS-PAC staff at ISOO with any issues that should be discussed at succeeding Committee meetings. If the membership would like an issue placed on the agenda or discuss an idea, they should contact Mr. Pannoni, Mr. Robert Skwirot, or himself. The Chair noted that ISOO would work with DHS regarding issues raised and provide appropriate responses. He acknowledged that DHS now has more authority to pursue initiatives with the signing of the Implementing Directive. There were no more comments and the Chair moved to adjourn the meeting.

V. Closing Remarks and Adjournment

The Chair thanked everyone for attending the meeting and for contributing to this effort. Noting that the Committee is required to meet at least twice a year, he announced tentative dates for the next SLTPS-PAC meetings: Wednesday, January 30, 2013, in the National Archives Building, from 10:00 a.m. to 12:00 noon and Wednesday, July 24, 2013, in the National Archives Building from 10:00 a.m. to 12 p.m. The meeting was adjourned at 12:10 p.m.