State, Local, Tribal, and Private Sector Policy Advisory Committee (SLTPS-PAC) Meeting
Wednesday, January 26, 2022 - 10:00 a.m. - 12:00 p.m.
National Archives and Records Administration (NARA)
Information Security Oversight Office (ISOO)
The call-in information is 888-331-6674, and the participant passcode is 8510110

Agenda

Welcome, Introductions, and Administrative Matters	**10 mins**
Reports and Updates	
New York City Police Department (NYPD) Briefing	**15 mins**
Action Item Follow Up	**10 mins**
Reports and Updates	
Department of Homeland Security (DHS) Executive Agent Update	**5 mins**
Federal Bureau of Investigations (FBI) Action Item Update	**10 mins**
Executive Office of the President (EOP), Office of the National Cyber Director Briefing	**15 mins**
Controlled Unclassified Information (CUI) Update	**10 mins**
General Discussion, Remarks and Adjournment	**10 mins**

State, Local, Tribal, Public Sector Policy Advisory Committee (SLTPS-PAC) Meeting Minutes January 26, 2022

I hereby certify that, to the best of my knowledge, the foregoing minutes are accurate and complete.

Greg Pannoni signature

These minutes will be formally considered by the Council at its next meeting, and any corrections or notations will be incorporated in the minutes of that meeting.

The SLTPS-PAC held its 21st meeting on Wednesday, January 26, 2022, virtually. Mark A. Bradley, Director, Information Security Oversight Office (ISOO) served as Chair. Mr. Bradley introduced two new SLTPS members: Ms. Kate Connor replaced Mr. Leo Masciana at the State Department, while Mr. Jacob Zockert replaced Mr. Angel Catalan at the Federal Bureau of Investigation (FBI). Mr. Bradley also mentioned that SLTPS-PAC members, Thomas Carr and Marcus Sachs' membership is set to expire at the end of this year.

Ms, Meghann Teubner, New York City Police Department, provided an update on a New York City Critical Infrastructure Initiative. This initiative started in 2017 in recognition of the growing cyber threat and the need to ensure critical information sharing. New York City Cyber Critical Services and Infrastructure Group (CCSI) protects New York City's critical infrastructure and essential services by communicating critical cyber threat intelligence to all 17 sectors in New York City. The driving force of this working group is information sharing so that public and private sector critical information agencies have the information they need to protect their systems.

One of the main functions of CCSI is information sharing to ensure that all partners have access to information when they need it the most. A few years ago, CCSI conducted a cyber range kind of tabletop exercise, working through various scenarios based on actual cases of cyberattacks, bringing together the public and private sector. They worked through different scenarios aimed at bringing improvement upon certain security measures.

Recently, there was a meeting in New York City concerning a red zone attack in which participants discussed what they would be doing as a worst-case scenario unfolded and this included a potential cyberattack. She also explained that among the ways they share information is through an email or signal group distribution. There is a closed and encrypted network in which information is shared. The main concern is ensuring that the information is shared and acted upon.

Ms. Teubner wants to push this concept to other cities and municipalities. This is a blueprint for them to use. Mr. Marcus Sachs, Vice-Chair, SLTPS, mentioned the Secret Service training facility in Hoover, Alabama, and suggested that perhaps they could provide a briefing on cyber forensics for law enforcement across the country.

Office of the Director of National Intelligence (ODNI) Update

Ms. Valerie Kerben, Chief Policy, and Collaboration Group, Special Security Directorate, National Counterintelligence, and Security Center (NCSC), ODNI, provided the next update, discussing Trusted Workforce (TW) 2.0. The goal is to modernize and transform the process of investigations and adjudications. The Transforming Federal Personnel Vetting Cabinet Memorandum was signed on December 14th and disseminated to federal agencies. In addition, ODNI is requesting departments and

agencies prioritize and implement those reforms. Finally, ODNI is requesting that agencies designate senior implementation officials to ensure a successful transition during this process.

Department of Homeland Security (DHS) Update

Mr. Richard McComb, Chief Security Officer, DHS, provided an update on the SLTPS security program. There are approximately 9,600 SLTPS partners with DHS-sponsored clearances, of which eighty-eight percent have a Secret clearance and 12 percent are at the Top Secret level. The compliance and governance team performed three-room certifications of SLTPS locations and 18 security performance assessments. Forty-three percent of all the findings in these security assessments were administrative in nature and were resolved within 30 days of the final report. For FY 22, there are scheduled assessments at 17 SLTPS facilities. However, this is dependent upon the restrictions of the pandemic.

Mr. McComb, referring to Ms. Kerben's comments about TW, reminded SLTPS partners that this model changes the U.S. government vetting, from online periodic reinvestigations to a continuous vetting model.

Mr. McComb stated that DHS is piloting an automated reporting tool that allows DHS sponsored clearance holders to report through a portal which will make it easier for them and partners to monitor those changes required by Security Executive Agent Directive (SEAD) 3, Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position.

Federal Bureau of Investigation (FBI) Update

Section Chief, Jacob Zockert provided the FBI briefing. He advised that FBI coordinated with their Information Technology (IT) application and data discussion to ensure that they sent 11,669 records from the task force over to Continuous Vetting. Section Chief Mr. Zockert addressed the action item, which is the discussion of the remaining private sector clearances that the FBI holds. The FBI has identified approximately 1,245 private sector clearances that the FBI holds. The FBI will provide a more comprehensive summary at the next meeting.

Ms. Marie Bernoi, FBI, added that they will continue to work with DCSA for the CVS feed. They are examining the effort to send the remaining private sector clearances.

Controlled Unclassified Information (CUI) update

Ms. Kimberley Keravuori, Regulatory and External Policy Program Manager, National Archives and Records Administration (NARA), provided an update on CUI matters, discussing the CUI Federal Acquisition Regulation (FAR) that's being reviewed with the FAR Council, and is expected to come out for public comment at some point in the future.

Next, Ms. Keravuori addressed the revisions to the CUI registry. This registry lists all the categories of CUI and the authorities within each category that require protection. This registry is important for determining what kinds of information are covered by the category and which agencies can make use of that information as a protected category.

There is a major revision process to the registry list of categories looking at all the authorities and writing up additional information on the authorities that will include what agencies are covered by them and the scope of information covered by each authority.

The CUI team at ISOO is vetting the agencies across the Executive Branch to ensure that the authorities are summarized correctly and then putting additional information on the registry pages for each of the authorities. Furthermore, CUI is considering streamlining the categories, potentially merging some and reorganizing them in a way that will work better.

CUI is also beginning a project on addressing specified authorities. Ms. Keravuori advised that the vast bulk of CUI is protected using a standardized set of protections, CUI Basic. These items have authorities that state the information must be protected, but doesn't set out the requirements, and so they default to the CUI Basic requirements. The first part of the project is to bring new CUI Basic requirements into alignment with the new CUI framework to address areas that have limited dissemination on other filing types of requirements that are in a gray area.

She added that CUI is working heavily on information sharing agreements, including a number of state, local, tribal, and private sectors outside of contracts to share information.

Ms. Keravuori stated that the CUI requirements are not state or local requirements which will create handling issues of CUI. The solution to this problem is information-sharing agreements. Specifically, one of the issues the CUI team is working on is sharing tribal information. There is a working group of agencies that work with tribal organizations to address this issue and determine the scope of the agreements.

There are also international agreement issues. Additionally, there are broader state and local private sector partners working with CUI that also need to be addressed.

Executive Office of the President (EOP) Update

Mr. John Costello, Chief of Staff, Office of the National Cyber Director, Executive Office of the President, provided a briefing. His office is a new component in the White House that was created out of the Fiscal Year (FY) 2021 National Defense Authorization Act (NDAA). The purpose of this office is to put together all the elements of the U.S. government and the EOP into a single entity.

Mr. Costello discussed four enduring priorities and principles that his office is focused on. The first priority is federal coherence. There is a division of labor between departments and agencies, and it has become very confusing. The main goal is that everything will flow in an understandable and easily communicated way to the private sector, state and local, and to other governments.

The second goal is centered on private sector public partnerships, referring to the private sector in the U.S. government and state, local, tribal, and territorial entities. Mr. Costello said that cooperation among all of them is essential for the process to function cohesively. As a result, a shared approach has been adopted, and they share each other's agency moving forward.

The third focus is reconciling resources to aspirations. This particularly applies to accountability with a clear understanding of the risk and where that risk needs to be ultimately mitigated. Mr. Costello mentioned that his office was given Budget Review Authority, which gives them a platform to review departments and agency budgets and make recommendations that can align to strategic goals.

The fourth line of focus is present and future resilience. The level of cyber instances reflecting critical infrastructure is extremely high at the present time and steps must be taken in the interim to reduce that risk. Ultimately, there is a need to create a technology ecosystem. It is a matter of looking at the people, process, technology, and all the elements that comprise that ecosystem.

Next, Mr. Costello addressed the principle and scope of work that his office is focused on. The first item he addressed is federal cybersecurity. Chief Information Security Officer, Mr. Chris De Rusha was appointed as the deputy for federal cybersecurity. Mr. De Rusha is working with the Office of Management and Budget, as well as departments and agencies, ensuring that enterprise security rests on a solid foundation. The second principle is national cybersecurity. The concern is to ensure that the private sector, state, and local governments have all the tools they need and are aware of new and emerging incidents as well as vulnerabilities.

In addition, there is a need to look at the supply chain technology security. There is a need to review the products, software, hardware, devices, and services that make up the ecosystem and their supply chains to ensure they are safe from foreign influence and major vulnerabilities. Furthermore, cyber planning and operations is creating a unified effort across departments and agencies to ensure there is common understanding of the threat.

The fifth line of focus is workforce training and education. There is a major talent gap across all sectors, levels, and enterprises in the field of cybersecurity. The solution is to bolster the force within the federal government, increase training opportunities, expand pipelines and install training programs.

The final element is budget services and assessments. There is a need to review strategic priorities through the prism of the agency budget. At that point, strategy is developed which will translate into money.

Mr. Costello advised they are standing up a stakeholder engagement for how the private sector can assist with this initiative.

General

There was no new business to discuss.

The next SLTPS is scheduled for June 15, 2022. All SLTPS meeting announcements are posted on the federal register at https://federalregister.gov/ approximately 30 days before the meeting, along with the ISOO blog at https://isoo-overview.blogs.archives.gov.

Summary of Action Items

- The FBI was going to provide its SLTPS personnel security clearance date to the Defense Counterintelligence and Security Agency (DCSA). This would provide access to the extensive database of all SLTPS that have been granted security clearances.

  This item was discussed at a later point in the meeting.

- When COVID-19 restrictions have eased, ISOO will host a meeting in its SCIF with the ODNI, and other entities as appropriate, to examine why the Intelligence Community is unable to determine the current number of SLTPS personnel that it has cleared and to seek a means to obtain this information. Until then, the issue is tabled.

  Mr. Pannoni stated that the situation has not changed and ISOO is unable to host the meeting at the present time. Consequently, the issue remains tabled.

- The last items concerning the recommendation of putting forward the Cyber Threat Information Sharing Group.

  The DHS Vice-Chair provided DHS's formal comments on 15 recommendations. ISOO and DHS are engaged in discussing the recommendations and comments from DHS to determine a path forward and communicate them to SLTPS membership.

- Mr. Sachs suggests having a briefing on cyber forensics for law enforcement at the next meeting.

  Ms. Teubner was open to this idea and this will hopefully be discussed at the next meeting.

Attendees

Glenn Bensley, Department of Justice (DOJ)
Marie Bernoi, FBI
Mark Bradley, ISOO
Derrick Broussard, DCSA
John Castro, FBI
Larry Clark, ISOO
John Cofer, DCSA
Kate Connor, Department of State
John Costello, EOP
Sidonie Durham, Department of Transportation
Ricardo Duron, Department of Homeland Security
Juan Estrada, Department of Homeland Security
Scott Gerlach, FBI
Jeffrey Imsdahl, Deputy, SCO and Sr. Director, Systemic Monitoring Analysis and Resilience Services,
Valerie Kerben, ODNI
Kimberley Keravuori, NARA
Tracey Kindle, Department of Energy
Kevin Klein, Director, Colorado Division of Homeland Security and Emergency Management
Carolina Klink, ISOO
Richard McComb, Department of Homeland Security, Vice-Chair
Bryan O'Neal, CIA
Heather Harris Pagan, ISOO
Greg Pannoni, ISOO
Darryl Parsons, Nuclear Regulatory Commission
Michael Russo, Department of Defense
Marcus Sachs, SLTPS Vice-Chair, Pattern Computer, Inc.
Steven Stern, FBI
Natasha Sumter, Department of Energy
Meghann Teubner, New York City Police Department, New York, New York
Robert Tringali, ISOO
Eric Tysarczyk, New Jersey Office of Homeland Security and Preparedness
Debra Winsor, Washington State Fusion Center
Jacob Zockert, FBI