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

SUMMARY MINUTES OF THE MEETING

The SLTPS-PAC held its seventh meeting on Wednesday, January 24, 2014, at 10:00 a.m., at the National Archives Building, 700 Pennsylvania Avenue, NW, Washington, DC. Mr. 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 July 2, 2014.

Welcome, Introductions, and Administrative Matters

The Chair welcomed the attendees. (See Attachment 1 for a list of members and guests in attendance.) He informed everyone that SLTPS-PAC meetings are recorded events subject to the Federal Advisory Committee Act and a transcript of the meeting would be made available through the ISOO website. Next, he stated that the meeting folders included the agenda, the minutes from the last meeting, and the slides for today's presentations. He reminded government members of the requirement to submit their respective financial disclosure forms to the National Archives and Records Administration to verify there is no actual or apparent conflict of interest with respect to service on the Committee.

The Chair introduced the new SLTPS Vice Chair Clyde Miller, Director, Corporate Security for BASF Corporation, and new SLTPS members James Dewey Webb, Senior Director/Chief Operating Officer, National Native American Law Enforcement Association; Special Agent Benjamin Edward Leingang, Director, North Dakota State and Local Intelligence Center, and Special Agent, Bureau of Criminal Investigation; and Ashley Wilson, Director, Joint Regional Intelligence Center. Following the Chair's introductions, all present proceeded with their introductions.

The Chair called on SLTPS Vice Chair Clyde Miller to provide introductory comments. Mr. Miller praised the value of the Committee and briefly stated that one of his objectives in his new role is to increase information sharing between government and non-government entities.

I. Old Business

Updates from the Designated Federal Official (DFO)

Greg Pannoni, DFO, stated that the minutes of the July 24, 2013, SLTPS-PAC meeting were finalized and certified on November 7, 2013. He emphasized that, due to Federal sequestration, reimbursement of travel expenses is not possible and encouraged future Committee participation via teleconference. He then reminded members of the previous meeting's four action items: first, the Department of Homeland Security (DHS) to inquire regarding the possibility that they may be required to eliminate their Intelligence and Analysis (I&A) agents from the National Network of Fusion Centers; second, DHS's efforts to invite persons with Controlled Unclassified Information (CUI) expertise from a number of government agencies to serve on its Integrated Task Force Working Group (ITFWG); and third, DHS's efforts to identify knowledgeable

personnel to brief the Committee on the potential impact of environmental terrorism on various critical infrastructure elements. The fourth action item related to the appointment of a new Vice Chair, which was accomplished through Mr. Miller's appointment. Action items from the current meeting are provided in Attachment 2.

II. New Business

A) Response to the Action Items

Charlie Rogers, DHS, stated that, at present, funding for I&A agents in fusion centers remains intact and DHS has no plans to withdraw them. In reference to the CUI action item, he noted the initiative to invite CUI experts from various government agencies ultimately did not correspond to the objectives of the ITFWG. He commented, in terms of environmental terrorism, that none of the 16 DHS critical infrastructure elements specifically focus on environmental terrorism, rather all DHS elements engage in multiple threat analysis.

B) Status Update on Office of Personnel Management's (OPM) Central Verification System (CVS) Transformation

The Chair called on Trisha Prasnikar, Senior Program Analyst, External Affairs, Federal Investigative Services, OPM, to provide an update on the incorporation of SLTPS security clearance data into OPM's CVS. (See Attachment 3 for her presentation.) She stated that after having worked with a sub-working group of members from the SLTPS community, OPM identified changes to the system the SLTPS community seeks to incorporate. She cautioned the Committee that the database development remains a work in progress and there are additional enhancements yet to be completed.

Ms. Prasnikar noted that OPM partnered with DHS, the Office of the Director of National Intelligence (ODNI), and the Department of Defense (DoD) to input clearances into CVS for reciprocity purposes in compliance with Executive Order (E.O.) 13549, "Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities."

She noted that, a year ago, OPM formed a working group to focus on identifying SLTPS requirements for CVS, which included new data fields and data reports to assist Federal agencies in carrying out SLTPS duties. The working group's objectives are to be implemented in two phases. Phase one's goals are to be met by February 2, 2014, or shortly thereafter. During this phase, SLTPS security clearance information will be added to CVS for existing measures. She stated that OPM had already added some additional data fields to CVS, including clearance affiliation and relevant SLTPS community attributes, such as the program office sector and details on an individual's primary duty station. Ultimately, population of these data fields will permit the generation of a clearance-holder listing report, which will be made available to all active agencies to assist with their program administration. Then, she briefly described phase two of the implementation process. OPM worked with DoD to incorporate Joint Personnel Adjudication System data. She explained that the primary phase two goal will involve creating a new specific user role, "security liaison," for fusion center staff that will enable clearance verification at the Secret level. She acknowledged that the completion date for phase two has not yet been projected. She noted that changes and updates will be posted on the OPM website

through Federal Investigation Notices (FINs). In addition, relevant FINs will be sent to the Committee via email. She also mentioned that instructional documents for CVS are published on the OPM website.

The Chair inquired if the affiliation of the clearance is the same as indentifying the granting Federal agency. Ms. Prasnikar responded that affiliation speaks to whether an individual is civilian, contractor, or military and expands further by capturing if the affiliation is state, local, or tribal. Alaina Clark, DHS, inquired if security liaisons associated with DHS Homeland Security Advisors would have the same access as the new user role security liaisons. Mr. Rogers responded that account access is granted as necessary. Then, Mr. Pannoni asked about a security liaison's capabilities to verify a Top Secret clearance if only Secret clearance verification is authorized in CVS. Ms. Prasnikar stated that fusion center security liaisons would coordinate with the appropriate Federal agencies to verify a Top Secret clearance. Mr. Rogers and Ms. Prasnikar both added that the reason behind limiting security clearance verification up to the Secret level is a direct result of fusion centers only being allowed to conduct meetings and store information up to the Secret level.

C) Security Liaison Training Workshop

The Chair called on Nicole Stone, Office of Intelligence and Analysis (OI&A), DHS, to provide an update on the Security Liaison Training Workshop scheduled for April 8–10, 2014. Ms. Stone confirmed that the workshop would be held in Albuquerque, New Mexico and explained it is open to all primary fusion center security liaisons and alternates if funding is available through their respective fusion center.

Ms. Stone proceeded to cover the tentative workshop agenda. She noted that Scott McAllister, Deputy Under Secretary, DHS OI&A, will be making the opening remarks. His remarks will be followed by security updates and a Federal Bureau of Investigation presentation. She added that workshop attendees will be asked to form three groups, and each group will have something to do at different breakout times of the day. Furthermore, she noted that the first day will be comprised of the following briefs: counterintelligence foreign access management, insider threat, clearance evaluations, and foreign disclosure. The briefs will be staggered throughout the day, so each group will have the opportunity for interaction and to raise questions. She explained the day would end with a Standard Form (SF) 312, "Classified Information Nondisclosure Agreement," briefing. Afterwards, presenters will be available for additional questions and hands-on labs.

She described day two as covering briefs on security compliance review (SCR) programs, the clearance and adjudication process, operations security, and social networking. Later in the day, these sessions will be followed by briefs on classified meetings, classified information handling, cyber security, and communication security policies. The day will conclude with hands-on labs and opportunities for attendees to ask in-depth questions. She noted that on day three attendees will be asked to revert back to one large group. The group will be given a presentation on derivative classification training. The day will conclude with a question-and-answer portion followed by closing remarks.

Concluding, Ms. Stone explained that DHS will be hosting a two-day security liaison training event in Washington, D.C., prior to the Security Liaison Training Workshop. The training is intended for new security liaisons as required by the DHS Implementing Directive.

D) Updates on SLTPS Security Program Implementation

The Chair called Mr. Rogers to provide updates on implementation of the SLTPS security program. Mr. Rogers reminded the Committee that in previous meetings he had discussed the establishment of an SCR program and reported that, in FY 2012, DHS conducted pilot SCRs.

He stated that 21 SCRs were conducted in FY 2013 and eight in FY 2014. In the last 15 months, DHS has conducted 30 SCRs. The SCRs have led DHS to conclude that fusion centers are working effectively; however, there is a significant turnover of security liaisons. At some centers there are full-time dedicated security liaisons positions, while at other locations law enforcement individuals are assigned these duties and frequently rotate to other assignments. For FY 2014, Mr. Rogers reported that DHS's goal is to complete a minimum of 15 SCRs. Having already completed eight SCRs, DHS will exceed the minimum.

Mr. Rogers briefly mentioned the self-inspection program as required by E.O. 13526, "Classified National Security Information." He explained that DHS had developed a self-inspection checklist to aid security liaisons. He elaborated that DHS assisted security liaisons with their respective self-inspections while DHS conducted the 21 SCRs of FY 2013. The findings where assimilated into the DHS final self-inspection report. He cautioned that the self-inspection program is a work in progress, requiring continual training and education. He mentioned that this requirement is necessary to condition fusion center personnel on the importance of self-inspections and nurture a self-inspection minded organizational culture.

In the course of Mr. Roger's presentation, Mr. Pannoni inquired about the extent of information sharing and the formal means of evaluating the effectiveness of information sharing. He asked if something like a survey could be included in self-inspections to evaluate satisfaction with information sharing. Mr. Rogers replied it is an element that can be considered and falls within the responsibilities of the State, Local, and Tribal Program Office in OI&A, which primarily oversees fusion center information sharing. This office may have evaluation metrics associated with information sharing. He indicated that he can contact OI&A to determine if there are evaluation metrics derived from their surveys. He emphasized that the role of his office is to ensure shared classified and sensitive information is adequately protected.

Mr. Pannoni deferred to the Chair asking whether the evaluation of information sharing among Federal agencies, not just DHS, should be a subject of consideration for the Committee. In reply, the Chair stated that it is a topic worthy of Committee consideration. Moreover, the question of whether information sharing increases in relation to specific security barrier eliminations could also be considered. He noted that once phase one of CVS implementation is completed an examination could be undertaken to assess whether information sharing has increased due to the removal of known or unknown security barriers. Mr. Rogers reiterated that he would refer this question to the State, Local, and Tribal Program Office. He furthered stated that a questionnaire could certainly be integrated into the SCR survey to ascertain if security barriers are impacting the information sharing mission.

Mr. Rogers continued, discussing training for security liaisons, emphasizing that training is a major focus of FY 2014. In addition to monthly webinar training sessions, there are plans to hold a quarterly two-day training session at DHS headquarters for newly appointed fusion center security liaisons. He noted that DHS views security liaison training as instrumental in disseminating training to all the fusion centers. DHS is utilizing the Homeland Security Information Network (HSIN) to deliver the training. He explained that there are about 1,700 private sector individuals cleared by DHS, and approximately 4,800 cleared state and local individuals.

Then, Mr. Rogers briefed the Committee on the HSIN. He stated that the HSIN underwent a revision requiring DHS to re-invite all members. At present, there are only 100 registered members. The goal is to have all cleared fusion center employees HSIN-registered, along with all cleared employees at the governors' offices. He went on to talk about an HSIN pilot program that is delivering two blocks of training: initial and annual refresher national security information (NSI) training. In conjunction with NSI training, DHS intends to add a briefing on the SF 312. He announced that DHS was given the approval to hire information technology personnel to accomplish the HSIN goals. The new hires, along with other DHS personnel, will develop a web-based platform to deliver training to private sector personnel, as well as state and local personnel. He concluded that in the past the primary focus for training was given to state and local personnel due to the fact that two thirds of the 72 fusion centers have HSIN access.

Mr. Miller asked whether, given the high turnover of security liaisons, DHS has helped security liaisons develop a transition document that they can provide to newly appointed security liaisons to inform them of their responsibilities. Mr. Rogers replied that no document has been developed, but DHS can consider developing such a document. In lieu of the availability of a transition document, DHS conducts monthly webinars that newly appointed security liaisons can attend, and many fusion centers have alternate security liaisons. Lindsey Johnson, SLTPS, added that, at the fusion center where she works, she created a transition document using the self-inspection checklist as a template and suggested it may be something other security liaisons could use. Mr. Rogers concurred.

E) Executive Branch Insider Threat Policy

The Chair then called Alegra Woodard, ISOO, to brief the Committee on the insider threat program. (See Attachment 4 for her presentation.) Ms. Woodard stated that she represents ISOO at the National Insider Threat Task Force (NITTF) and all the activity surrounding insider threat. She proceeded to briefly provide an overview of E.O. 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information." She mentioned that E.O. 13587 established the Senior Information Sharing and Safeguarding Steering Committee, which is co-chaired by the senior representatives of the Office of Management and Budget and the National Security Staff. It also established the NITTF, which is responsible for staffing and completing the national insider threat policy and minimum standards.

She stated that the insider threat program is a national security system priority and noted that on November 21, 2012, the President issued the National Insider Threat Policy and Minimum

Standards for the Executive Branch. The policy and minimum standards prescribe that each department and agency is to establish an insider threat program within 180 days. Agencies, at a minimum, should designate an insider threat program senior official. The senior official will be responsible for management and oversight of their agency's insider threat program. Furthermore, she noted that agencies are responsible for issuing an insider threat policy, signed by the agency head, and submitting an insider threat program implementation plan to agency leadership. The Chair clarified that the requirements apply to Federal agencies and these requirements, as expressed, do not apply to nonfederal entities, although, some portions of the requirement may affect members of nonfederal entities when those members engage with a Federal agency.

Ms. Woodard continued, noting that the insider threat program is intended to deter cleared employees from becoming insider threats, detect insiders who pose a risk to classified information, and mitigate risk through administrative, investigative, or other response actions. She explained that as part the program agencies are required to build and maintain an analytical and response capability which can be manual and/or electronic. The capability should encompass the integration of information derived from counterintelligence, security, information assurance, human resources, and law enforcement. Then, Ms. Woodard referenced the specific training requirements for insider threat program personnel, which include counterintelligence, security fundamentals, and procedures for conducting insider threat. She stated that these personnel should be allowed access to counterintelligence, information assurance, human resources, relevant organizational components, and classified or unclassified information necessary to identify, analyze, and resolve insider threat matters. In reference to accessing information, she noted that monitoring user activity networks is sensitive in nature, because it has to be cleared and requires the appropriate approvals. Either internally or via an agreement with external agencies, a technical capability must exist that allows monitoring of user activities on all classified networks. This will allow for detection of activity indicative of insider threat behavior.

Finally, Ms. Woodard mentioned overall employee insider threat training and awareness. She specified that an insider threat program will provide initial and annual refresher insider threat awareness training, either in person or computer-based, and verify that all cleared employees have completed the required insider threat awareness training. The training shall address current and potential threats in the work and personal environment and cover, at a minimum, the importance of detecting potential insider threat. The program should specify how to report suspicious activity, methodologies of adversaries to recruit trusted insiders and collect classified information, indicators of insider threat behavior, and procedures to report such behavior. She stated that if any member was interested in learning more about insider threat awareness training, the Defense Security Service provides an insider threat awareness course online, accessible at www.dss.mil under course code CI 121.06.

Following Ms. Woodard's presentation, Mr. Miller inquired if the creation of E.O. 13587 was influenced by root analysis of the Army Private Bradley Manning case or whether this a situation where we don't have anything that's effective so we're just going to build a whole solution for it. The Chair answered there were specific damage assessments done that included analysis of the Manning case. The Chair elaborated on E.O. 13587, stating that it can be viewed as a two-part policy: one, improving the safeguards in classified networks and two, safeguarding and sharing

of classified information. He noted that by increasing classified information sharing, the potential for compromise is omnipresent. In the past, intelligence and law enforcement communities were sensitive to this possibility of compromise and incorporated insider threat programs as a matter of course. He surmised that increased information sharing has led to analysis driving the evolution of the insider threat program and policies. He explained that the insider threat program requirements being promulgated are not to bring the Central Intelligence Agency or National Security Agency insider threat environment to all Federal agencies. The task of the insider threat program is to establish a framework to detect, mitigate, and respond to potential compromise of classified information, in essence a program that is always vigilant. Further, it is to have an appointed senior agency official accountable to the President. He pointed out that if private-sector personnel operate within the industrial security space there is a separate policy regime outlining which components of the insider threat program are going to be required. Ms. Woodard added that fundamentally it is about having a security framework to detect, deter, and react to an insider threat.

Mr. Rogers commented that DHS, like every Federal agency, is standing up an insider threat program that in all likelihood will impact the state and local sectors especially those that manage classified systems. Over time, as the DHS insider threat program becomes more defined, it will change the DHS SCR program.

III. General Open Forum/Discussion

The Chair indicated that the end of the planned agenda had been reached and solicited final questions and comments from all in attendance. Ashley Wilson, SLTPS, inquired as to what was the website mentioned by Ms. Woodard referencing insider threat awareness. The Chair responded the website address would be sent via email.

Then, Mr. Miller asked the Federal members whether their agencies were utilizing the concept of the fusion center model to cascade information out or previous communication models used prior to the stand up of fusion centers. Dr. Garmon West, Nuclear Regulatory Commission (NRC), responded that NRC, through its four regional offices, does have connection with fusion centers. Richard Donovan, Department of Energy (DOE), acknowledged that all DOE offices are in contact with fusion centers in their regional proximity. He elaborated that DOE tends to operate on a distributed model and each individual field office contacts a fusion center, unless there is a particular issue where access to restricted data or access to one of the DOE assets, such as a radiation monitoring team would be required.

Neal Duckworth, ODNI, added that the ODNI Interagency Threat Analysis and Coordination Group (ITACG) examines classified intelligence to identify actionable information of value to the State, Local, and Tribal elements and declassifies this information to a level which will be accessible to fusion centers. Ms. Johnson replied that ITACG is very effective. The Chair motioned that a briefing on the ITACG could be considered for the next Committee meeting or in a similar venue.

At the conclusion of the open forum remarks, Mr. Donovan noted that restricted data was not included in E.O. 13549. However, this does not signify that DOE will not share this type of information; rather it will be shared via a different route. He stated that restricted data would be

shared through state sector individuals cleared by DOE, as opposed to DHS, and facilities would be able to store restricted data if there is a need. Also, he emphasized that there are authorities the Secretary of Energy can invoke to disseminate restricted information to the state, local, and any other sector in a state of emergency or any critical national security event.

IV. Closing Remarks and Adjournment

The Chair thanked everyone for attending the meeting and for their contributions. He announced that the next SLTPS-PAC meeting would be held on Wednesday, July 23, 2014, in the National Archives Building from 10:00 a.m. to 12 noon. Also, he stated that ISOO plans to continue to provide teleconferencing capability for future SLTPS-PCA meetings. The meeting was adjourned at 11:25 a.m.

Attachment 1

SLTPS-PAC MEETING ATTENDEES/ABSENTEES

The following individuals were present at the January 24, 2014, SLTPS meeting:

• John Fitzpatrick	Information Security Oversight Office	Chairman
• Greg Pannoni	Information Security Oversight Office	DFO
• Clyde Miller	SLTPS Entity Representative	Vice Chair
• Joseph W. Lambert	Central Intelligence Agency	Member
• Neal Duckworth	Office of the Director of National Intelligence	Alternate Member
• Timothy A. Davis	Department of Defense	Member
• Richard Donovan	Department of Energy	Member
• Mark Perkul	Department of Energy	Alternate Member
• Leo Masciana	Department of State	Member
• Elizabeth (Beth) Hanley	Department of State	Alternate Member
• James Dewey Webb	SLTPS Entity Representative	Member*
• Benjamin E. Leingang	SLTPS Entity Representative	Member*
• Lindsey N. Johnson	SLTPS Entity Representative	Member
• William F. Pelgrin	SLTPS Entity Representative	Member*
• Ashley Wilson	SLTPS Entity Representative	Member*
• Trisha Prasnikar	Office of Personnel Management	Presenter*
• Nicole Stone	Department of Homeland Security	Presenter
• Charles Rogers	Department of Homeland Security	Presenter**
• Alegra Woodard	Information Security Oversight Office	Presenter
• Julie King	Department of Homeland Security	Observer
• Alaina Clark	Department of Homeland Security	Observer
• Britt Guilbert	Department of Homeland Security	Observer
• David Munro	Department of Homeland Security	Observer
• Carol Morehart	Office of Personnel Management	Observer*
• Booker Bland	Defense Security Service	Observer**
• Lt. Holly L. Barrett	SLTPS	Observer**
• Rich Hollas	Federal Bureau of Investigation	Observer**
• Nicholas J. Sims	Federal Bureau of Investigation	Observer*
• Dr. Garmon West	Nuclear Regulatory Commission	Observer**
• Bryan Oklin	Information Security Oversight Office	Staff
• Robert Skwirot	Information Security Oversight Office	Staff
• Joseph Taylor	Information Security Oversight Office	Staff

* Participated via teleconference

** Observing due to absence of member/alternate

Not Present at Meeting:

• John Young	Department of Homeland Security	Vice Chair
• Richard L. Hohman	Office of the Director of National Intelligence	Member
• Glenn R. Bensley	Department of Justice	Member
• Louis Widawski	Department of Transportation	Member
• Dr. Elaine Cummins	Federal Bureau of Investigation	Member
• Dr. Patricia Holahan,	Nuclear Regulatory Commission	Member
• Louis Widawski	Department of Transportation	Member
• Drew Winneberger	Defense Security Service	Member
• Robert Maloney	SLTPS Entity Representative	Member
• Kevin Donovan	SLTPS Entity Representative	Member

Attachment 2 – January 24, 2014, SLTPS-PAC Action items

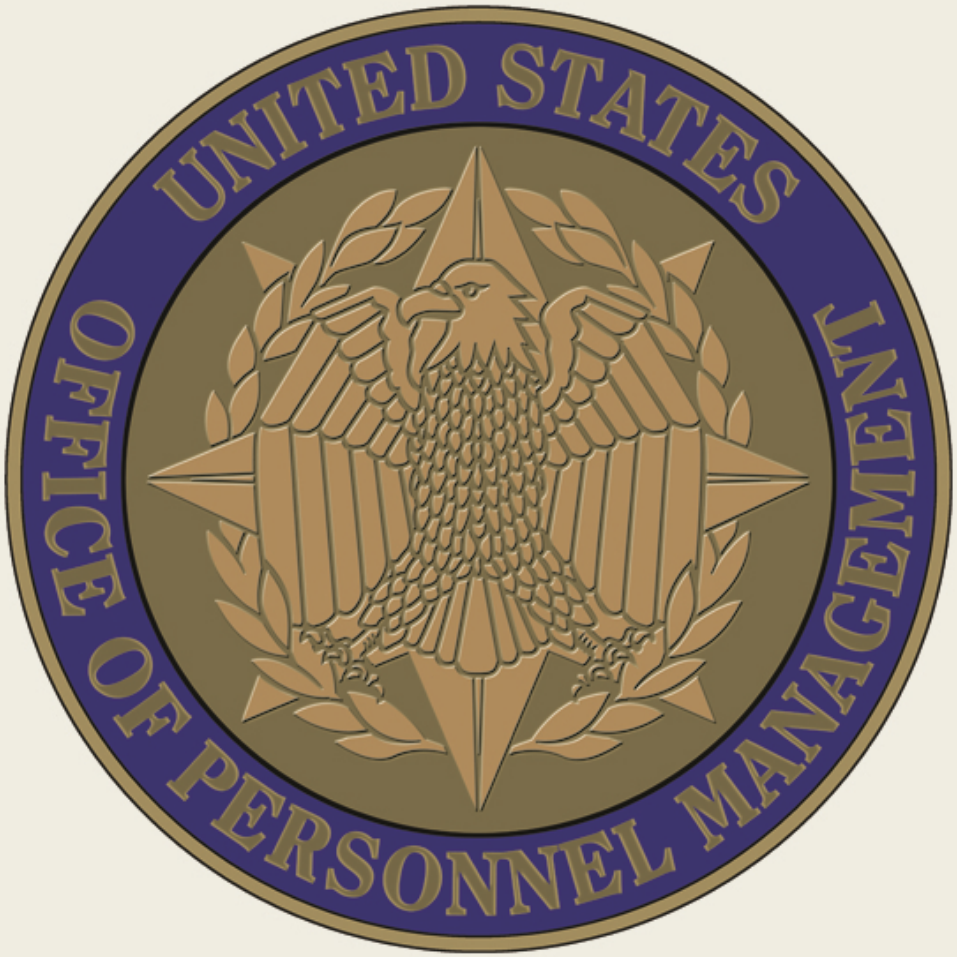
The following were action items identified during the meeting:

(1) DHS will report on efforts to identify/obtain evaluation metrics to ascertain the satisfaction with and effectiveness of information sharing.

(2) DHS will report on efforts to identify/develop a means to determine/measure increases in information sharing due to the removal of security barriers and the impact of security on information sharing.

(3) DHS will report on its efforts to develop a transition document that can be given to all newly appointed security liaisons to inform them of newly acquired responsibilities.

(4) The SLTPS-PAC staff will work with ODNI to determine the feasibility of arranging a briefing for the Committee on the Interagency Threat Analysis and Coordination Group.



a New Day for Federal Service

a New Day for Federal Service

OPM's Central Verification System (CVS)

Expansion Planned for Clearances Granted to State, Local, Tribal, Private Sector (SLTPS)

January 24, 2014

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

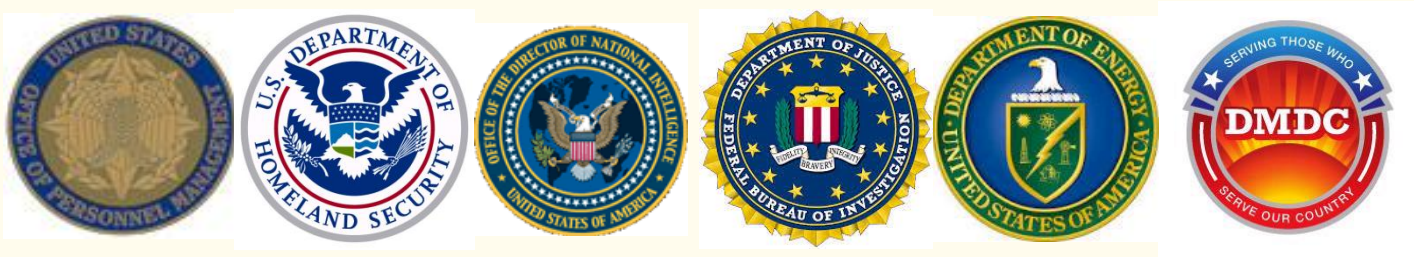
Overview

- **Status of the State, Local, Tribal, Private Sector (SLTPS) reciprocity project**
- **Review CVS changes**

SLTPS Project

- Partner with Department of Homeland Security (DHS), Office of Defense and National Intelligence (ODNI), and Department of Defense (DoD) to document and track security clearances granted to SLTPS personnel
- Clearance reciprocity and reporting is mandated by Executive Order 13549

Project to Date



- A working group formed in January 2013, and focused on requirements gathering
- Identified the need for new fields, a new user role and data reports
- Project split into phases

Phase 1

- Goal: February 2, 2014
- Add SLTPS security clearances to CVS
- Add data fields to the CVS database:
  - Affiliation of the clearance
  - SLTPS data (Program Office, Sector, and Details on the Subject's Duty Station)
- Produce a report of clearance holders for the granting federal agency

Phase 2

- Create a new user role for the Fusion Center staff known as “Security Liaisons”
- Enable Security Liaisons to verify clearances at the Secret Level
- Implementation date: TBD

Phase 1 next steps

- Continued development by OPM's Chief Information Officer
- Communicate information from OPM
  - Federal Investigations Notice
  - "Job Aid" for CVS users
- Testing & deployment by OPM staff
- Implementation goal of Phase 1: February 2, 2014

Questions?

OPM Points of Contact

Carol Morehart

CVS Functional Lead

Carol.Morehart@opm.gov

Trisha Prasnikar

Requirements & Policy

Trisha.Prasnikar@opm.gov

Attachment 4

Executive Branch Insider Threat Programs

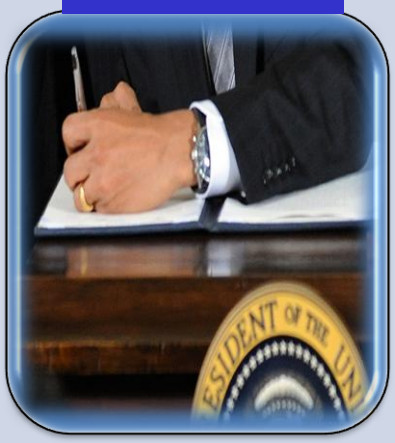
Alegra E. Woodard
Information Assurance Specialist - Operations & Industrial Security
Information Security Oversight Office (ISOO)
National Archives and Records Administration

January 2014

Executive Order 13587 Background

Unlawful disclosure of classified information by WikiLeaks in the summer of 2010

EO 13587
Oct 2011



The committee recommended government-wide actions to reduce the risk of a future breach

Senior Information Sharing and Safeguarding Steering Committee

Insider Threat Task Force

National Policy
Nov 2012

National Security System Priorities

Removable Media – Limit the number of users with removable media permissions and strengthen accountability for their use.

Insider Threat Programs – *Integrate specialized abilities, tools, and techniques to deter, detect, disrupt the insider threat, and provide training.*

Reduced Anonymity – Strengthen verification of the identity of individuals logging on to classified systems, and enable tracking.

Access Control – Implement standardized and interoperable access control systems to enforce access privileges at the network, application, and data levels.

Enterprise Audit – Integrate specialized abilities, tools, and techniques to deter, detect, disrupt the insider threat, and provide training and assistance to agencies to help them meet national policy and minimum standards requirements in this area.

Program Establishment

Designate an insider threat program senior official(s);

Issue an insider threat policy signed by your D/A head; and

Submit to D/A leadership an insider threat program implementation plan that addresses how D/As intend to meet the requirements set forth in the minimum standards.

Insider Threat Minimum Standards

Designate an insider threat program senior official(s);

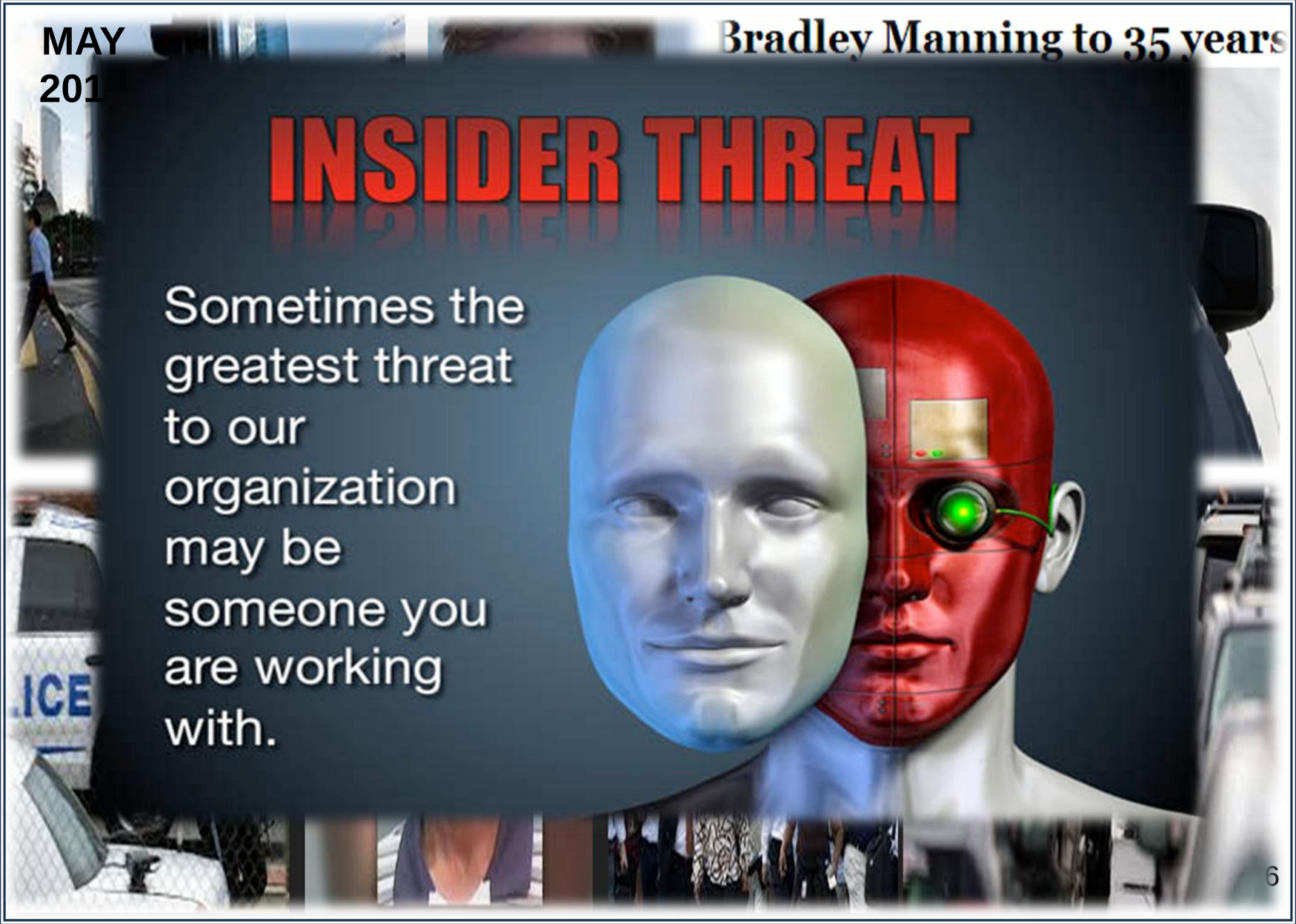
Information integration, analysis and response;

Insider threat program personnel;

Access to information;

Monitoring user activity on networks;

Employee training and awareness.


MAY
201
Bradley Manning to 35 years
INSIDER THREAT
Sometimes the greatest threat to our organization may be someone you are working with.
ICE

QUESTIONS?

Contact Information

Information Security Oversight Office
National Archives and Records Administration
700 Pennsylvania Avenue, N.W., Room 502C
Washington, DC 20408-0001

(202) 357-5351 (voice)
(202) 357-5908 (fax)
alegra.woodard@nara.gov

7