STATE, LOCAL, TRIBAL, AND PRIVATE SECTOR POLICY ADVISORY COMMITTEE (SLTPS-PAC)
January 24, 2018

SUMMARY MINUTES OF THE MEETING

The SLTPS-PAC held its fourteenth meeting on Wednesday, January 24, 2018, 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 May 31, 2018.

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

I. Welcome, Introductions, and Administrative Matters (Reference transcript pages 1–12.)

The Chair welcomed the attendees and participants. He noted that there have been some changes in SLTPS-entity membership since the last meeting. He announced that the new SLTPS Vice-Chair is Jeffery Friedland, and he welcomed new SLTPS members Thomas Woolworth, President, National, Native American Law Enforcement Association, and Mike Steinmetz, Rhode Island principal advisor for homeland security, cybersecurity, and counterterrorism. He welcomed the newest SLTPS-PAC federal member, Valerie Kerbin, Senior Security Advisor, Special Security Director, Office of the Director of National Intelligence (ODNI), National Counterintelligence, and Security Center, and Christopher Jones, Office of Data and Information Sharing, Office of the Chief Information Officer, who was attending for the Federal Bureau of Investigation (FBI).

The Chair reminded the federal members that they have a yearly responsibility to submit financial disclosure forms to the National Archives and Records Administration to ensure that federal government advisory committee members and their alternates have no actual or apparent conflict of interest with respect to service on such committees. Federal government members and alternates must send either an OGE Form 450 or OGE Form 278, whichever form is required by your home agency. (See Attachment 1 for a list of the attendees and participants.)

II. Old Business (Reference transcript pages 12–17.)

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

Mr. Pannoni reminded the attendees that there was one action item from the last meeting: a working group of federal SLTPS-PAC members would be convened to study the multiple separate and unconnected security clearance databases in the Executive branch and the effect this has on effective clearance reciprocity. This working group, containing representatives from the Performance Accountability Council (PAC) Program Management Office (PMO), the National Background Investigations Bureau (NBIB), the ODNI, the Office of the Undersecretary of Defense for Intelligence (OUSD(I)), the Department of Homeland Security (DHS), and ISOO, met on January 12, 2018, here at the National Archives. A representative from the FBI was unable to attend due to a last-minute commitment. The group discussed the various aspects of this

mechanism that would allow select SLTPS personnel access to clearance information. The group recognized that the concept of security clearance database access has been around for some time, having been included in the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, in which the President formalized the concept of a central security database. The subsequent result of that directive was to create the Central Verification System (CVS), designed to be the primary tool for verifying whether or not there is an existing investigation on a person seeking a security clearance or access, the oversight for which would be the responsibility of the Office of Personnel Management (OPM). In addition to providing a repository of security clearances, the CVS also provides information on candidate suitability, fitness, and Homeland Security Presidential Directive 12, personal verification credentialing determinations. Further, the intelligence community's sensitive compartmented information, managed through the Scattered Castles database, and the Department of Defense's Joint Personnel Adjudication System, would funnel their security clearance data into the CVS. The one exception being that, in the instance of national security concerns, some of that data could be withheld. Also, Executive Order 13549, "Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities," further established this concept. Among other principles, there are some line items that speak to both reciprocity of personnel security clearances and facility physical spaces, as well as the DHS having a role in clearance tracking. All this resulted in representatives from the various agencies that maintain security clearance database information convening and deciding to use a system that was already in place, the CVS. This led to the creation of a portal on the CVS that would enable the DoD, the FBI, and other sponsoring agencies to enter their data for SLTPS personnel into the CVS. For the most part, this system is working properly. The aforementioned action item arose from concerns of SLTPS personnel regarding their ability to maintain unobstructed access to the CVS, and primarily the inability of these entities to get access to FBI clearance data. The working group's conclusion was to ask NBIB to reach out to the FBI concerning the submission of clearance information for state and locals into the CVS. Further, the ODNI representative, as the executive agent, would also follow up with FBI, as they too have an interest in ensuring unobstructed access to similar SLTPS data. The PAC PMO representative restated the working group's primary objective that the long-term goal is to ensure the development of a single security clearance repository that can be accessed by all personnel having a clear need. The PAC PMO also reminded the group that the security executive agent directive, "Reciprocity of Background Investigations and National Security Adjudications," is nearing completion and is certain to clarify questions related to security clearance reciprocity at all levels

III. New Business

A. SLTPS Security Program Update (Reference transcript pages 17-27.)
Mr. Charlie Rogers, SLTPS Vice-Chair and Chief of the DHS's SLTPS Management Division

Mr. Rogers provided an update on the SLTPS security program. He reviewed last year's metrics for state and local security compliance reviews and updated the Committee on issues involving the security liaison training program. Mr. Pannoni asked if the DHS would, in addition to the oversight and safeguarding aspects of this program, be accountable for the sharing of information with the SLTPS community. Ms. Susan Rogers responded that her office, the DHS Office of Intelligence and Analysis, is responsible for the sharing of both classified and unclassified information with the state and local community, and noted that they have several forms of measurement, as well as a number of mechanisms through which the performance of fusion centers are annually assessed.

Finally, Mr. Rogers pointed out that the DHS Center for International Safety and Security Division, has assumed the primary task of creating a database, which will improve sharing efficiency and into which the state and local communities will be appropriately incorporated.

B. Multi-State Information Sharing & Analysis Center (MS-ISAC): Mission and Overview
Ms. Roisin Suver, Program Executive and Senior National Cyber Security and Communications Integration Center Liaison, MS-ISAC, Center for Internet Security
(Reference transcript pages 27-55.)

The Chair introduced Ms. Roisin Suver to speak about her institution's information sharing and analysis process. She began with an overview of the MS-ISAC's function, explaining that their primary mission, on behalf of DHS objectives, was to serve as a key resource for state, local, tribal, and territorial (SLTT) cybersecurity initiatives. They act as a critical touchpoint for information exchange and coordination between the SLTT community and the federal government and primarily serve as a cyber information sharing entity under a cooperative agreement with the DHS to enhance cyber-threat prevention, protection, response, and recovery. In addition, they reduce the cyber-risk throughout the SLTT/government cyber-domain by promoting cooperation and collaboration; providing direct technical assistance; expanding awareness of cyber-issues; providing opportunities for education and training on cybersecurity controls, standards, and best practices; alerting and advising on critical threats and vulnerabilities; and functioning as a centralized hub for multi-directional information-sharing between SLTT governments and the DHS. She pointed out that there are a number of ISACs that support critical infrastructure sectors, and that her institution partners with them in a group called the National Council of ISACs. However, her institution is unique, in that it serves all of the different sectors, including 50 state governments, 79 fusion centers, 43 tribal governments, and over 1,600 local governments, as well as maintaining membership in law enforcement agencies; Urban Area Security Initiatives; airports and port authorities; transit associations; public utilities; educational institutions; research, medical, and health hospitals; and local small town and municipal libraries. Further, they maintain a Homeland Security Information Network (HSIN) portal to facilitate the flow of information, and to allow them to share best practices and ask questions of each other. Thus, because of this extremely large data set, they are in a very good position to understand what the SLTT community is experiencing with respect to cyber-incidents, and they constantly monitor approximately 200 different threat actors that have been known to target SLTT entities. In addition, their Computer Emergency Response Team (CERT) provides incident response and digital forensics to their SLTT members, thus identifying sources of compromise as well as the activity of attackers and malicious actors. The net result of this activity is to provide both their membership and their federal partners with a detailed forensic analysis report. They also share their findings with the National Cybersecurity and Communications Integration Center (NCCIC), a multi-state ISAC located in Arlington, Virginia, through which they provide insight regarding the cyber domain. There are other initiatives, such as the Vulnerability Management Program, a proactive cybersecurity program wherein they assess the state of readiness of the various domain and IP software available in the communities and correlated against known, identified threats and compromises, and their Malicious Code Analysis Platform, which allows both members and SLTT community-related non-members to submit suspicious files for analysis. Ms. Suver described the MS-ISAC as a true force multiplier, in that they participate in local and national cybersecurity exercises, provide several ongoing working groups, to include education and training groups, and operate a monthly membership call wherein they provide intelligence they share with their organization. The chair asked how one would join the MS-ISAC and what challenges it faces. Ms. Suver responded that to join was a simple matter of registering at

the website and then demonstrating a SLTT-related association. As for the challenges faced by the MS-ISAC, they remain the same as always, that is, getting timely, downgraded intelligence, providing it to the fusion centers, and delivering it to their membership. All of these capabilities have matured in recent times, but the process remains complicated in that each state functions differently, each fusion center has its own unique processes, and each cybersecurity center has its own operating objectives, all of which combine to inhibit rapid, opportune information communications and sharing. Mr. Pannoni asked whether there were any checks and balances in place to ensure proper candidate vetting prior to extending membership. Ms. Suver responded that the MS-ISAC consults candidate state officials to ensure that each is accurately representing himself and completes, prior to approving membership, a domain check to ensure the absence of site vulnerabilities. Mr. Leo Masciana, Department of State, asked to what extent the U.S. CERT's incident reporting feeds into the MS-ISAC efforts, and do they provide enhanced membership access into U.S. CERT activities. Ms. Suver responded that they work closely with the U.S. CERT, as well as all entities that make up the NCCIC, and that through HSIN they make all of the U.S CERT's indicator bulletin products available to their membership. Mr. Masciana asked if Ms. Suver saw, in addition to what is already being provided within the organizations she has named, any need for an international reporting mechanism. She responded that there is already an international team that works with the different CERTs now functioning, including some MS-ISAC international working groups, but that their information is not generally provided to their membership so much as it is incorporated into their formal analysis products. The Chair thanked Ms. Suver for her most enlightening presentation.

IV. General Open Forum/Discussion (Reference transcript page 55-61.)

The Chair asked the group to provide recommendations for other presenters from organizations that are engaged in activities related to the objectives of the SLTPS. Mr. Mike Steinmetz, SLTPS member, recommended that the Committee invite Mr. Scott DePasquale, President of the Financial Systemic Analysis & Resilience Center, to speak to the committee. The Center was established by financial institutions to deepen analytic capabilities to combat cyber risk and strengthen the resiliency of the U.S. financial system. It is engaged in some very interesting projects with real-time analysis involving some of the largest U.S. banks and departments and agencies within the U.S. Government that supply highly sensitive information. Ms. Suver suggested that the Committee would benefit from hearing from some of the entities within the National Guard Bureau that have developed a number of cybersecurity, cyber-defense initiatives to help them improve state and local capabilities. Mr. Steinmetz added that the Bureau's adjutant general would perhaps be delighted to speak with the Committee. Mr. Masciana recommended that the Committee invite the National Institute of Standards and Technology's Dr. Ron Ross, whose focus areas include information security, systems security engineering, and risk management, as he is an acknowledged expert in standards and guidelines for the federal government, contractors, and the United States critical infrastructure. Finally, the Chair suggested that others on the Committee should consider bringing to our attention state, local, tribal, and/or private sector initiatives that their own agencies have underway from which we might learn.

V. Closing Remarks and Adjournment (Reference transcript pages 61–62.)

The Chair reminded everyone that the next SLTPS-PAC meeting would be held on Wednesday, July 25, 2018, 10:00 a.m. to 12:00 noon, at the National Archives. He thanked all in attendance, both in person and via teleconference, and he noted that we should keep positive thoughts for the

continuation of the important work of this committee and to contemplate the ideas we heard today and seek ways to build a strong agenda for our next meeting. The meeting was adjourned at 11:16 a.m.

Attachment 1

State, Local, Tribal, and Private Sector (SLTPS) Policy Advisory Committee (PAC)
January 24, 2018, Meeting Attendees and Teleconference Participants

Blake, Matthew	Office of the Under Secretary of Defense for Intelligence	Teleconference
Bower, Susan	Department of Homeland Security (DHS) Observer	Attending
Bradley, Mark A.	Chair, Director, Information Security Oversight Office (ISOO)	Attending
Broussard, Derrick	Defense Security Service Alternate	Teleconference
Friedland, Jeffery Alan	Vice Chair SLTPS	Teleconference
Garcia, Milagro M.	Federal Bureau of Investigation (FBI) Observer	Attending
Good, Marcia	Department of Justice Observer	Attending
Guier, Linda	DOT Observer	Teleconference
Johnson, Kim	DHS Observer	Attending
Jones, Christopher H.	FBI Member	Attending
Kerben, Valerie	Office of the Director of National Intelligence (ODNI) Member	Attending
Mackey, Marvin	DOT Observer	Attending
Masciana, Leo	Department of State Member Member	Attending
Morgan, Nancy	Central Intelligence Agency Member	Attending
Parsons, Darryl	Nuclear Regulatory Commission Alternate	Teleconference
Pannoni, Greg	Designated Federal Officer, Associate Director, ISOO	Attending
Rogers, Charles	Vice Chair Department of Homeland Security	Attending
Schouten, Mark Jay	SLTPS Member	Teleconference
Skwirot, Robert	ISOO	Attending
Smith, Brandon R.	DOT Observer	Attending
Steinmetz, Mike	SLTPS Member	Teleconference
Suver, Roisen	Multi-State Information Sharing & Analysis Center	Presenter
Taylor, Joseph R., Jr.	ISOO	Attending
Woolworth, Thomas	SLTPS Member	Teleconference
Wright, Natasha	Department of Energy Observer	Attending

Attachment 2

Multi-State Information Sharing and Analysis Center

The MS-ISAC has been designated by DHS as the key resource for cyber threat prevention, protection, response and recovery for the nation's state, local, tribal, and territorial governments

https://www.cisecurity.org/ms-isac/

TLP: WHITE

Who We Serve

Members include:

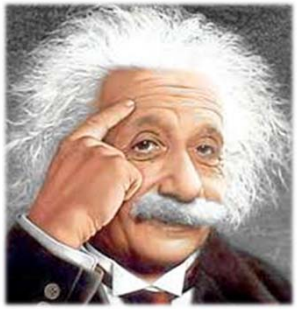
- 50 State Governments
- 79 DHS-Recognized Fusion Centers
- 6 Territorial Governments
- 43 Tribal Governments
- More than 1,600 local governments

State, Local, Tribal, and Territorial

Cities, counties, towns, airports, public education, police departments, ports, transit associations, and more

24x7 Security Operations Center

- **Support:**
  - Network Monitoring Services - Albert
  - Research and Analysis
  - Incident Response



- **Analysis:**
  - Threats & Trends
  - Vulnerabilities
  - Attacks & TTPs
  - Cyber Threat Actor Activity

- **Reporting:**
  - Cyber Alerts & Advisories
  - IP & Domain Monitoring
  - Automated Indicator Sharing
  - Strategic Intelligence

CERT

Computer Emergency Response Team

- Incident Response
- Malware Analysis
- Computer & Network Forensics
- Log Analysis

TLP: WHITE

NCCIC Liaisons

- **Conduit between the Federal Government and SLTT members**
  - Develop and maintain relationships with government and private sector organizations represented at the NCCIC
  - FBI, USSS, DHS I&A, US CERT, ICS CERT, Cyber Command, NTOC, IC, Sector ISACs, CISCP
- **Access to classified incident reporting pertaining to SLTT entities**
  - Analyze and downgrades in order to share actionable intelligence with impacted members and broader membership if appropriate
- **Correlate MS-ISAC information with NCCIC partners; create a broader understanding of the threat landscape**

Provides a trusted environment for information sharing on cyber threats between the Federal Government and SLTT

NCSR

Nationwide Cyber Security Review

A voluntary self-assessment survey designed to evaluate cybersecurity management within SLTT governments

October 2 – December 15

All states (and agencies within),
local government jurisdictions (and departments within),
tribal and territorial governments can participate.

MS-ISAC™
Multi-State Information Sharing & Analysis Center®

TLP: WHITE

VMP

Vulnerability Management Program

Notifies members on a monthly basis about any outdated software that could pose a threat to assets

Not Vulnerable

- System's patch level is current for vulnerabilities

Vulnerable

- System is not up-to-date
- Provides CVE score and links to the CVE

- **IP Monitoring**
  - IPs connecting to sinkholed C2s
  - Compromised IPs
  - Indicators of compromise from MS-ISAC network monitoring
- **Domain Monitoring**
  - Notifications on compromised user credentials, open source, and third party information

MCAP

Malicious Code Analysis Platform

A web-based service, which allows members to submit files and IOCs for analysis in a controlled and non-public fashion

Submit:

- Executables
- DLLs
- Documents
- Quarantine files
- Archives
- Domains

Analyze:

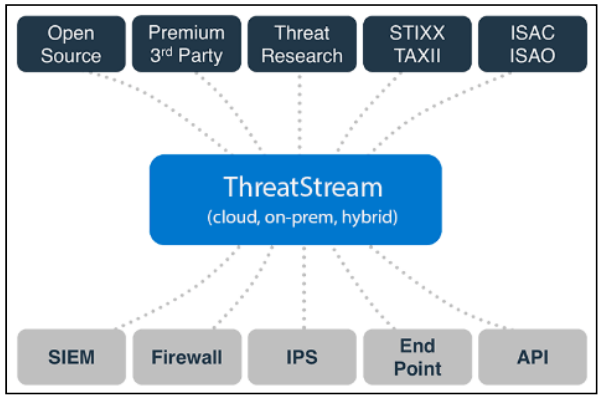
- Domains
- IP addresses
- URLs
- Hashes
- IOCs

Anomali

ANOMALI

Machine-to-Machine indicator transfer

Two free
Threatstream accounts



Benefits of MS-ISAC Membership

Free and Voluntary

No Mandated Information Sharing

Only an NDA Required

Benefits:

- Access to information, intelligence, products, resources, and webcasts
- Insider access to federal information
- Training and resource discounts
- CIS SecureSuite (NEW)
- HSIN Community of Interest (COI)
- Cybersecurity exercise participation
- Malicious Code Analysis Platform (MCAP)

https://learn.cisecurity.org/ms-isac-registration

MS-ISAC™
Multi-State Information
Sharing & Analysis Center®

MS-ISAC 24x7 Security Operations Center

1-866-787-4722

SOC@msisac.org

Roisin Suver
NCCIC Senior Liaison
703-235-8843
Roisin.s.suver@associates.hq.dhs.gov