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

SUMMARY MINUTES OF THE MEETING

The SLTPS-PAC held its sixth meeting on Wednesday, July 24, 2013, at 10:00 a.m., at the National Archives Building, 700 Pennsylvania Avenue, NW, Washington, DC. Mr. Greg Pannoni, Information Security Oversight Office (ISOO), chaired the meeting, which was open to the public. The following minutes were finalized and certified on November 7, 2013.

Welcome, Introductions, and Administrative Matters

The Chair welcomed the attendees and, after introductions of those present, reminded everyone that SLTPS-PAC meetings are recorded events subject to the Federal Advisory Committee Act. He informed the members that the minutes would be made available through the ISOO website. (See Attachment 1 for a list of members and guests in attendance.)

The Chair introduced new SLTPS member Mr. William Pelgrin, President and Chief Executive Officer of the Center for Internet Security, and new Federal agency member Glenn Bensley, Assistant Director of Security and Emergency Planning, Justice Management Division, Department of Justice (DOJ). He also stated that there is vacancy on the SLTPS-PAC, because Mr. Gerald Wheeler is no longer the Executive Director of the Office of Public Safety, Seminole Tribe of Florida. The SLTPS-PAC staff will soon solicit a request for nominations from the membership. The Chair informed the meeting participants that their meeting folders included the meeting agenda, the minutes from the last meeting, and the slides for today's presentations. He stated that ISOO had e-mailed a copy of the 2012 National Network of Fusion Centers' (NNFC) final report and highly encouraged everyone to read it.

The Chair called on Ms. Terri Suit, SLTPS Vice Chair, to provide introductory comments. Ms. Suit informed the Committee that the Senate Select Committee on Intelligence is proposing the elimination of Department of Homeland Security (DHS) Intelligence and Analysis (I&A) agents from the NNFC, and she warned that this would be problematic for the interests of both the centers and the states. She emphasized that discourse with our state partners represents the Federal government's information conduit to state and local entities. She reminded the Committee that the Homeland Secure Data Network (HSDN) terminals are located in the fusion centers and that having an I&A agent in residence affords state and local analysts access to information maintained in the classified databases. Finally, the loss of access to classified information could hinder the capabilities of law enforcement officials as well as our other partners. She advised that the Committee closely monitor this potential problem, as the I&A agents are critical to state and local intelligence operations. The Chair suggested that this was likely a funding issue and asked Mr. Charlie Rogers, DHS, to bring the problem to the attention of the appropriate officials. Ms. Alaina Duggan, DHS, added that the information to which Ms. Suit alluded had originated in the Office of Intergovernmental Affairs and that she was in possession of two stakeholder letters from that office which she would share with Mr. Rogers. Ms. Suit reiterated that the issue affects crucial product development enterprises that assist officials in preparing for potential threats. She reminded the Committee that non-Federal partners must maintain access to the databases in order to continue analysis of published reports in support of the Threat and Hazard Identification and Risk Assessment process and to avoid hindering ongoing efforts to secure funding under the Urban Area Security Initiative grant program.

The Chair called on Mr. Rogers, who was representing the Federal government Vice Chair, to provide introductory comments. Mr. Rogers thanked several individuals and groups for the diligent work each performed in the preparation of the SLTPS clearance database, especially Ms. Carol Morehart and other staff members of the Federal Investigative Services Division of the Office of Personnel Management (OPM). He acknowledged the efforts of Joint Personnel Adjudication System (JPAS) personnel for completion of the database interface. He recognized Mr. Jim Plehal, DHS, for significant contributions to the development of database methodology, which expertly captured both Federal and SLTPS interests. Finally, he emphasized that although the project is not yet complete, substantial progress has been made.

I. Old Business

Updates from the Alternate Designated Federal Official (ADFO)

Mr. Bob Skwirot, ADFO, stated that the minutes of the January 30, 2013, SLTPS-PAC meeting were finalized and certified on March 20, 2013. He reminded the members that due to Federal sequestration we are unable to provide reimbursement of travel expenses and suggested that this perhaps accounts for the fact that some members were today participating via teleconference. He extended special appreciation to SLTPS members Ms. Suit, Mr. Pelgrin, and Mr. Clyde Miller who traveled at their own expense to participate in today's meeting. He stated that there were no action items from the last meeting. (Action items for this meeting are provided at Attachment 2.)

II. New Business

A) Incorporating SLTPS Security Clearance Data into the Central Verification System (CVS)

The Chair called on Ms. Carol Morehart to provide an update on the incorporation of SLTPS security clearance data into OPM's CVS. She stated that the SLTPS Working Group (SLTPSWG) continues to make significant progress in database design and development and expressed appreciation to Ms. Trisha Prasnikar, who was responsible for assembling today's presentation. She cautioned the Committee that the database development remains a work in progress and that there were additional enhancements yet to be completed. (See Attachment 2.) She stated that although there had been prior, unofficial planning meetings, the SLTPSWG's task on behalf of this project commenced in January 2013, with the primary goal being to implement requirements for depicting and displaying the SLTPS' users' view. The SLTPSWG, henceforth to be known as the CVS Stakeholder's Group (CVSSG), would be a collaborative effort and include representatives from OPM, DHS, the Office of the Director of National Intelligence (ODNI), DOJ, the Department of Energy (DOE), and the Defense Manpower Data Center of the Office of the Secretary of Defense. The working group's objective was to provide process input and to pose and provide answers to requirement items and concerns. Ultimately, the process would be built in two phases. During phase 1, the goals were to enter SLTPS clearance-holder information into this system and to identify new data fields that were necessary to facilitate this in order to make the CVS useful to the SLTPS community. Population of these data fields would permit the generation of a clearance-holder listing report, which would then be made available to all active agencies. Phase 2, the requirements for which were delivered to the fusion center staff developers on May 31, 2013, created a new user role within CVS called the "Security Liaison." Previously there had been but one CVS user role, the Security Officer, as well as some back-end suitability adjudicators from DoD. The new user role would give SLTPS security liaisons the capability to confirm security clearances. Mr. Rogers asked if the clearance status query would apply to everyone in the SLTPS community. Ms. Morehart responded that the query would apply to everyone whose clearance appears in either CVS or JPAS.

Ms. Morehart provided an artist's representation of the CVS "Display Clearance Detail" screen and described the query results as providing a detailed summary of the individual's clearance information. She described the contents of some of the new database fields, as well as some additional fields to be added in the future. She described a "pop-up" screen that the user can access, namely the "View SLTPS Info" screen, which contains such personalized information as program office, sector, and duty region. She reiterated that these screens were originally developed for the programmers but have subsequently been approved and disseminated to the developers. Ms. Morehart followed with an overview of the next steps in the process, including the two levels of training envisioned: initial level training, for existing CVS users, and second level training, specifically designed for the security liaisons. She requested that Mr. Rogers provide updates regarding additional training that the CVSSG has been tentatively discussing. He described a security liaisons' training workshop, perhaps to occur in early FY 2014 and promised to let her know when more details were available, so that they could prepare the advance training materials. However, he assured the Committee that DHS has other training initiatives even if the workshop should not prove feasible. Ms. Morehart then explained that, pending final deployment of Phase 1, now on target for delivery by December 2013, there will be an OPM-conducted testing and deployment period. She reminded the Committee that there is as no date yet for Phase 2 implementation, as timeframe and timeline decisions have not been made. Further, she stated that the CVSSG continues to discuss the need for a meeting roster, and she reminded all Federal agencies who have SLTPS clearance holders to please enter their information into the CVS. The Chair asked if there might be something, such as a memorandum of understanding, which the DNI, as the Security Executive Agent, might use to encourage the data entry initiative, as the exercise will be unprofitable if it is not soon completed. Mr. Neal Duckworth, ODNI, stated that such an idea is feasible for discussion, and he reminded the Committee that there is already an initiative which promotes combining CVS and JPAS information, followed by entering the results into Scattered Castles, in order to attain the desired centralized repository for clearance information. Ms. Morehart indicated it was her understanding that the fields that were being created are all optional. Mr. Rogers noted that DHS will certainly populate the fields but that all it can do with regard to other agencies is to highly encourage them to do the same, especially as the fields are designed to recognize private sector affiliations and to enable the Federal community to identify cleared critical infrastructure personnel. Finally, Ms. Morehart reminded the membership that either she or Ms. Prasnikar could be reached at any time with CVS data questions, confirmation requirements, or other policy clarifications.

B) An Overview of DHS Activities and Initiatives associated with the Implementation of Executive Order (E.O.) 13636, "Improving Critical Infrastructure Cybersecurity, and Presidential Policy Directive (PPD) 21, "Critical Infrastructure Security and Resilience."

The Chair reviewed the February 2013 announcement of the two Presidential directives of critical importance to the SLTPS initiative, the signing of E.O. 13636 and PPD 21, and asked Mr. Bob Kolasky, Senior Advisor to the Assistant Secretary for Infrastructure Protection, DHS, to provide an overview of DHS activities and initiatives associated with their implementation.

Mr. Kolasky noted that the President had assigned approximately 20 specific cybersecurity tasks to various Federal government departments and agencies. He indicated that he would provide updates on completed tasks and on the status of initiatives still in process and that he would report on what was being done in addition to providing the deliverables mandated by E.O. 13636 and PPD 21. (See Attachment 3.) He emphasized that it is imperative that everyone understand how important the critical infrastructure mission is throughout Federal, state, and local governments and that the security and resilience of critical infrastructure is essential to national and homeland security, as well as to public safety. He reminded the Committee that we must recognize that our infrastructure needs to operate efficiently and effectively if our economy is to survive and that the key to accomplish this lies in community resiliency. Further, although the government has a clear and important role to play in critical infrastructure security and resilience, it is often in a supporting capacity, as the majority of the infrastructure is owned by private companies and state and local governments. In addition, there are complex ownership structures in place, particularly with regard to locally regulated industries, and we must acknowledge that this is a collaborative effort. Moreover, we have to improve information-sharing methodologies, by placing strategic emphasis on creating a joint-planning and joint-priority environment.

Mr. Kolasky noted that the President made the decision to release these two policies on the same day to encourage rapid joint implementation, as addressing cyber challenges is a key part of addressing the risks we are facing, equal in scope with an all-hazards risk environment and inseparable from an all-hazards homeland security mission. We have already heard from numerous state, local, and business entities that cybersecurity is part of their overall enterprise risk-management approach, that it is an integral part of the capability decisions they are making in the face of these challenges, and that we must take a holistic approach to the two issues of security and resiliency. Therefore, Mr. Kolasky asserted that all critical infrastructure policies have to take into account the protection of cyber systems and networks from potential threats, including such wide-ranging conditions as terrorism, extreme weather conditions, and aging infrastructure. In addition, all future cybersecurity policy must emphasize the terms security and resiliency and support continued evolution towards achieving these goals. Resiliency implies the continued delivery of services and functions, even when systems are under duress or face failure.

Mr. Kolasky emphasized that we are no longer thinking only in terms of simple public-private partnerships, but rather a multitude of partnership types, in which information sharing is at the core of our ability to achieve unity in joint mission direction. The essence of the strategic vision within the two presidential documents can be best described as the development of a voluntary, technology-neutral cybersecurity framework. The National Institute of Standards and Technology (NIST) has been assigned the lead on this, but the NIST has publicly observed that the private sector, as the owner-operator community, needs to be in at the forefront of cybersecurity framework development. It is only in this way that we will we achieve a process through which the owners and operators of critical infrastructure can demonstrate their commitment to cybersecurity, including the steps they must take to secure their networks and develop the dynamic risk management techniques they must put in place to address the cyber threat. Further, we must recognize that investing in cybersecurity and adopting a cybersecurity framework is a business decision, regardless of whether it is made by government on behalf of government systems or by private industry on behalf of industry systems. Undoubtedly, owners and operators of critical infrastructure already have a serious commitment to cybersecurity, and that is why extensive investment is being made in every community and in every governmental and private sector entity. The cybersecurity framework envisions even more investment and greater confidence in future enhanced systems.

Mr. Kolasky pointed out that the Federal government has the ability to incentivize and change the cost-benefit equation by adopting a progressive and interactive cybersecurity framework, and that, through E.O. 13636, we will advance the most effective and efficient ways to promote the adoption of a sound national cybersecurity framework. In addition, as an information-sharing initiative, there is unilateral interest in increasing the volume, timeliness, quality, and trustworthiness of cyber-threat information, and we are continually trying to enhance our own internal processes, even as we work with owners and operators at many levels to ensure that we maintain strong privacy and civil-liberties protections. Moreover, the E.O. takes into account existing regulations, policies, and procedures that promote cybersecurity, such as that which exists in the Chemical Facility Anti-Terrorism Standards program, and asks regulatory agencies to study whether the cybersecurity framework will meet the regulatory requirements that are already in place. With regard to PPD 21 specifically, it too is concerned with taking and promoting immediate risk-management actions in the face of the cyber threat, and it challenges us to continuously evolve such practices in the face of all hazards. It forces us to continuously improve situational awareness capabilities and to address both physical and cyber risk, with a particular focus on interdependencies and the cascading impacts of failed infrastructure. It promotes an enhanced, collective understanding of infrastructure resiliency, so that we can learn to make decisions that, in the midst of the inevitable attacks and adverse incidents, will allow us to quickly and cost-effectively return our infrastructure or that of our partner communities to timely production. PPD 21 challenges us to constantly reevaluate and mature public-private sector partnerships we have already begun, as it too recognizes these relationships as key to achieving national success. We have learned many lessons working within government agencies, between DHS and state and local governments, and between the Federal and private sectors. Through state, local, and private sector ventures, we must continue to apply the tactics described in the National Infrastructure Protection Plan (NIPP), through which we will refine our initial infrastructure model. Further, this model must then evolve into a comprehensive research and development plan, which is mandated for completion by February of 2015. Mr. Kolasky described the Integrated Task Force (ITF), a body implemented by DHS in support of this initiative, which purposes to engage the entire interagency community in the achievement of several critical objectives, including infrastructure awareness, stakeholder understanding, world-wide cybersecurity framework feedback, and the promotion of initiatives to enable processes and procedures that combat infrastructure threats.

Mr. Kolasky then outlined the E.O. 13636 and PPD 21 timeline deliverables. The first set he covered included the 120-day requirements, which consisted of instructions on unclassified threat information, a report on cybersecurity incentives, and procedures for the expansion of enhanced cybersecurity services. The second included the 150-day requirements, which consisted of the identification of cybersecurity critical infrastructure, an evaluation of new and existing public-private partnership models, and the completion of the process for expediting private sector security clearances. He noted that there are public-private partnership models, largely captured in the NIPP, which include cross-sector, sector-coordinating, and government-coordinating councils, as well as information sharing advisory groups, that are enjoying success with regard to joint-planning initiatives, priorities identification, and information dissemination. Mr. Kolasky described the private-sector security clearance initiatives, which were discussed at this committee's meeting in January of this year, as containing new provisions instituted in private sector organizations that own the most critical infrastructure systems and where incidents could have the most deleterious effects. Further, these same processes have been refined to include the development of criteria to more quickly evaluate private sector officials who have been nominated for clearances, including Protective Security Advisors, sector-specific agencies, and DHS's own sector specialists. The third set that Mr. Kolasky outlined includes the 240-day deliverables, all of which must be completed by October 10, 2013. Among these are the development of situational awareness capabilities, initial updates to the NIPP, and the publication of a voluntary national cybersecurity framework. He mentioned 365-day and beyond deliverables, but explained that although initial ground work has begun, none have matured enough to merit objective comment. Thus far, the primary achievement has been an enhanced sense of the cyber-nexus of critical infrastructure. He noted that the E.O. intentionally uses the word *catastrophe*, which sets a very high threshold. Many communities now rely heavily on greatly interconnected cyber systems, creating a situation in which cyber incidents would have significant economic impacts and instantaneous consequences. However, the good news is the considerable resilience in many critical infrastructure sectors, which have been helped by enhanced information-sharing efforts. So, while there is a potential for bad things to happen, efforts are well underway to create resilient systems in which vulnerability protections and back-up systems are in place and sound risk-management is applied.

Next, Mr. Kolasky described the efforts of DHS, in consultation with ODNI and DOJ, to meet the E.O. requirements for building systems and processes to track the dissemination of cyber-threat information. The objective is to gain a better understanding of the effectiveness of our owner-operator information-sharing processes and to determine whether the methodology is supportive of sound decision making. He spoke briefly about the focus of work being done in collaboration with the NIST on the draft cybersecurity framework, noting that this product is due in February of 2014, at which time DHS will have the responsibility to use it in collaboration with specific sector critical-infrastructure owner-operators to promote adoption of the processes. The hope is that all this will lead to the enhanced sharing of modernized risk reduction techniques and support for higher levels of cybersecurity models that include flexibility and innovation while ensuring long-term improvement. Ms. Suit asked Mr. Kolasky if he was aware of an initiative to have the National Guard become the responsible agent for all cybersecurity activities and as such to serve as the responding authority for all cybersecurity-related events. Mr. Kolasky stated that he was aware that the cybersecurity and communications officials at DHS were involved in discussions on the merits of such a scenario, especially in view of the fact that with so many disparate activities involved in this program there is the risk of misalignment.

In addition, he pointed out that one of the primary reasons for the President's creation of the Council of Governors (COG) was to institute a forum wherein state government representatives could work collaboratively on cybersecurity issues and that in that forum the concept of employing the National Guard as a first responder to cybersecurity events has become a main discussion topic. Mr. Kolasky recommended that Committee personnel consider addressing this and similar questions to Mr. Todd Rosenblum, who as Acting Assistant Secretary of Defense for Homeland Defense and America's Security Affairs, serves as DoD's representative to the COG, or to Ms. Suzanne Spaulding, who as Deputy Undersecretary for the National Protection and Programs Directorate at DHS, as well as the author of the National Infrastructure Advisory Council, would likely be best informed in this area.

The Chair drew attention to a related topic, the Controlled Unclassified Information (CUI) program, for which NARA is the Executive Agent. He pointed out that CUI representatives from a large number of government agencies have been developing a national registry of categories and subcategories that will ultimately be used in the identification of information that is unclassified but requires controls, and he suggested that DHS personnel associated with the SLTPS should invite CUI officials to serve on one of the working groups, such as the ITF. In addition, he mentioned a requirement of the National Defense Authorization Act (NDAA) of 2013 that calls for the creation of "Covered Networks." Such a network is described as an unclassified network or information system of a cleared defense contractor that contains information by or for the DoD with respect to which such contractor is required to apply enhanced protection. These networks will require certain unique reporting requirements. One such requirement involves a category of information called "DoD Controlled Technical Information." This will require controls that will be established in coordination with NARA and NIST.

Mr. Kolasky described one final E.O. and PPD 21 deliverable requirement, due in August of 2013 that prescribes baseline data and systems requirements to promote the interoperable sharing of physical and cyber risk information in order to ensure increased situational awareness. The Chair then mentioned one additional sensitive information initiative, a "spectrum" program, operated by the Office of Science and Technology. This is a partnership in which technology and innovation are shared in order to advance economic growth and/or new opportunities. Unintentionally, DHS was not included in this effort. ISOO has suggested that John Young, DHS, join the discussion, as it intersects with the actions that DHS is undertaking.

Mr. Leo Masciana, Department of State, asked if DHS has developed a model for the capabilities and skill sets for its Cyber Emergency Response Team (CERT). Mr. Kolasky responded that there is a model in place, but that he could not personally speak to its details. A report on specific details could be provided at a future meeting. However, he could report that DHS has already shared its CERT model with several nations, some of whom have subsequently deployed their own teams. Mr. Masciana also made the suggestion that the SLTPS-PAC get involved in the efforts of the ITF, as the Committee has a keen interest in any activities that relate to access shared within classified forums.

C) Updates on SLTPS Security Program Implementation

The Chair then called Charlie 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 a Security Compliance Review (SCR) program and reported that, in the fall of 2012, DHS conducted three pilot SCR program reviews at the Virginia Fusion Center, Richmond, Va., the West Virginia Intelligence/Fusion Center, Charleston, W. Va., and the Delaware Information and Analysis Center, Dover, Del. He stated that there have been 16 SCRs conducted at the state fusion centers, the most recent at the Vermont Information and Analysis Fusion Center, Williston, Vt., and the Connecticut Intelligence Center, New Haven, Conn. By the end of the fiscal year there will have been a total of 22. (See Attachment 4.) Mr. Rogers reminded the Committee that, when the implementing directive for E.O. 13549, "Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities" was published in February of 2012, it included some additional responsibilities the security liaisons would assume and formally established a security liaison program. He asserted that the SCRs have proven to be an effective tool to implement this program, as they evaluate how well the fusion centers are managing classified information and serve as a tool to help train the new security liaisons to assume their duties. The visits have uncovered no significant problems, and no classified information vulnerabilities were identified. Rather, the SCRs found only minor issues, which, wherever possible, were immediately addressed. For example, some centers have failed to perform the required quarterly alarm test; some centers were careful to confirm the security clearances of anyone entering a secure area but failed to maintain the required signature log; and some failed to make combination changes in the required timeframe. On a positive note, the SCRs found that both the leadership and the individual liaisons were taking their responsibilities very seriously. The SCR specialists also discovered that the liaisons work in close partnership with deployed I&A personnel. However, the reviews revealed that fusion center personnel are generally not taking advantage of the HSDN that DHS has provided for them. Although nearly all cleared fusion center personnel have HSDN accounts, it is mainly the I&A specialists who search the HSDN to find and retrieve documents that support fusion center mission requirements. Mr. Rogers explained that DHS requires everyone who has been authorized an HSDN account to be trained in derivative classification procedures, as there is always the possibility that they will need that skill, and was pleased to confirm that this training has now been completed for approximately 90% of the required personnel. He also noted that the fusion centers have not generated derivatively classified documents but have created a significant amount of sensitive but unclassified law enforcement material that would fall under the CUI program when it is fully implemented. He pointed out that the classified holdings stored at the fusion centers visited to date are extremely limited in number and are being maintained for reference use only. Also, he reported that only a few of the classified documents being held contain any marking discrepancies. The Chair asked if the SCRs explored the volume of information being shared among the fusion centers, especially in view of the related information available in the NNFC's recent report. Mr. Rogers responded that their analysis to date had not taken that factor into account. Rather, they have thus far focused on the aforementioned items, as well as the process for managing meetings and the procedures for verifying clearances. He pointed out that the SCRs did find an insufficient number of couriers and that I&A representatives will soon brief state government and law enforcement officials of that need. In addition, the SCR specialists report that notwithstanding the high turnover of both fusion center directors and security liaisons, the classified program is fairly well managed. Mr. Rogers reported to the Committee that DHS is holding monthly training sessions via teleconference webinar, that 44 security liaisons have been trained this far, and that a total of eight sessions will have been conducted by the end of the fiscal year. He also pointed out that each completed SCR constitutes a formal self-inspection. In addition, he described the development of a self-inspection checklist, a derivative-classification log, and a formally required documentation report. He stated that the field security coordinators are reaching out to all security liaisons to ensure that locations not yet scheduled for an SCR will complete the checklist in accordance with Executive Order 13526, "Classified National Security Information." Mr. Rogers expects to meet with ISOO officials at some future date to coordinate on the most effective means to report the results.

Mr. Rogers updated the Committee on the status of the Homeland Security Information Network (HSIN) website, describing it as a web-based platform designed to allow SLTPS, and Federal agencies to share sensitive but unclassified information over a secure channel. In addition, the HSDN provides three main functional categories: a SharePoint web portal that provides a basic collaboration workspace for agencies and events, a Jabber Web-Chat system with user-managed chat rooms, and a custom executive situational awareness web application based on the Oracle HyperText Markup Language known as the Common Operational Picture. The system currently has approximately 12,000 users, and encompasses numerous websites, to include those of law enforcement, first-responders, and I&A. The SLTPS program has a small piece of the HSDN: the security management website. Initially the focus was on enrolling the security liaisons so that they would have a secure place to post security products, but that has been expanded by encouraging participation by all cleared state and local users. In addition, the HSIN is in the midst of a redesign to enhance security and offer more efficient webinar capabilities. Also, DHS has reached out to the fusion centers to get cleared employee e-mail addresses, so that they can be invited to participate on HSIN as soon as its redesign is complete. Ms. Suit suggested that there is also a robust group of cleared personnel that have nothing directly to do with the fusion centers, including people working on potential bioterrorism issues, technology specialists who operate entire state infrastructures that address threat issues, as well as evacuation planning people in the National Capitol Region, who should be considered as viable user candidates. Mr. Rogers agreed and explained that DHS is well-positioned to expand to other markets, but he noted that it is presently concentrating on system stand up. Also, because the fusion centers have the largest classified footprint and up to 72 fusion centers still need to be reached, DHS believes it should begin with them.

Mr. Rogers concluded with an update on two previously announced security forms. The first is a private-sector acknowledgement form to be given to individuals who, though employed by contractors, are granted a clearance outside of the authority of the National Industrial Security Program Operating Manual. The purpose for this form is to advise cleared personnel of their responsibilities and to confirm that the clearance is associated with the individual rather than the company. The second is a form to be signed by senior personnel who are responsible for locations, such as fusion center directors; this form describes specific location responsibilities. He stated that both forms have made it through the coordination process and received legal comments, and that he will soon reformat them, highlight the legally required edits, and return them to SLTPS-PAC for concurrence, which baring a complete rewrite, should lead to early approval and publication.

III. General Open Forum/Discussion

The Chair indicated that we had reached the end of the planned agenda and solicited final questions and comments from the membership and all in attendance. Homero Navarro, ISOO, stated that the SLTPS-PAC has always placed significant emphasis on cybersecurity and international terrorism. However, in view of the nation's frequent incidents of environmental terrorism should not the Committee begin to place attention on its impact on state, local, tribal, and private sector activities? There followed general agreement that this issue should be explored, especially its relationship to various critical infrastructure components, such as chemical, physical, and cyber terrorism. Mr. Rogers offered to take the question back to DHS to find out who might be best able to enlighten the SLTPS community.

Ms. Suit advised the Committee that this meeting would be her last and recommended that the Committee leadership should begin the search for an SLTPS-PAC member to serve as Vice Chair. The Chair thanked her for many valuable contributions to the business of the SLTPS-PAC and acknowledged that we would indeed begin the search for her replacement.

IV. Closing Remarks and Adjournment

The Chair thanked everyone for attending the meeting and for all contributions. He announced that the next SLTPS-PAC meeting would be held on Friday, January 24, 2014, in the National Archives Building from 10:00 a.m. to 12 noon, followed by a meeting tentatively scheduled for Wednesday, July 23, 2014. Also, he stated that ISOO plans to continue to provide teleconferencing capability for future SLTPS-PCA meetings. The meeting was adjourned at 11:41 a.m.

Attachment 1

SLTPS-PAC MEETING ATTENDEES/ABSENTEES

The following individuals were present at the July 24, 2013, SLTPS meeting:

Greg Pannoni	Information Security Oversight Office	Acting Chairman
Robert Skwirot	Information Security Oversight Office	Alternate DFO
Terri Suit	SLTPS Entity Representative	Vice Chair
Glenn R. Bensley	Department of Justice	Member *
Leo Masciana	Department of State	Member
Clyde Miller	SLTPS Entity Representative	Member
William F. Pelgrin	SLTPS Entity Representative	Member
Lindsey N. Johnson	SLTPS Entity Representative	Member*
Col. Marcus L. Brown	SLTPS, Entity Representative	Member*
Mark Pekrul	Department of Energy,	Alternate Member
Bernard Stapleton	Nuclear Regulatory Commission	Alternate Member
Neal Duckworth	Office of the Director of National Intelligence	Alternate Member
Carol Morehart	Office of Personnel Management	Presenter
Robert Kolasky	Department of Homeland Security	Presenter
Charles Rogers	Department of Homeland Security	Observer**
Deborah Lebo	Central Intelligence Agency	Observer
Teresa Stasiuk	Central Intelligence Agency	Observer**
Richard Hollas	Federal Bureau of Investigation	Observer **
Kate Connor	Department of State	Observer
Erin Lane	Office of the Director of National Security	Observer
Janice Cornwell	Department Of Homeland Security	Observer
Tasha Bailey	Department of Homeland Security	Observer
Nicole Stone	Department of Homeland Security	Observer
James Plehal	Department of Homeland Security	Observer
Renee Murphy	Department of Homeland Security,	Observer
Booker Bland	Defense Security Service	Observer**
Lori Ellison	Department of Justice	Observer *
James Dunlap	Department of Justice	Observer*
Alaina Duggan	Department of Homeland Security	Observer*
Homero Navarro	Information Security Oversight Office	Staff
William Greco	Information Security Oversight Office	Staff
Joseph Taylor	Information Security Oversight Office	Staff

* - Teleconferenced the meeting
**- Representing Agency

Not Present at Meeting:

• John Young	Department of Homeland Security	Vice Chair
• Francis Taylor	SLTPS Entity Representative	Member
• Robert Maloney	SLTPS Entity Representative	Member
• Kevin Donovan	SLTPS Entity Representative	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
• Joseph W. Lambert	Central Intelligence Agency	Member

Attachment 2 – July 24, 2013, SLTPS-PAC Action items

The following were action items identified during the meeting:

(1) DHS will report on its inquiry into a possible threat to eliminate its Intelligence and Analysis agents from the National Network of Fusion Centers.

(2) DHS will report on its efforts to invite Controlled Unclassified Information officials from a number of government agencies to serve on its Integrated Task Force Working Group, or a similarly functioning activity, in order to take advantage of the developing national registry of categories and subcategories that will ultimately be used in the identification of information that is unclassified but requires controls.

(3) DHS will report on its efforts to identify the appropriate individual(s) to brief the SLTPS-PAC on the potential impact of environmental terrorism on various critical infrastructure elements, such as chemical, physical, and cyber, in state, local, tribal, and private sector contexts.

(4) Upon the departure of Ms. Teri Suit, ISOO will work with SLTPS representatives to nominate and select a new SLTPS-PAC Vice Chair.

Attachment # 3

Central Verification System Presentation

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

a New Day for Federal Service

a New Day for Federal Service

OPM's
Central Verification System (CVS)

This overview is presented to the
State, Local, Tribal, Private Sector
Policy Advisory Committee
July 24, 2013

Overview

- Provide an update on the SLTPS-CVS reciprocity project since January 2013

- Identify next steps for the partnership with SLTPS

Since our last presentation…

- A Working Group commenced and focused on gathering requirements
- Met several times, January – May
- CVS Stakeholders represented:

Produced user requirements…

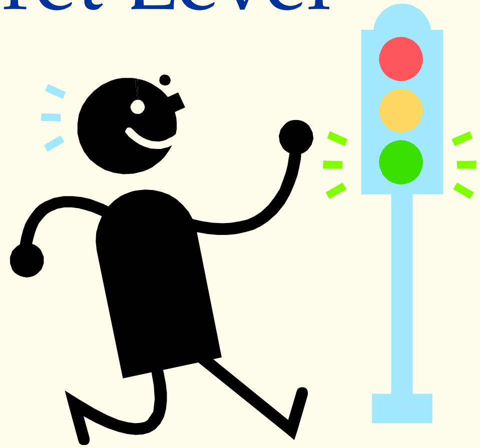
Phase 1 (Requirements delivered 3/31/13)

- 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

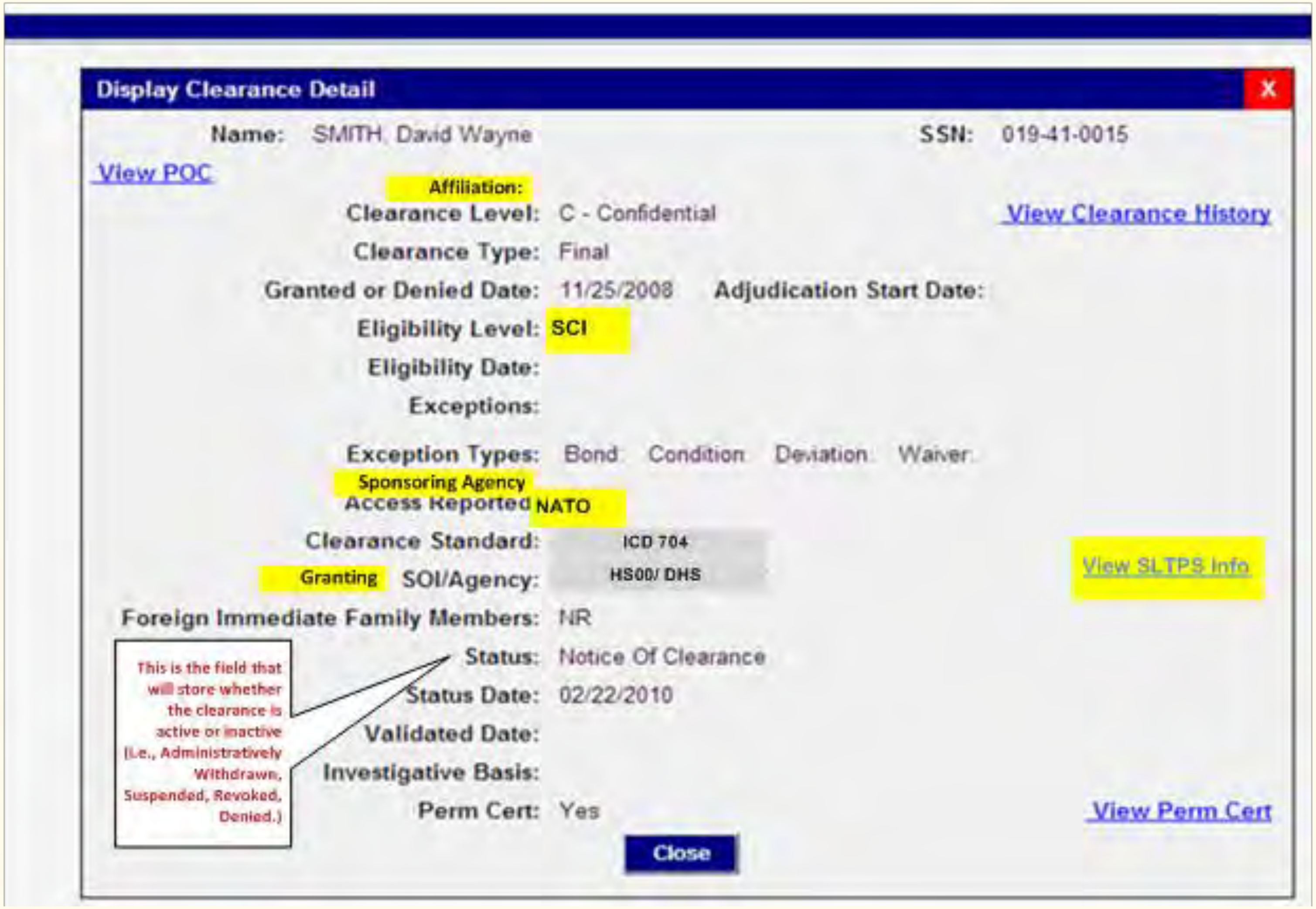
Produced user requirements…

Phase 2 (Requirements delivered 5/31/13)

- Create a new user role for the Fusion Center staff known as "Security Liaisons"
- Enable Security Liaisons to verify clearances at the Secret Level



Artist's rendering…



Display Clearance Detail

Name: SMITH, David Wayne

SSN: 019-41-0015

Affiliation:

Clearance Level: C - Confidential

Clearance Type: Final

Granted or Denied Date: 11/25/2008

Adjudication Start Date:

Eligibility Level: SCI

Eligibility Date:

Exceptions:

Exception Types: Bond Condition Deviation Waiver

Sponsoring Agency

Access Reported NATO

Clearance Standard: ICD 704

Granting SOI/Agency: HS00/ DHS

Foreign Immediate Family Members: NR

Status: Notice Of Clearance

Status Date: 02/22/2010

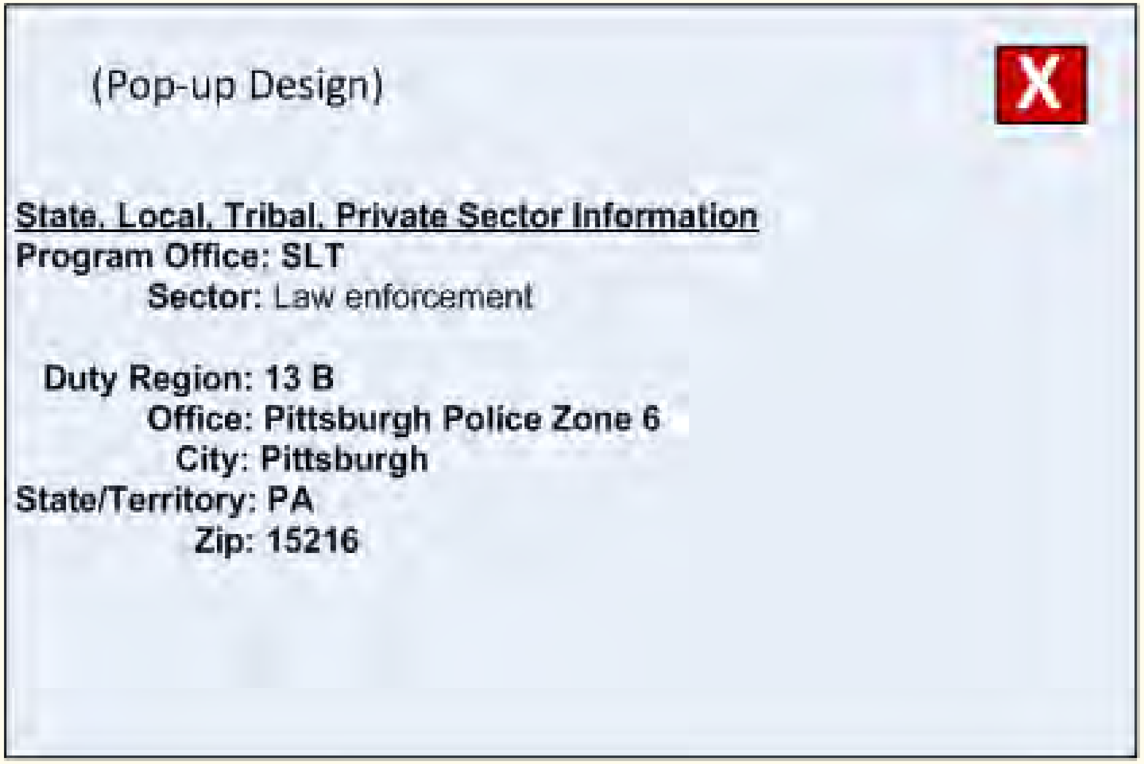
Validated Date:

Investigative Basis:

Perm Cert: Yes

This is the field that will store whether the clearance is active or inactive (i.e., Administratively Withdrawn, Suspended, Revoked, Denied.)

SLTPS "pop-up"



(Pop-up Design)

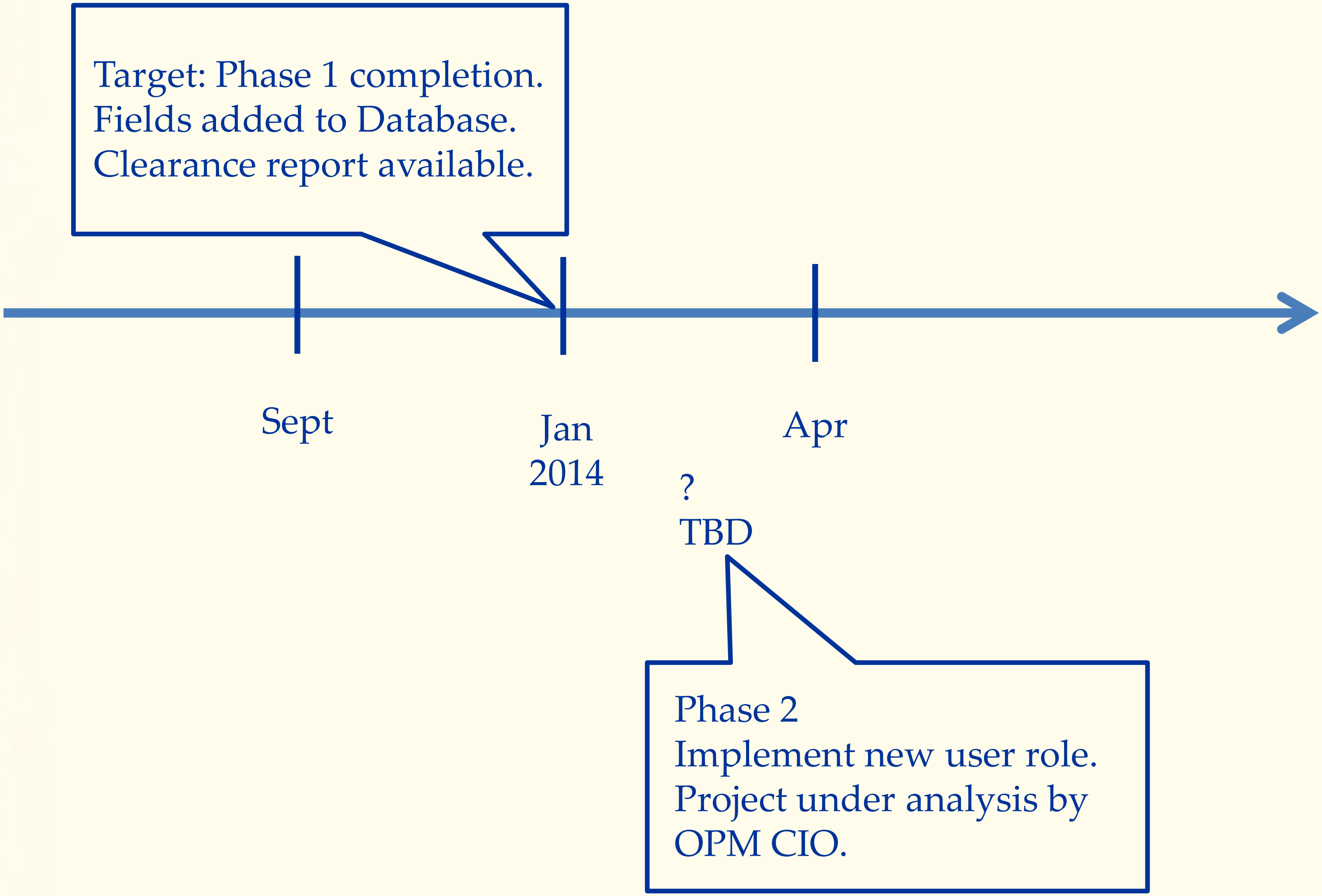
State, Local, Tribal, Private Sector Information
Program Office: SLT
Sector: Law enforcement

Duty Region: 13 B
Office: Pittsburgh Police Zone 6
City: Pittsburgh
State/Territory: PA
Zip: 15216

Next steps…

- Continued Analysis & Development by OPM's CIO
- Communication and Training plans needed
  - OPM (Existing CVS users)
  - DHS (SLTPS community)
- Testing & Deployment by OPM staff

Basic Timeline…



Target: Phase 1 completion.
Fields added to Database.
Clearance report available.

Sept

Jan
2014

Apr

?
TBD

Phase 2
Implement new user role.
Project under analysis by
OPM CIO.

Continued partnership…

- Requirements for "Meeting Rosters"?
- Encourage Federal agencies with SLTPS clearances to report those clearances to CVS
- Prepare Federal SLTPS stakeholders to populate new CVS database fields
- Prepare "Security Liaisons" as a new CVS user population (closer to deployment)

Questions?

OPM Points of Contact

Carol Morehart	**Trisha Prasnikar**
CVS Functional Lead	Requirements & Policy
Carol.Morehart@opm.gov	Trisha.Prasnikar@opm.gov

Attachment # 4

Cybersecurity Presentation

Implementing the Administration's Critical Infrastructure and Cybersecurity Policy

Cybersecurity Executive Order and Critical Infrastructure Security & Resilience Presidential Policy Directive Integrated Task Force

July 2013

Homeland Security

Enhancing Security & Resilience

- America's national security and economic prosperity are dependent upon the operation of critical infrastructure that are increasingly at risk to the effects of cyber attacks
- The vast majority of U.S. critical infrastructure is owned and operated by private companies
- A strong partnership between government and industry is indispensible to reducing the risk to these vital systems
- We are building critical infrastructure resiliency by establishing and leveraging these partnerships

Taking Action

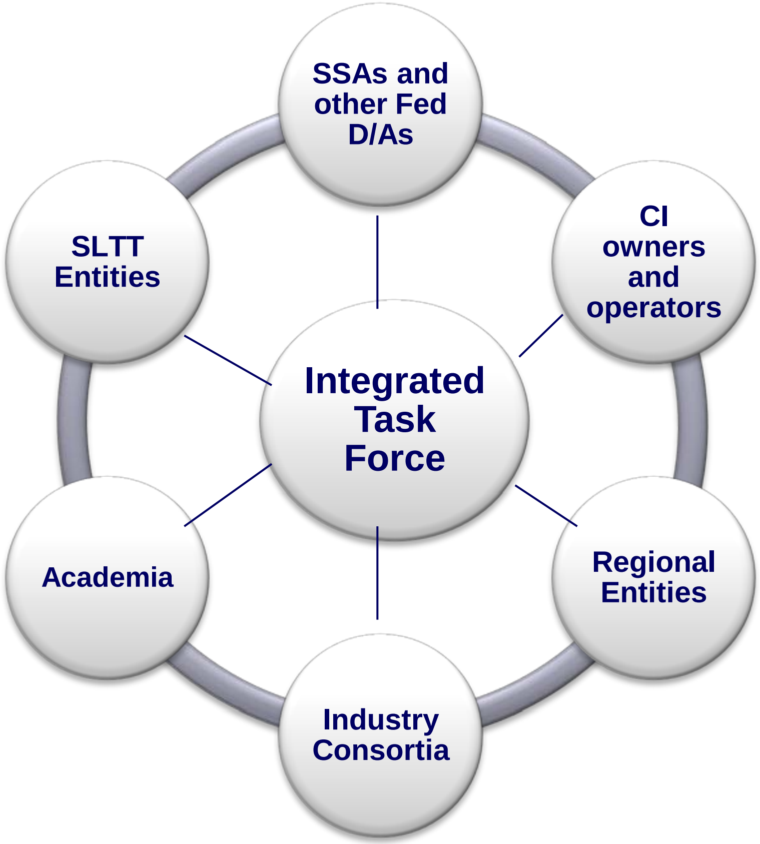
- In February 2013, the President announced two new policies
  1) Executive Order 13636: Improving Critical Infrastructure Cybersecurity
  2) Presidential Policy Directive – 21: Critical Infrastructure Security and Resilience
- Together, they create an opportunity to work together to effect a comprehensive national approach to security and risk management
- Implementation efforts will drive action toward ***system* and *network*** security and resiliency

Integrating Cyber-Physical Security

- ***Executive Order 13636: Improving Critical Infrastructure Cybersecurity*** directs the Executive Branch to:
  - Develop a technology-neutral voluntary cybersecurity framework
  - Promote and incentivize the adoption of cybersecurity practices
  - Increase the volume, timeliness and quality of cyber threat information sharing
  - Incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure
  - Explore the use of existing regulation to promote cyber security

- ***Presidential Policy Directive-21: Critical Infrastructure Security and Resilience*** replaces Homeland Security Presidential Directive-7 and directs the Executive Branch to:
  - Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time
  - Understand the cascading consequences of infrastructure failures
  - Evaluate and mature the public-private partnership
  - Update the National Infrastructure Protection Plan
  - Develop comprehensive research and development plan

Stakeholder Engagement Model



Guiding Principles

- Involve those responsible for critical infrastructure security and resilience.
- Reflect stakeholder views in program design and policy implementation.
- Use existing bodies and channels when possible, supplemented as needed to ensure a diversity of relevant viewpoints.

EO-PPD Deliverables

120 days – **June 12, 2013**

- Publish instructions: unclassified threat information
- Report on cybersecurity incentives
- Publish procedures: expand the Enhanced Cybersecurity Services

☑

150 Days - **July 12, 2013**

- Identify cybersecurity critical infrastructure
- Evaluate public-private partnership models
- Expedite security clearances for private sector

☑

240 Days – **October 10, 2013**

- Develop a situational awareness capability
- Update the National Infrastructure Protection Plan
- Publish draft voluntary Cybersecurity Framework

365 days – **February 12, 2014**

- Report on privacy and civil rights and civil liberties cybersecurity enhancement risks
- Stand up voluntary program based on finalized Cybersecurity Framework

Beyond 365 - **TBD**

- Critical Infrastructure Security and Resilience R&D Plan

Integrated Task Force (ITF)

- Establishes and manages working groups to accomplish the major deliverables and action items
- Integrates efforts for delivering EO and PPD requirements
- Develops and manages the governance process
- Engages relevant partners and stakeholders to develop products
    - Request for Information, Federal Register Notices, social media, meetings, presentations, workshops, interviews, etc
- Regularly reports on progress made throughout the EO and PPD implementation to partners and stakeholders

Working Groups

1) Stakeholder Engagement
2) Planning and Evaluation
3) Situational Awareness and Information Exchange
4) Cyber-Dependent Infrastructure Identification
5) Voluntary Program
6) Information Sharing
7) Research and Development
8) Framework Collaboration
9) Assessments: Privacy and Civil Rights & Civil Liberties

Principles of Engagement

- Partnership and inclusivity
- Leverage existing and ongoing work, frameworks, and venues
  - … and identify opportunities to expand
- Strive towards broad support for EO and PPD products
- Communicate clearly
- Be transparent in product development
- Embed privacy and civil rights & civil liberties protections
- Innovate engagement opportunities

Collaborative Community: IdeaScale

- Information sharing has been a key component of this process. In April, the ITF launched another critical component to implementation of the EO and PPD – a platform for posting and sharing public comments and feedback.
- The ITF has created a Collaboration Community on IdeaScale for critical infrastructure stakeholders and all interested members of the public to participate in dialogue about strengthening the security and resilience of our Nation’s critical infrastructure.
- To participate, visit http://eoppd.ideascale.com.

Contact Us and Participation

- DHS administers the working groups
- The working groups seek regular and substantive engagement from across the community
- The ITF has engagements with Federal, State, local, Tribal, Territorial, international, private sector and academic partners
  - We welcome and encourage additional engagements
- Inquires can be sent to EO-PPDTaskForce@hq.dhs.gov

http://www.dhs.gov/eoppd

U.S. DEPARTMENT OF HOMELAND SECURITY

Homeland
Security

Attachment # 5

Security Compliance Reviews Presentation

Office of the Chief Security Officer
U.S. Department of Homeland Security
Washington, DC 20528

Homeland
Security

State, Local & Tribal (SLT) Security Compliance Reviews (SCR)

1. Virginia Fusion Center, Richmond, VA in September 27-28; (FY-12)
(First SCR conducted)

The following locations have been conducted in (FY-13):

2. West Virginia Intelligence/Fusion Center, Charleston, WV on November 14-15.
3. The Delaware Information and Analysis Center, Dover, DE on December 11-12.
4. State Terrorism Threat Assessment Center, Mather, CA on February 20-21.
5. Georgia Information and Analysis Center, Atlanta, GA on February 26-27.
6. Florida Fusion Center, Tallahassee, FL, on March 5-6.
7. Southeast Florida Fusion Center, Doral, Florida on March 19-20.
8. Ohio Homeland Security, Strategic Analysis & Info Center, Columbus, OH on April 9-10.
9. Houston Regional Information Sharing Center, Houston, TX on April 22-24.
10. North Central Texas Fusion Center, McKinney, TX on April 24-25.
11. Indiana Intelligence Fusion Center, Indianapolis, IN on May 14-15.
12. County Regional Terrorism Early Warning Group, Cincinnati, OH on May 16-17.
13. Boston Regional Intelligence Center (BRIC) Roxbury, MA on May 21-22.
14. Commonwealth Fusion Center, Maynard, MA on May 23-24.

By the end of the 3rd quarter (FY-13) 14 SCRs were conducted, 13 in FY-13.

15. Vermont Information and Analysis Fusion Center, Williston, VT on July 16-17.
16. Connecticut Intelligence Center (CTIC) New Haven, CT on July 18-19

The following SCRs are planned:

17. Crime Prevention and Information Center (CPIC) Chicago, IL on July 30-31.
18. Iowa Intelligence Fusion Center, Des Moines, IA on August 1-2.
19. Nebraska Information Analysis Center (NIAC) Lincoln, NE on August 6-7.
20. Kansas City Regional Terrorism Early Warning Group Interagency Analysis Center Kansas City, MO on August 8-9.
21. Missouri Information Analysis Center (MIAC) Jefferson, MO on August 20-21.
22. St. Louis Missouri Fusion Center Terrorism Early Warning Group, St. Louis, MO on August 22-23.