STATE, LOCAL, TRIBAL, AND PRIVATE SECTOR POLICY ADVISORY COMMITTEE (SLTPS-PAC)
July 24, 2019

SUMMARY MINUTES OF THE MEETING

The SLTPS-PAC held its sixteenth meeting on Wednesday, July 24, 2019, at 10:00 a.m., at the National Archives Building, 700 Pennsylvania Avenue, NW, Washington, DC. Mark Bradley, Director, Information Security Oversight Office (ISOO), chaired the meeting, which was open to the public. The following minutes were finalized and certified on November 8, 2019.

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

I. Welcome, Introductions, and Administrative Matters (Reference transcript pages 1–5.)

The Chair welcomed the attendees and participants. He reported that four SLTPS-entity members—Jeff Friedland, Mike Steinmetz, Doug Reynolds, and Hans Olson—are no longer available to serve on the Committee. He encouraged all the members to submit nominations to fill these vacancies. He also reminded the SLTPS-entity members that they need to select a Vice Chair, as Jeff Friedland had been serving in that role. On the Federal side, there were changes at the CIA: Brian O'Neill, Director, Information Management Services Group, replaced Nancy Morgan as the CIA member; and Riggs Monfort, Chief, Information Review and Release Division, Information Management Services, was named as the alternate. (See Attachment 1 for a list of the attendees and participants.)

II. Old Business (Reference transcript pages 5–17.)

Updates from the DFO
Greg Pannoni, SLTPS-PAC Designated Federal Officer
Associate Director, Operations and Industrial Security, ISOO

Mr. Pannoni noted that there was one action item from the previous meeting. It related to personal security clearances being populated in the Central Verification System CVS), which is the repository where all SLTPS personnel clearances should be maintained or accessible. The action item was that Erik Galow, FBI member, was to meet with FBI security division personnel to formulate a plan to remedy the current situation in which clearance information for SLTPS personnel sponsored by the FBI is often not readily available to agency and SLTPS personnel because it is provided only to Scattered Castles and not to the CVS or JPAS. Mr. Pannoni turned to Mr. Galow for an update.

Mr. Galow read a prepared statement of behalf of the Office of the Chief Information Officer of the FBI and the FBI Security Division:

> "The FBI is awaiting further guidance before making any determinations about the future of its security clearance processes due to the recent announcements of the merger of DSS and NBIB, that being the DCSA, and the Trusted Workforce 2.0 Initiative. Those determinations include prospective planning and budgeting for technical interoperability

with systems other than Scattered Castles, and that includes CVS, which is among the issues that we addressed last year for storage of clearance related information for FBI and FBI-sponsored personnel. At this time the bureau has no plans to change its standard operating procedure regarding the continued exclusive use of Scattered Castles until otherwise directed. It is the system for all FBI personnel and sponsored personnel, in which their information is stored, and at this time we haven't budgeted for any technical interoperability with CVS."

The Chair noted that this is a critical problem for which a solution must be found. Leo Masciana, Department of State member, suggested that it would be worth looking into the feasibility of having a customer service point of contact to perform a check on behalf of the SLTPS personnel as an interim fix. Charlie Rogers, DHS Vice Chair, reminded everyone that E.O. 13549 required DHS to work with the Office of Personnel Management (OPM), the Department of Defense (DoD), and the Information Security Oversight Office to find a central database for SLTPS personnel clearances. CVS was that database. Mr. Pannoni recommended the formation of a working group to find a fix for this issue. Marc Sachs, SLTPs member, provided the private sector perspective, observing that often the individual knows he or she has a clearance but does not know the details, such as who holds it or when it expires. He suggested that these personnel would benefit from having a single point where this information can be obtained. Mr. Rogers noted that DHS has stood up a web site that is relevant to this discussion. Though it does not necessarily solve who holds someone's clearance, it has a lot of forms and does help inform people about the clearance process.

The Chair asked if there any reason why these agencies aren't entering this information in the database. Is it willful disregard of the order? Is it lack of resources? Is it not knowing the order? The Chair called for the formation of a working group on this issue, whose participants will include ISOO, the Office of the Director of National Intelligence (ODNI), DoD, and DHS. The Chair added the Department of Energy after a suggestion by Mr. Galow.

Action Item 1 (of 2): Convene a working group on the security clearance database for SLTPS personnel.

III. New Business

A. SLTPS Security Program Update (Reference transcript pages 17–22.)
Mr. Charlie Rogers, SLTPS Vice-Chair and Chief, SLTPS Management Division, DHS

Mr. Rogers provided an update on the SLTPS security program. He began with the compliance review program, reporting that by the end of the year the DHS will have performed 108 compliance reviews of SLTPS entities since they began in 2012. He noted that there are about approximately 80 recognized fusion centers, some of which are accessing classified from an FBI secure space, but the great majority are DHS certified secure rooms. The compliance reviews are conducted in these secure rooms to verify that the rooms are still secure and that personnel are following the federal and national policies for safeguarding classified information. Training and other program support are also provided during the reviews. In 2018, the DHS performed 16 compliance reviews and seven room certifications and are on-track to perform 19 reviews in 2019.

Mr. Rogers indicted that the DHS has appointed security liaisons in the fusion centers, who act as their security officers in the field. He noted that there is a fair amount of turnover and it is necessary to train these personnel. DHS is constantly working with them on the telephone and also conducts webinars with them. In 2018, they did 21 webinars and directly trained about 48 security liaison. In 2018, DHS also ran a regional training event in Nashville, Tennessee that brought in 17 security liaisons representing 10 states. This was a trial of the regional training concept, which they hope to use again depending on funding and opportunities. Mr. Rogers reported that thus far in 2019, DHS has conducted 12 webinars with 48 participants. He added that during the last week of July, the DHS Office of Intelligence and Analysis (I&A) is sponsoring a security liaison training venue for two days in Columbus, Ohio, where staff from SLTPS Security Management Division and from I&A will provide training.

Mr. Rogers's final metrics relate to the number of clearances granted to SLTPS personnel. There are approximately 2100 cleared private sector people nationwide and 6150 state and local personnel, which comes to about 8250, most of which are the collateral, Secret level. About 450 of them have TS/SCI. Some of these are state and local personnel who are working with the FBI on Joint Terrorism Task Forces and other task forces, but a good number of them are from the private sector and are involved in cybersecurity, where they must have that level of access to get the information they need.

Mr. Pannoni asked all the government members if there any other entities besides the fusion centers where a state local or tribal has been authorized the physical custody of classified information, of course only up to the secret level. Mr. Rogers responded that there are limited number; his office works with I&A to sponsor the capability. However, there isn't a great deal of storage at these locations. Mr. Galow indicated that he did not know the answer with regard to the FBI. Mr. Rogers added that the FBI has a number of locations where they invite state and locals in but that is different form giving the state and locals custody. Mr. Sachs asked if the National Guard did this. Mr. Rogers indicated that the Guard could independently do it, but he has no indication that it has been done, noting that DHS is supposed to be notified if there is storage. Mr. Pannoni asked if there were places other than the fusion centers where the state, local, and tribal community could access classified information. Members identified FBI field offices as obvious examples and also noted other locations that may have seemed less likely, such as a Secret Service secure space and an Immigration and Customs Enforcement facility.

B. Classification as an Impediment to Sharing Cyber Threat Information with Critical Infrastructure Partners, and the Case for Classification Reform (Reference transcript pages 23–39 and the presentation slides, which are attached to these minutes.)
Leo Masciana, SLTPS-PAC Member, Senior Policy Advisor, Office of Information Security, Bureau of Diplomatic Security, U.S. Department of State

Mr. Masciana began by referencing national policy that has mandated the sharing of classified information and recounting attacks on American soil that might have been prevented if the federal government did a better job of communicating and information sharing. He noted several broad shifts in the threat environment and cited polices issued in response. The shifts were first, cyber threats; second, terrorism; and third, cyberwarfare. Mr. Masciana argued that it is reasonable to ask if classification guidance and practices of U.S. government agencies help or hinder cooperation with SLTPS partners to defend the nation's critical infrastructure from cyber threats. He stated that

industry cannot defend itself against cyberattacks by nation states without U.S. Government assistance; nor can the government cannot protect the nation without private sector assistance. He observed that cyberthreat tactics, techniques and procedures are frequently classified at the Top Secret level. However, the clearances of SLTPS partners are generally limited to the Secret level. This results in a misalignment as fusion center staffers who hold Secret clearances have classified system access and a need to know, but are unable to receive or share timely cyberthreat information because it is classified Top Secret. Consequently, federal cooperation with our infrastructure partners largely takes place through sensitive but unclassified information exchanges.

Mr. Masciana highlighted four issues and concerns: fist, whether there is over-classification of cyberthreat information by applying blanket classification as a default practice without a determination that each classification decision meets the standards for classification established by Executive Order 13526; second, whether adequate oversight and accountability is in place to ensure balanced, well considered classification decisions with respect to cyberthreat information; third, whether cyberthreat classification guides exist at all, and if they do, are they consistent and contain subject matter relevance and specificity; and fourth, whether the relevant cyberthreat agencies should continue to issue individual guides or enter into a joint classification guide. Mr. Masciana recommended that the advisory committee continue work to resolve procedural gaps that hinder reciprocity access to Secret information by Secret clearance holders assigned to state and local fusion centers and that it should take a fresh look at the executive order's provisions on classification guidance. He recommended two broad initiatives to establish effective oversight in this area: first, to ensure classification training requires a risk balancing approach to classification decisions; and second, to amend Executive Order 13526 to include minimum standards and new requirements for ISOO review of classification guides. His specific recommendations were to require ISOO approval of classification guides, to require previsions in the guides for expediting dissemination and prompt releases of threat information, to seek a statutory FOIA exemption for classification for cyberthreat information, to require drafters of threat based guides to seek input from infrastructure partners, and to authorize ISOO to establish a working group to get started on these proposals.

Mr. Sachs commented that the big takeaway is the mismatch between Top Secret and Secret. Threat intelligence personnel working these cases are very comfortable creating TS/SCI, but with the timely nature of cyberspace where information can lose value in 24 hours or less, the normal downgrading process that could take weeks or months or years doesn't work in cyberspace.
Mr. Pannoni added that there may be sort of middle ground for improvement, something along the lines of what the National Geospatial Intelligence Agency did with its Consolidated Classification Guide, wherein they require enhanced statements that indicate the value and the damage.
Mr. Masciana observed that the current executive order has roots in a Cold War mindset, and change is needed. The Chair agreed and noted that a process is under way to reform E.O. 13526, led by John Fitzpatrick, former ISOO Director and SLTPS-PAC Chair, who is now at the National Security Council (NSC). He stated that we need to come up with a better way to do this, to start thinking in a new way.

Mr. Pannoni recommended the Committee collectively come up with five or ten recommendations, perhaps using Mr. Masciana's as the starting point, that are the most significant and important that could then be brought by the committee to the Chair to take to the NSC. He recommended the formation of another small ad hoc working group that would meet to reach a consensus on recommendations to hand off to the Chair. Mr. Bradley Chair agreed and directed the membership

to form such a working group. He appointed Mr. Masciana and Mr. Sachs to it and invited other members to join, noting that this is an important initiative.

Action Item 2 (of 2): Convene an ad hoc working group to develop recommendations for improvements to the classification system to better facilitate the sharing of information with SLTPS partners.

C. Collaboration for Insider Threat Programs (Reference transcript pages 40–52 and the presentation slides, which are attached to these minutes.)
Megan Davey, Branch Chief, Strategic Planning and Policy, DHS Insider Threat Program

Ms. Davey began her presentation by providing a brief history of insider threat program, starting with E.O 13587. She noted that the DHS insider threat program has full operating capacity, meaning it is monitoring user activity. She indicated that this would apply to SLTPS personnel who were in locations with DHS classified networks. The insider threat program deters, detects, identifies, and mitigates insider threats to DHS to protect the Department's mission, resources, personnel, facilities, information, equipment, networks, and systems. She emphasized that this definition goes beyond the requirements of executive order, beyond the protection of classified information, to include all DHS information, noting that this is unique to the DHS.

Ms. Davey emphasized the importance of collaboration in the implementation of the insider threat program at the DHS. She observed that the DHS is an umbrella organization that includes eight operational components and seven support components. This can present challenges when developing standards. To meet these challenges, the DHS runs an insider threat working group that encompasses all of these organizations. They have representation at the level of a senior insider threat official and an insider threat program manager in the meetings every two weeks. They provide information on what needs to be protected at the individual components, what is happening there, and how the DHS insider threat program can help them. Ms. Davey indicted that it is necessary to build a consensus across the Department by engaging and collaborating with key stakeholders across multiple lines of business including strategic, oversight, programmatic, operational, and technical capabilities. She again noted that the reach goes beyond the protection of classified information, covering seven areas to include workplace violence, espionage, terrorism, sabotage, unauthorized disclosure, investigative support, and transnational criminal organizations. They look at the big picture and what is the significant threat from the insider. They work with the components, the various stakeholders, and their subject matter experts to identify and prioritize their mission critical assets to ensure that the DHS is protecting them.

Mr. Pannoni asked if DHS were at the point where it is formalizing the requirements in contracts with external supporters. Specifically, he inquired about instances where classified information was not involved but controlled unclassified is. Chris Dzurilla, Branch Chief, Insider Threat Operations, DHS Insider Threat Program, responded, indicating that they are not at that point yet, though it does apply to contracts that involve classified information. Mr. Masciana asked three questions about the organization of the program: the office level of the program office; whether the decision process formalizes direct input from other organizational elements, and whether DHS is working directly with other agencies. Ms. Davey responded that the program is situated under the DHS Chief Security Officer, who is DHS's senior agency official for insider threat. She indicated all stakeholders in the program have input in the development of the policies that underpin the

program. To the third question, she responded yes, they do meet with other agencies to see their best practices and lessons learned. The Chair inquired as to what authority the DHS used to expand the insider threat program to cover unclassified information. Ms. Davey replied that the Secretary of Homeland Security expanded the definition in 2017. Mr. Pannoni added that it was his understanding that the program established under E.O. 13587 gives the agency head the authority of expand the program. Ms. Davey agreed and added "based on mission needs."

D. Controlled Unclassified Information (CUI) Program Update (Reference transcript pages 53–61.)
Devin Casey, Controlled Unclassified Information Staff, ISOO

Mr. Casey opened his presentation with a short description of the controlled unclassified information program and directed the audience to access the CUI website at archives.gov/CUI for additional information. He began a more detailed discussion of CUI program areas with the minimum standard for non-federal information systems, which was created and is enforced through the National Institute of Standards and Technology Special Publication 800-171 (NIST 800-171). Its purpose is to standardize how the government requires or asks nonfederal entities—state, local, tribal, as well as academia and industry—to configure their information systems to protect controlled unclassified information. Mr. Casey noted that the NIST 800-171 is already in use by the DoD, in academia, and in some states. He noted that the 800-171 was in Revision 2, which was issued in association with NIST 800-181(b). This document has additional controls that can be levied by the government to address things like high value assets for particularly sensitive types of CUI that face advanced persistent threats. He then mentioned quarterly stakeholders meetings, which are advertised on the CUI website. Also, he reported that most agencies have indicated that they will have CUI policies in place this year.

Mr. Casey then turned to another big project that the CUI office has been working on: the creation of a FAR case, which is a new federal acquisition regulation set of clauses to address and standardize the communication of cybersecurity requirements as part of the CUI program to industry as a whole. He noted that the DoD is already implementing these requirements via their DFAR 7012, which addresses a lot of the same topics the CUI FAR clause will. He advised that the FAR is likely to be out for public comment in the fall. Mr. Casey then spoke of the two sides of the CUI program: It is an information security program and it is also an information program, which ensures that individuals who have a lawful government purpose or are authorized to receive information don't have to jump through unnecessary barriers to access it.

Mr. Masciana asked if it will be up to agencies to implement the security clauses in contracts for facilities and systems they are authorizing to process CUI information. Mr. Casey responded that there will be a universal FAR clause included in all contracts that will have a self-delete if CUI is not being shared. Mr. Masciana inquired if there was an expectation that the industrial security program will incorporate this into their security clauses. Mr. Casey replied that it is very likely they will use similar language. Mr. Pannoni added that the draft of the FAR clause calls for a companion document, similar to a contract security classification specification, that identifies what CUI is required in order to fulfill this contract. Mr. Casey affirmed that this is correct, noting that there is an accompanying standard form that's going through the FAR that includes a lot of information. So, the government will have requirements to enter into these contracts as well. The form requires

the government to identify the types of information that will be shared in this contract and whether or not they have special security or handling or dissemination requirements on them.

IV. General Open Forum/Discussion (Reference transcript pages 62–79.)

Discussion during the open forum centered a number of items that Mr. Sachs raised for consideration in an e-mail prior to the meeting. The first was the need for a single point of contact in the government for SLTPS personnel to track clearances, which was discussed earlier in the meeting. The open forum discussion began with the second item—a concierge type of service for clearances at the DHS. Mr. Sachs noted that he only mentioned the DHS because it holds most of the private sector's clearances. He opined that it would be nice if there was just one place—an 800 number, an e-mail, or something with a concierge service—in the federal government where SLTPS clearance holders could go to find out the status of their clearance, a single place that could also serve as the conduit to alert them if there are changes or things ongoing. Mr. Rogers observed that the key element is that there can't be a concierge service until the database is figured out. Mr. Pannoni agreed we need to start with the database to try to have something where the consolidation of all of the clearance data for SLTPS is available in one place. He added that then there is the challenge of trying to give non-federal people access on those systems. Mr. Sachs further explained that the individual clearance holder has no place to go that says here is when your clearance expires or here is who to call to have your clearance passed. There was then some discussion about the Joint Personnel Adjudication System (JPAS) and the Central Verification System (CVS). Mr. Masciana indicated that it was his understanding that CVS and JPAS would be merged and asked if this might be the answer. Mr. Pannoni responded that that it was his understanding that JPAS is being overtaken by the Defense Information System for Security (DISS). He noted that there is a way to get JPAS data through CVS. Mr. Rogers added that he heard that the information is JPAS is based on the person's investigation, but it doesn't tell whether the individual is currently authorized to have access. Marvin Mackey, Department of Transportation, who previously worked at DoD, clarified the discussion in terms of eligibility and then access. JPAS contains the clearance adjudication and eligibility information. Access is determined at the local by their parent organization.

The discussion then turned to the third item that Mr. Sachs raised in his e-mail: the need for rapid declassification of time-sensitive cyber information, an issue raised by Mr. Masciana during his presentation earlier in the meeting when he noted that the value of most cyber alerts decrease significantly within 24 to 48 hours of the government discovering the issue, while it often takes days or weeks to declassify the information and provide a warning, by which time damage has already done. Mr. Sachs added with cyber information, if the intel is picking up on someone is trying to launch an attack against a private entity, they frequently will not call the private entity because their hands are tied or their sources and methods will not allow them to tip the private sector. He argued that's the piece we have to get in front of. There need to be awareness when creating products at the SCI level, when an analyst is creating it, thinking ahead of how to create an unclassified tearline of just the tactical, technical stuff—actionable information. Mr. Pannoni observed that it is a challenge. Pam Miles, Office of the Director of National Intelligence (ODNI) stated that it's really difficult because in order to turn that information around you have to give up sources and methods. There are various agencies and mission needs are different. They have their own classification guides; they put out their own products. She indicated that because the various mission needs and the various agencies involved, it's really hard to say okay here is a policy and

everybody has to follow it in order to get that information. Mr. Pannoni asked if there might be a middle ground. Noting there are more than 80 fusion centers throughout the country and perhaps other locations that operate at the Secret level, he asked if there were a way to break down the actionable information to that level and have SLTPS personnel to get to that fusion center to get the information. Mr. Rogers responded that there are a couple of fusion centers that have distribution lists, lists, for example, for hospitals, for ports, or whatever is the regional area of concern. He said that for cyber, the information is personalized, and someone in the federal government needs to determine who they want to give it to. There was also some discussion about a one-day read-on for briefing private sector individuals and the clause in E.O. 13526 on the release of classified information to uncleared individual in response to an imminent threat. With regard to issues of temporary eligibility, Ms. Miles noted it is expected that Security Executive Agent Directive (SEAD) 8 will be published by the end of the year.

The open forum ended with a brief discussion of the last suggestion Mr. Sachs offered in his e-mail: maintaining Secret security clearances for government employees and contractors after they depart the government or after the contract ends, so that they can easily be brought back and given access without having to go through the entire adjudication process. Mr. Pannoni noted that this is something the Trusted Workforce 2.0 is looking at.

V. Closing Remarks and Adjournment (Reference transcript page 79.)

The Chair thanked everyone for a good meeting. He reminded everyone that the next SLTPS-PAC meeting would be held on Wednesday, January 29, 2020, 10:00 a.m. to 12:00 noon, at the National Archives. The meeting was adjourned at 12:06 p.m.

Attachment 1

State, Local, Tribal, and Private Sector Policy Advisory Committee

Meeting Attendees and Teleconference Participants, July 24, 2019

Bigsby, Linda	FBI Obesrver	Attending
Bradley, Mark A.	Chair, Director, Information Security Oversight Office (ISOO)	Attending
Casey, Devon	ISOO	Attending
Connor, Kate	Department of State (State) Alternate	Attending
Davenport, Jessica	SLTPS Member	Teleconference
Davey, Megan	Department of Homeland Security (DHS)	Attending
Dunham, Sidonie	Department of Transportation (DOT)	Teleconference
Estrada, Juan	DHS	Attending
Dzurilla, Christopher	DHS	Attending
Galow, Erik	FBI Member	Attending
Good, Marcia	Office of Tribal Justice, Department of Justice	Teleconference
Kennedy, Kelbie	National Congress of American Indians	Teleconference
Mackey, Marvin	DOT Observer	Attending
Masciana, Leo	Department of State Member	Attending
Miles, Pamela	Office of the Director of National Intelligence Observer	Attending
Pannoni, Greg	Designated Federal Officer, Associate Director, ISOO	Attending
Park, Susan	FBI	Attending
Parsons, Darryl	Nuclear Regulatory Commission Alternate	Teleconference
Richards, Douglas	Central Intelligence Agency Observer	Attending
Rogers, Charles	Vice Chair, DHS	Attending
Sachs, Marcus	SLTPS Member	Attending
Skwirot, Robert	ISOO	Attending
Woolworth, Thomas E.	SLTPS Member	Teleconference
Wright, Natasha	Department of Energy Observer	Teleconference

Attachment 2

Classification as an Impediment to Sharing Cyber Threat Information with Critical Infrastructure Partners: And the Case for Classification Reform

Briefing for the

State, Local, Tribal and Private Sector

Policy Advisory Committee (SLTPS-PAC)

July 24, 2019

EO 13549 (2010) – Section 3 establishes a SLTPS *"Policy Advisory Committee to recommend changes to policies and procedures that are designed to remove undue impediments to the sharing of [classified] information under the Program."*

EO 13587 (2011), Structural Reforms to Improve Security of Classified Networks and Responsible Sharing . .. of Classified Information.

- In the interest of *"our Nation's Security"* this order seeks to *"share classified information* ***immediately*** *with authorized users around the world . . . ."*

National Security Strategy (2017) --

- "[The] *U.S. Government will work with our critical infrastructure partners to assess their information needs and to reduce barriers to information sharing,* ***such as speed and classification levels****."*

Briefing on CNSI Programs for SLTPS Entities

Overview –

December 7, 1941, **Pearl Harbor.** History attributes a failure of communications to warn the base of imminent Japanese attack until after the attack was over.

April 19, 1995**, Oklahoma City. Bombing** of the Murrah Federal Building **occurred as mutual mistrust by the FBI and ATF contributed to a critical lapse in information sharing between the agencies** – both were aware something was going to happen but neither had all of the pieces.

September 11, 2001, **Terrorist Attacks.** The devastating attacks on 9/11 are largely attributed to a failure of U.S. intelligence to "connect the dots."

All three **national tragedies** might have been prevented had we done a better job of information sharing.

Official reactions that followed the Oklahoma City bombing and the terrorist attacks on 9/11 comprise the following **three broad shifts**:

Briefing on CNSI Programs for SLTPS Entities

First shift (Cyber Threats, 1998-2018) – countering Cyber Threats (exploitation, theft, disruption) thru defense of Cyberspace with public-private partnerships

- **PDD-63 (CIAO, NIPC, FedCIRC, ISACs)**
- **EO 12333, EO 13549, EO 13587, NSS**
- **CNCI**
- **DoD: JTF-CND/CNO/GNO (1998-2010) and CYBERCOM (estab 2010; elevated 2018)**

Second shift (Terrorism, 2001-2005) – post-9/11 focused legislation and counter-terrorism directives to promote unprecedented information sharing with critical infrastructure partners.

- **USA PATRIOT ACT, HSA, IRTPA,**
- **HSPD-5, HSPD-7, EO 13388, EO 13526 ,**

Third shift (Cyber Warfare, 2008-present) – We are in a new era of nation states aggressively using the Internet as a weapons platform to launch tremendously destructive cyber attacks (Estonia; N Korea; Iran)

Briefing on CNSI Programs for SLTPS Entities

It is reasonable to ask –

Do USG agencies classification guidance and practices help or hinder cooperation with SLTPS partners to defend the nation's critical infrastructure from cyber threats?

_____

What do we think we know?

National Security Council priorities have shifted to embrace collaboration with non-USG partners to unify the nation's efforts in overcoming emerging cyber threats.

NSS 2017 emphasized the emergence of great-power competition and noted its spread into cyberspace.

2018 NCS asserted the USG will *strengthen efforts to share information with ICT providers to respond to and remediate malicious cyber activity at the network level – to include sharing classified threat and vulnerability information.*

Briefing on CNSI Programs for SLTPS Entities

What do we think we know? -- (Continued)

The private sector owns & operates about 85% of the critical physical and economic infrastructure of the U.S.

We know that industry cannot defend itself against cyber attacks by nation-states without US Government assistance. (And likewise the government cannot protect the nation without private sector assistance.)

We also know that cyber attacks are very different than traditional NS threats.

DIRNSA (Nakasone) calls them *'**corrosive threats by** malicious actors [who] weaponize personal information, steal intellectual property, and mount influence campaigns.'* **His assessment** - *'globally the scope and pace of malicious cyber activity continues to rise and the growing dependence on cyberspace for nearly every essential civilian and military function makes this an urgent and unacceptable risk to the Nation.'*

Research finding –

Based on transcripts of Senate Armed Services committee testimony and an Oct 2018 OMB memo (M-19-02) *government efforts to share classified cyber threat information with critical infrastructure partners are being hindered by the classification process*.

This is because Cyber Threat TTPs (Tactics, Techniques & Procedures) are frequently classified at the TOP SECRET level.

By comparison, SLTPS partners' access (both systems and clearances) are limited to the SECRET level. This results in a misalignment between fusion center staffers who hold SECRET clearances, have CLAN access, and a NTK, but are nevertheless unable to receive or share timely cyber threat information ***because it is classified TOP SECRET***.

Consequently, Federal cooperation with our infrastructure partners largely takes place through SBU information exchanges.

Issues and Concerns:

(1) Whether there is **over classification** of cyber threat information – Applying blanket classification as a default practice, without a determination that each classification decision meets the standards for classification, contravenes EO 13526.

(2) Whether **adequate oversight and accountability is in place** to ensure balanced, well considered classification decisions with respect to cyber threat information.

(3) Whether cyber threat **classification guides exist, are consistent**, and **contain subject matter relevance and specificity**.

(4) Whether the relevant cyber threat agencies should **continue to issue individual guides or enter into a joint classification guide**.

Briefing on CNSI Programs for SLTPS Entities

Recommendations:

That the Advisory Committee continue **resolving procedural gaps that hinder reciprocity access** to SECRET information by SECRET clearance holders assigned to State and Local fusion centers. Those efforts, however, do not improve sharing of cyber threats classified **TOP SECRET when our SLTPS** partners' clearance access are limited to SECRET level information.

Consistent with this Committee's responsibility '. . . to remove undue impediments to the sharing classified information under the Program,' the Committee **should take a fresh look at the EO's provisions** on classification guidance.

Such a review should **take a multifaceted approach** to reforming classification in the EO with the objective of improving the Federal partnership.

Recommendations (Continued)

Initiative 1: Establish effective oversight to ensure classification training requires a risk balancing approach to classification decisions.

Initiative 2: Amend EO 13526 to include minimum standards and new requirements for ISOO review of classification guides.

Specific Actions to carry out these initiatives:

(1) Require ISOO approval of class guides.

(2) Require provisions in the guides for expediting dissemination and prompt releases of threat information to U.S. entities.

(3) Seek a statutory FOIA exemption for cyber threat information.

(4) Require drafters of threat-based guides to seek input from infrastructure partners.

(5) Authorize an ISOO working group to get started on these proposals.

Conclusion:

Much has been accomplished and much remains to be done. The most important thing the government can do is to enter into a full collaborative partnership with the private sector at every level – **technology, policy, governance and operations** – in order to provide critical protection to the nation.

In countering cyber threats the critical infrastructure partnership must be a two-way effort; it must be able to anticipate and prevent, or at least minimize threats.

If collaboration is to be effective, U.S. classification **policies and practices must be sufficiently flexible and balanced to address the emerging threats of our time**.

The **NSC's evolving vision** and the strategic direction have converged on the right path forward.

Cooperation to counter serious threats to U.S. interests **must be made predictive** (rather than reactive) if we are to harden the nation's networks. This is a logical and reasonable national security objective, but it will require a much more dynamic collaboration with our critical infrastructure partners.

An important step in getting there is for ISOO to **pursue classification reform as a mission priority**.

Briefing on CNSI Programs for SLTPS Entities

July 24, 2019

by
Leo Masciana
State Department PAC Member and
Senior State Department Policy Advisor for Information Security, DS/IS
mascianalp@state.gov, 571-345-2266

Note: All statements made in connection with this briefing are solely the opinion of the presenter and are in no way endorsed by or approved as official positions of the State Department or U.S. Government.

Attachment 3

COLLABORATION FOR INSIDER THREAT PROGRAMS

Megan Davey
Department of Homeland Security
Office of the Chief Security Officer (OCSO)

July 24, 2019

Insider Threat Program History

(U) Executive Order 13587

- Issued October, 2011 and directs all federal departments and agencies with classified networks to establish insider threat programs
- Establishes the National Insider Threat Task Force (NITTF), which is responsible for the development and oversight of the Government-wide standards

(U) National Insider Threat Policy and Minimum Standards

- Developed November, 2012
- DHS reached Full Operational Capability (FOC) in classified systems for User Activity Monitoring (UAM) and is fully compliant with all mandatory insider threat training requirements.

Defining the Insider Threat Mission

- The Department of Homeland Security (DHS) Insider Threat Program (ITP) deters, detects, identifies, and mitigates insider threats to DHS and protects the Department's mission, resources, personnel, facilities, information, equipment, networks, and systems.

- DHS goes beyond the NITTF minimum standards of protecting classified information

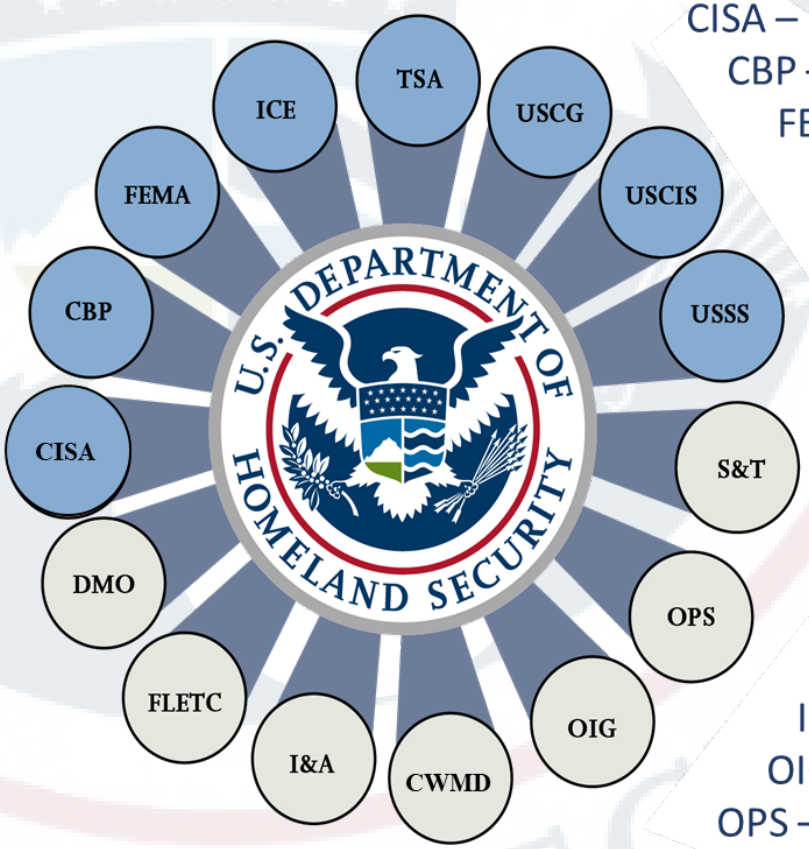
Defining the Problem

- An “Insider Threat” is a person who may use authorized access, wittingly or unwittingly, to do harm to the Department’s mission, resources, personnel, facilities, information, equipment, networks, or systems

- Insider would include any person who has or had authorized access to any DHS facilities, information, equipment, networks, or systems

- Insiders are motivated by money, ideology, compromise, ego, excitement, disgruntlement, or other reasons

Organizational Structure



Operational Components

CISA – Cybersecurity and Infrastructure Security Agency
CBP – U.S. Customs and Border Protection
FEMA – Federal Emergency Management Agency
ICE – U.S. Immigration and Customs Enforcement
TSA – Transportation Security Administration
USCG – U.S. Coast Guard
USCIS – U.S. Citizenship and Immigration Services
USSS – U.S. Secret Service

Support Components

CWMD – Countering Weapons of Mass Destruction
DMO – Departmental Management and Operations
FLETC – Federal Law Enforcement Training Centers
I&A – Office of Intelligence and Analysis
OIG – Office of Inspector General
OPS – Office of Operations Coordination
S&T – Science and Technology Directorate

Building Consensus

The Department of Homeland Security (DHS) has successfully implemented a robust Insider Threat Program (ITP) by engaging and collaborating with key stakeholders across multiple lines of business. Groups of key stakeholders can include:

Strategic – Leadership, Executives, Decision Makers

Oversight – Legal, HR, Privacy Office, Civil Rights & Civil Liberties

Programmatic – Components, Subgroups, Information Sharing

Operational – Security Partners, Internal and External Actors

Technical – CIO, CISO, IT, Engineering, Behavioral Scientists

Key Stakeholder Collaboration

Oversight

Ensures the protection of individuals rights and ensures compliance with all legal requirements.

Strategic

Ensures the program is adequately resources and has buy-in at the highest levels.

Programmatic

Ensures the program operates efficiently and consistently across the organization.

Operational

Ensures coordination for operations across all elements of the organization.

Technical

Ensures technical stakeholders have a clear understanding of requirements and are a partner in the success of the program.

Homeland Security

Defining Core Mission Areas

Workplace Violence

Espionage

Terrorism

Sabotage

Unauthorized Disclosure

Investigative Support

Transnational Criminal Organizations

Homeland Security

Identifying Critical Assets

In order to protect your organization, key stakeholders need to be engaged in order to identify critical assets that require protection.

Key Stakeholders will have the subject matter expertise in order to identify critical assets, including:

- **Personnel**
- **Facilities**
- **Information**
- **Equipment**
- **Networks**
- **Systems**

Lessons Learned

The main lessons Learned from our experience at the DHS ITP is that a successful program relies on:

COLLABORATION

COMMUNICATION & INFORMAITON SHARING

CORE MISSION AREAS

CRITICAL ASSET IDENTIFICATION