STATE, LOCAL, TRIBAL, AND PRIVATE SECTOR POLICY ADVISORY COMMITTEE (SLTPS-PAC)
July 26, 2017

SUMMARY MINUTES OF THE MEETING

The SLTPS-PAC held its thirteenth meeting on Wednesday, July 26, 2017, 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 September 8, 2017.

(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 1–18.)

The Chair welcomed the attendees and participants. He noted that there have been no changes in SLTPS-entity membership, but that there were federal government membership changes. He welcomed members of the State and Local Homeland Security and Law Enforcement Advisory Board, which is hosted by the Office of the Director of National Intelligence (ODNI). He reminded the Committee that the SLTPS-PAC is subject to biennial presidential renewal and noted that ISOO has strongly recommended that it continue, though in today's environment it is not clear if it is to be sustained. (See Attachment 1 for a list of the attendees and participants.)

II. Old Business (Reference transcript pages 18–21.)

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 were three action items from the last meeting:

(1) Continue to explore the issues related to fusion center and other state, local, and tribal personnel seeking to obtain JWICS access without the requirement of being detailed to a federal agency, on which SLTPS-entity Vice-Chair Tip Wight will provide a brief update;
(2) DHS to invite a guest speaker for the SLTPS-PAC meeting from Office of Intelligence and Analysis (I&A) to discuss the process to prioritize Homeland Secure Data Network deployment for their field operations, which Ms. Denise DeLawter, I&A Executive Officer for Field Operations, will cover in a briefing at this meeting; and
(3) DHS to provide an update on the implementation of the hybrid (Additional National Industrial Security Program Procedures for Sharing and Safeguarding Classified Information with Certain Private Sector or Other Non-Federal Entities), which Mr. Jim Ervin, Deputy Director of the National Security Services Division, will address at this meeting.

III. New Business

A. SLTPS Security Program Update (Reference transcript pages 21–35.)
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. He updated the Committee on issues involving the security liaison training program. He noted that the DHS continues to clear SLTPS personnel, as well as some additional private sector personnel, who work primarily with their National Protection and Programs Directorate (NPPD), and to some extent, with cybersecurity initiatives. Finally, he described DHS Office of Security realignment initiatives, which are an attempt to explore a more enterprise-oriented approach, as well as to identify redundant functions. He pointed out that the "Hybrid" program will employ a compliance piece that will ultimately be absorbed into his division, its primary purpose being to serve industrial security sector interests. Mr. Pannoni asked if there was at least one individual cleared to the Top Secret/Sensitive Compartmented Information (TS/SCI) level at each fusion center. Mr. Rogers responded that this is not always the case, as their function is mission driven.

B. Update on Implementation of the "Hybrid" (Reference transcript pages 35–46.)
James Ervin, Deputy Director, National Security Services Division, DHS

Mr. Ervin described the "Hybrid" program as a classified critical information protection process derived from the Cybersecurity Enhancement Act of 2014. The project later received additional White House requisites and is now under implementation as a joint effort between the DHS Office of Security and the NPPD. It serves as the national framework for the sharing of classified information with the private sector and companies not otherwise processed under the NISP, who are not considered government contractors. Mr. Rogers added that DHS recognizes that it will require quite some time and effort to achieve the depth of knowledge already existing in the NISP and that his Division is struggling with limited resources while trying to acquire significant expertise.

C. Overview of the DHS I&A Field Operations Division (Reference transcript pages 46–63.)
Denise A. DeLawter, Executive Officer, Field Operations Division, I&A

Ms. DeLawter provided a description of I&A's Field Operation Division, an illustration of the 12 regions incorporated in its "field footprint," and a sketch of the duties of the various classes of field operations personnel and where they are strategically located within the fusion centers and throughout the twelve divisions. (See Attachment 3.) She noted that the objective of this deployment pattern is to build relationships by enhancing I&A's information-sharing mission and focusing the efforts of private sector partnerships currently working with the DHS Intelligence Enterprise, the Intelligence Community (IC), and DHS's other partners. She characterized field personnel responsibilities as having been defined by the implementing recommendations of the 9/11 Commission Act of 2007: leading, managing, and supporting intelligence cycle execution and threat-related information-sharing, and supporting fusion center partners in developing, maintaining, and applying IC tradecraft, skills, tools, and resources necessary to effectively execute the intelligence cycle. She noted that the DHS has 77 HSDN sites providing S-level connectivity, though not all are located at the fusion centers. The Chair asked if there had been discussions regarding the criteria for deploying HSDN. Ms. DeLawter stated that it was her understanding that the deployment of the HSDNs is designated by the primary at the recognized state-owned fusion

center. Finally, the Chair asked her to comment on the kinds of finished intelligence products her analysts produce and to whom they are disseminated. She described the finished intelligence products as Federal Acquisitions Regulations, Field Analytic Reports, and Intelligence Information Reports, and noted that they are disseminated back to headquarters and, in turn, to the IC.

D. Discussion of the Report, "Review of Domestic Sharing of Counterterrorism Information," (Reference transcript pages 63–89.)

A joint report was issued in March 2017 by the Office of Inspector's General (OIG) of the Intelligence Community, the Department of Homeland Security, and the Department of Justice, on their "Review of Domestic Sharing of Counterterrorism Information." In the report, the DHS OIG recommended that DHS coordinate with the ODNI and FBI to develop and implement a strategy to efficiently and effectively provide security clearances and reciprocity to state and local personnel. This report was brought to the attention of the Chair because clearances and reciprocity touch the core of the information sharing purpose of the SLTPS program. (The full OIG report can be found at https://oig.justice.gov/reports/2017/a1721.pdf. See Attachment 3 for excerpts.) Dr. Elaine Cummins, SLTPS-PAC member, Federal Bureau of Investigation (FBI), and Mr. Rogers discussed issues related to the IG recommendation and steps that were being taken to address it.

Dr. Cummins explained that in 2008 the FBI, published an electronic communication (EC) that permitted personnel working in fusion centers, as well as in other joint spaces, to be granted unescorted access, including physical access to FBI.net desktops, as long as they possess at least a Secret (S) clearance. This was contrary to the FBI's normal clearance policy that requires a TS clearance for persons occupying FBI-managed classified space, in particular in the vicinity of the FBI's classified systems. Later that year, an agreement was signed between the FBI and the DHS that clarified the original agreement as a "reciprocal security construction standard" for DHS-sponsored state and local security areas. It is an agreement about facility standards, how to build them, and how to ensure space security. This action made it possible to achieve the aforementioned secure area policy mitigation by delineating that classified information not under control and observation of an authorized person is to be properly stored in a GSA-approved security container, that all parties would be required to use extra care in processing classified information whenever working in a non-FBI space, and that all system hard drives that store classified information would be formally secured after each day's use. Over time, and with the movement of security locations coupled with changes in security officials, these 2008 agreements became lost or obscured, and this has resulted in misunderstandings. It is important to note that neither the FBI nor the DHS and its affected parties knowingly abandoned or altered these agreements, but rather some subsequent, unfavorable rulings did occur, and the OIG team did not receive all information pertinent to their investigation. Moreover, FBI personnel in the New York region are working with DHS officials to clarify and reconstitute the 2008 agreements, and once this initiative is complete, they will work with the FBI office of partner engagement to send out a refresher and to subsequently re-publicize the original agreements so as to ensure that all officials have at their disposal all facts and requirements and can achieve full understanding and compliance.

Mr. Rogers amplified Dr. Cummins' remarks from the DHS perspective. He essentially concurred with Dr. Cummins and reported that DHS had met with FBI officials and were able to conclude that the FBI does maintain existing policy that permits access and that FBI was to reach back to its New York affiliate so as to ensure that there was a clear understanding of the context in which this problem occurred. The Chair then asked Mr. Rogers to expand on exactly what happened when the

OIG attempted to visit the New York facilities. He responded that the FBI report states that it is yet unclear what happened but that the OIG team was denied unescorted facility access, even though they had S clearances. The reason for this denial was that there was no proof that the team members had been subject to Single Scope Background Investigations (SSBI) in support of those clearances. Mr. Pannoni, clarifying that the room in question was indeed authorized to store up to S information, asked why the FBI should determine that a certified S clearance alone should not be found acceptable for access. There ensued (see the transcript, pp. 70-89) a discussion on criteria for an S clearance vs database clearance certifications, and whether or not all government entities have sufficient access to clearance information to determine the permanent certification of all security clearance personnel. It was quickly determined that the multiple separate and unconnected clearance databases in the Executive branch leads to frequent disconnects in across-the-board access to clearance information, which impose barriers to effective clearance reciprocity. ISOO agreed to convene a working group to study this issue.

- **ACTION ITEM: A working group of federal SLTPS-PAC members will 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, in order to identify steps that can be taken to address any obstacles to reciprocity that may exist because of current clearance database deployment.** (See Attachment 2.)

IV. General Open Forum/Discussion (Reference transcript pages 89–93.)

Mr. Mark Schouten, SLTPS member, noted that all appreciate the complexity of these issues at the federal level, and that the need to get them resolved, particularly with regards to cyber- and information- sharing, is fully understood for the heavy burden it represents. Nevertheless, he implored the Committee to preserve the simplicity of solutions whenever possible, so as to avoid impeding information flow.

V. Closing Remarks and Adjournment (Reference transcript pages 93–94.)

The Chair reminded everyone that the next SLTPS-PAC meeting would be held on Wednesday, January 24, 2018, 10:00 a.m. to 12:00 noon, in the National Archives, and that beyond that, the succeeding meeting would be held at the same time and place on Wednesday, July 25, 2018. 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. The meeting was adjourned at 11:48 a.m.

Attachment 1

State, Local, Tribal, and Private Sector (SLTPS) Policy Advisory Committee (PAC)
July 26, 2017, Meeting Attendees and Teleconference Participants

Bell, Maurisa Paris	Department of Justice (DOJ) Observer	Attending
Bower, Susan	Department of Homeland Security (DHS) Observer	Attending
Bradley, Mark A.	Chair, Director, Information Security Oversight Office (ISOO)	Attending
Buckley, Steve	DHS Observer	Attending
Cummins, Dr. C. Elaine	Federal Bureau of Investigation (FBI) Member	Attending
Davenport, Jessica	SLTPS Member	Teleconference
Dejausserand, Richard	DHS Observer	Attending
DeLawter, Denise A.	DHS Observer, Presenter	Attending
Ederheimer, Joshua A	DOJ Office of Tribal Justice Observer	Attending
Ervin, James	DHS Observer, Presenter	Attending
Friedland, Jeffery Alan	SLTPS Member	Teleconference
Godsey, Van	SLTPS Observer	Attending
Gunter, Chase	Observer	Attending
Hewitt, Steve	SLTPS Observer	Attending
Johnson, Kim	DHS Observer	Attending
Jones, Christopher H.	FBI Observer	Attending
Kirk, Agnes	SLTPS Member	Teleconference
Leingang, Benjamin E.	SLTPS Member	Teleconference
Lew, Kimberly	DHS Observer	Attending
Licht, Richard	SLTPS Member	Attending
Maltais, Samantha D.	DOJ Observer	Attending
Manley, Gary	Office of the Director of National Intelligence (ODNI) Observer	Teleconference
Masciana, Leo	Department of State Member	Attending
Morgan, Nancy	Central Intelligence Agency	Attending
Parsons, Darryl	Nuclear Regulatory Commission Alternate	Teleconference
Pannoni, Greg	Designated Federal Officer, Associate Director ISOO	Attending
Paterini, Robert	DOJ Observer	Teleconference
Pichardo, Milagro M.	FBI Observer	Attending

State, Local, Tribal, and Private Sector (SLTPS) Policy Advisory Committee (PAC)
July 26, 2017, Meeting Attendees and Teleconference Participants

Polk, Ken	DHS Observer	Attending
Porter, Russ	ODNI Observer	Attending
Richardson, Benjamin	Department of Defense Member	Attending
Rogers, Charles	Vice Chair Department of Homeland Security	Attending
Schouten, Mark Jay	SLTPS Member	Teleconference
Sena, Mike	SLTPS Observer	Attending
Skwirot, Robert	ISOO	Attending
Smith-Pritchard, Dr. Sam	ODNI Observer	Attending
Stone, Nichole	DHS Observer	Attending
Taylor, Joseph R., Jr.	ISOO	Attending
Webb, James Dewey	SLTPS Member	Teleconference
Wright, Lee (Tip)	Vice Chair SLTPS	Attending
Wright, Natasha	Department of Energy Observer	Attending

Attachment 2

Action Item from SLTPS-PAC Meeting, July 26, 2017

A working group of federal SLTPS-PAC members will 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 in order to identify steps that can be taken to address any obstacles to reciprocity that may exist because of current clearance database deployment.

Attachment 3

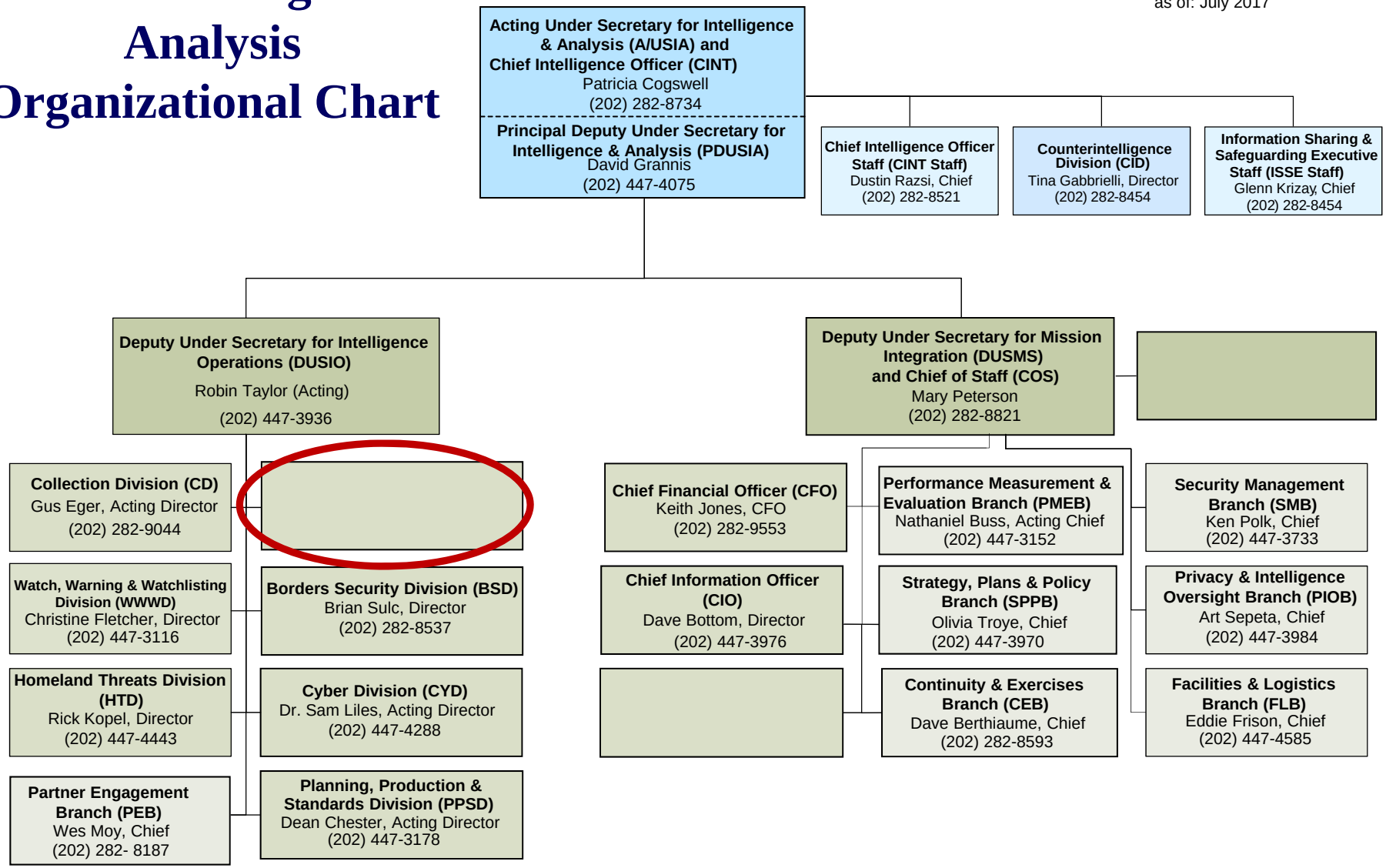
Office of Intelligence & Analysis
Intelligence Operations
Field Operations Division

Homeland Security

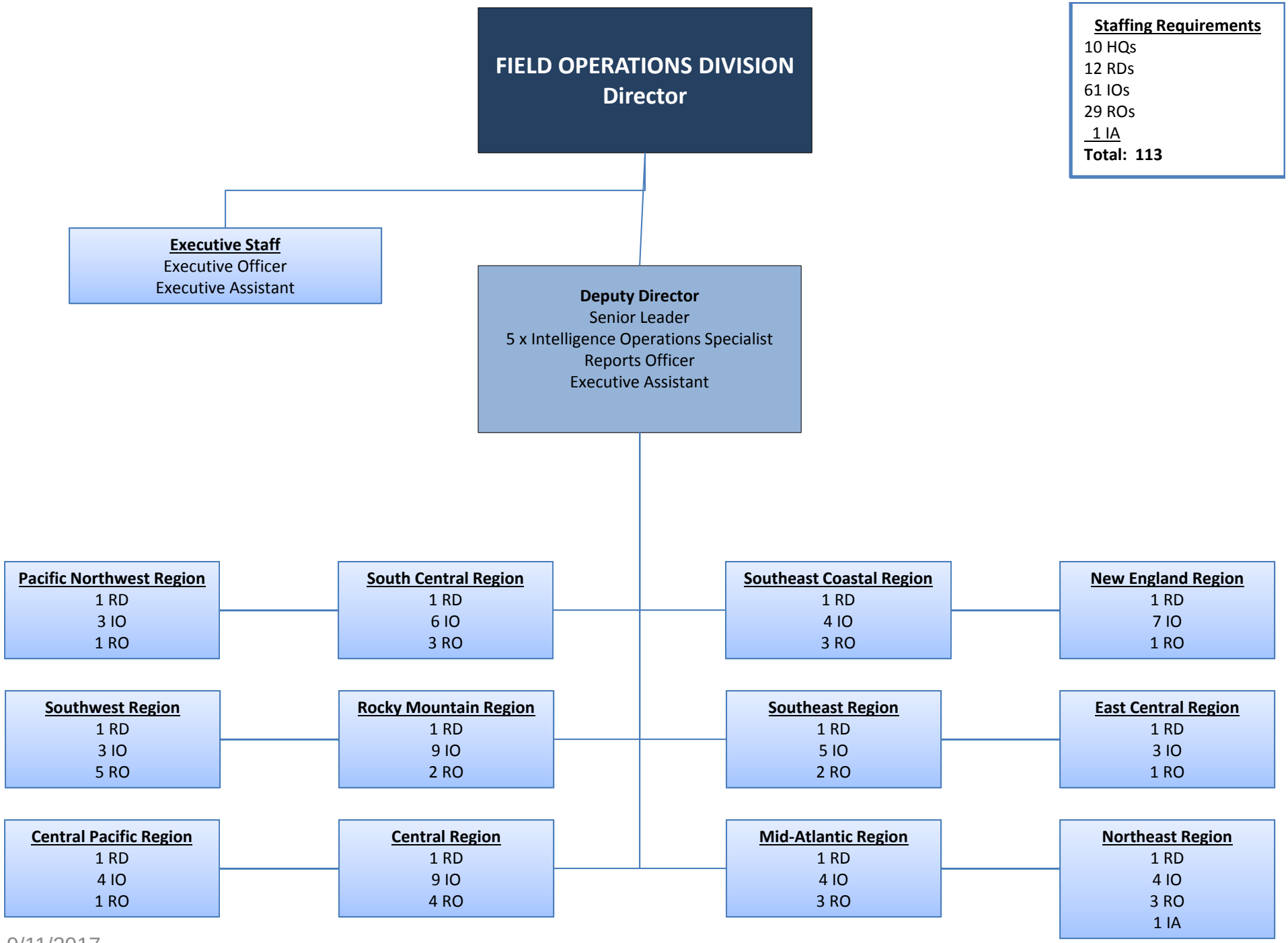
27 July 2017

Office of Intelligence & Analysis Organizational Chart

as of: July 2017



Homeland Security


FIELD OPERATIONS DIVISION
Director
Staffing Requirements
10 HQs
12 RDs
61 IOs
29 ROs
1 IA
Total: 113
Executive Staff
Executive Officer
Executive Assistant
Deputy Director
Senior Leader
5 x Intelligence Operations Specialist
Reports Officer
Executive Assistant
Pacific Northwest Region
1 RD
3 IO
1 RO
South Central Region
1 RD
6 IO
3 RO
Southeast Coastal Region
1 RD
4 IO
3 RO
New England Region
1 RD
7 IO
1 RO
Southwest Region
1 RD
3 IO
5 RO
Rocky Mountain Region
1 RD
9 IO
2 RO
Southeast Region
1 RD
5 IO
2 RO
East Central Region
1 RD
3 IO
1 RO
Central Pacific Region
1 RD
4 IO
1 RO
Central Region
1 RD
9 IO
4 RO
Mid-Atlantic Region
1 RD
4 IO
3 RO
Northeast Region
1 RD
4 IO
3 RO
1 IA

9/11/2017

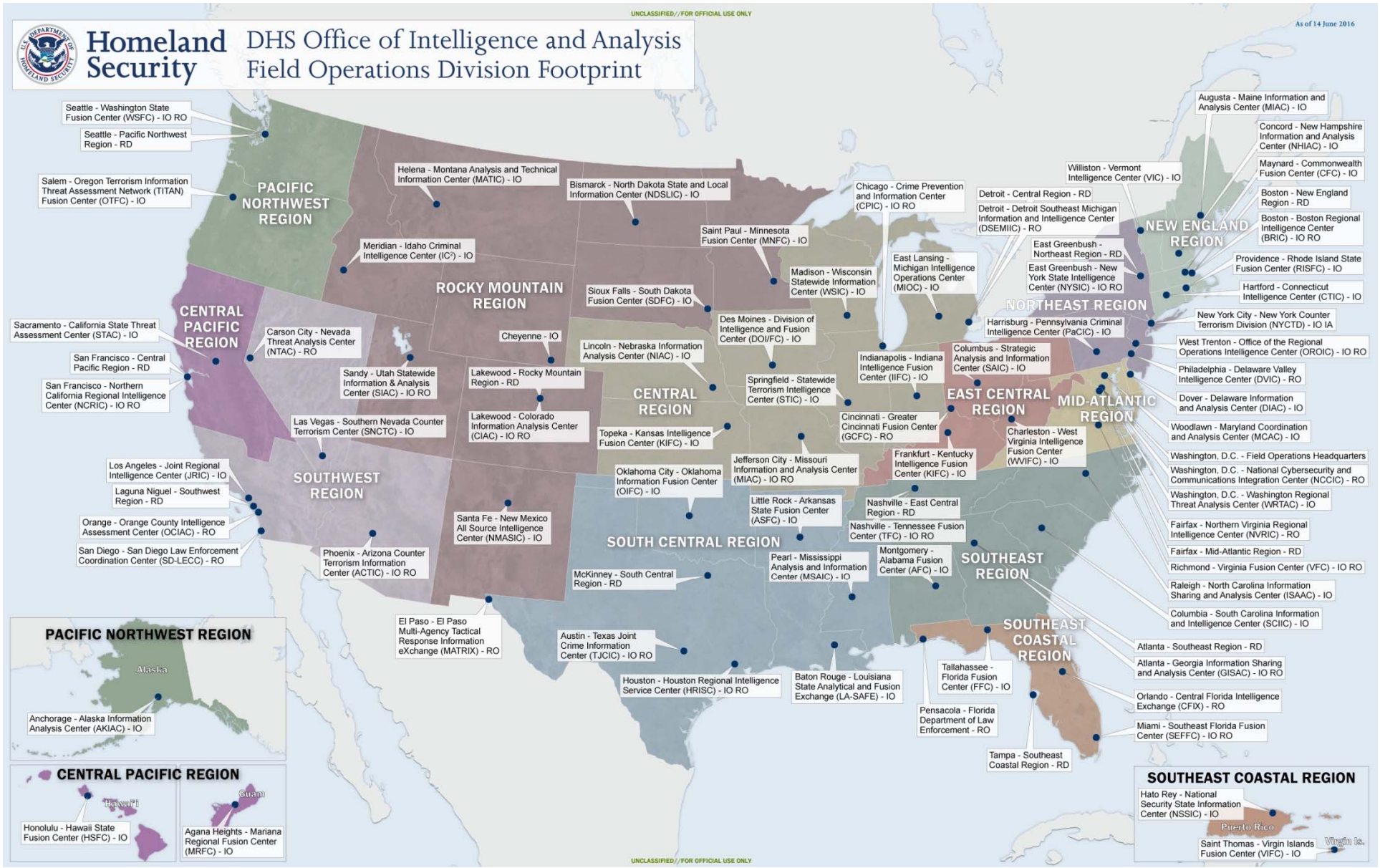
Field Ops Personnel by the Numbers

	Staffing
Regional Directors	12
Intelligence Officers	61
Reports Officers	29
Intelligence Analysts	1
HQ Leadership & Support	10
Total	**113**

Homeland Security

I&A Field Footprint

Homeland Security



Homeland Security

I&A Field Personnel Overview

- I&A deploys Intelligence Community (IC) professionals dedicated to providing relationship building and intelligence and information sharing; intelligence collection and reporting; and intelligence analysis in support of State, local, tribal, territorial, and private sector (SLTTP) partners, the DHS Intelligence Enterprise (IE), the IC, and other homeland security partners to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards.
- I&A Field Personnel are responsible for three primary functions:
  - Lead, manage, or support intelligence cycle execution in their area of responsibility (AOR) in concert with I&A, SLTTP, DHS IE, or other homeland security partners as appropriate.
  - Lead, manage, or support threat-related information sharing to and from SLTTP, DHS IE, and the IC to inform the national threat picture.
  - Support fusion center partners in developing, maintaining, and applying IC tradecraft skills, tools, and resources necessary to effectively execute the intelligence cycle.

I&A Field Personnel Responsibilities

- I&A Field Personnel perform their responsibilities as defined by the Implementing Recommendations of the 9/11 Commission Act of 2007, including:
  - Assist fusion centers and SLTTP partners in sharing and analyzing intelligence and information to develop a comprehensive threat picture.
  - Review relevant homeland security information from SLTTP partners and support the generation of intelligence products for sharing with federal partners and the IC.
  - Provide guidance for the production and dissemination of intelligence and information products to SLTTP partners, other fusion centers, and the federal government.
  - Facilitate fusion center access to training, technical assistance, and exercises.
  - Assist in the identification and reporting of threats and hazards to the homeland consistent with DHS authorities and missions.
  - Facilitate access to specialized subject-matter expertise resident within both DHS and the IC.

Fusion Center Definition

What a Fusion Center IS

- **Focused on the Fusion Process:** Fusion centers receive, analyze, disseminate, and gather threat-related information, in coordination with law enforcement and multi-disciplinary partners
- **Positioned to Provide Local Context**: Fusion centers blend intelligence and information from federal and State, local, tribal, and territorial (SLTT) partners to provide state and local context to help enhance the national threat picture
- **Flexible**: Fusion center missions vary based on the environment in which the center operates; most have adopted an "all-crimes" approach, whereas others have also included an "all-hazards" approach

What a Fusion Center is NOT

- **Focused on Terrorism:** Fusion centers have broader capabilities to assist in counterterrorism as well as all-crimes and all-hazards missions
- **Owned by the Federal Government:** Fusion centers are owned and operated by state and local entities with support from federal partners
- **A Base for Domestic Spies:** Fusion centers are committed to protecting the privacy, civil rights, and civil liberties of Americans

Homeland Security

Fusion Center Overview

- **Focal Points:** State and major urban area fusion centers (fusion centers) serve as the focal points within the SLTT environment for the receipt, analysis, gathering, and sharing of threat-related information
- **Diversity of Expertise:** Fusion center staff provide subject matter expertise, integrating specialized experience across law enforcement, intelligence, critical infrastructure and key resources (CIKR), fire, health, and emergency operations disciplines
- **Collaborative:** Fusion centers are uniquely situated to empower front-line law enforcement, public safety, emergency response, and private sector security personnel to lawfully **gather and share information** to identify emerging threats

"A fusion center is a collaborative effort of two or more agencies that provide resources, expertise and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity."

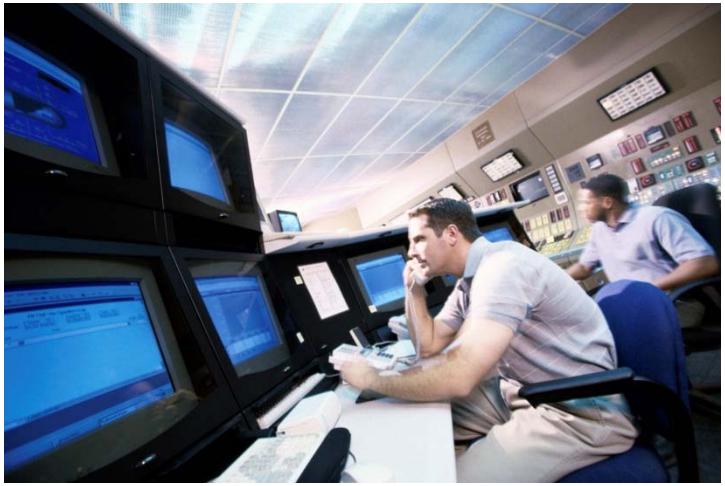
Baseline Capabilities for State and Major Urban Area Fusion Centers

Homeland Security

Resources

- Current strength is **62 *Intelligence Officers (IOs), 26 Reports Officers (SROs and ROs), 1 Intelligence Analyst, and 12 Regional Directors (RDs)***.

- To date, DHS has deployed ***77 Homeland Secure Data Network (HSDN) sites*** to provide SECRET connectivity, though not all of them are located within fusion centers.



Homeland Security

Regional Directors

- Serve as the DHS manager for all I&A Field personnel in their respective region, and the DHS representative to the DomDNI.
- Supervise national-level intelligence support provided to regional SLTTP partners and other federal agencies.
- Facilitate the identification and prevention of threats within the scope of DHS's authority and supervise the implementation of the intelligence cycle.
- Supervise and engage in the information sharing with SLTTP officials, federal entities, and other DHS field offices.

Intelligence Officers

- Provide national and local-level intelligence and information sharing support, as well as guide the management and implementation of the intelligence cycle among SLTTP and fusion center partners.
- Support SLTTP efforts to develop, implement, and execute the intelligence cycle:
  - **Collection:** Support intelligence collection efforts in the Field with SLTT partners, including writing/releasing raw intelligence such as Intelligence Information Reports (IIRs) and Field Intelligence Reports (FIRs).
  - **Analysis:** Lead analytical production among federal and SLTT partners, including joint seal intelligence assessments and Field Analysis Reports.
  - **Engagement:** Promote engagement with federal and SLTTP partners in their assigned AORs, in order to support the coordination of DHS IE intelligence-related efforts.

Homeland Security

Reports Officers

- Identify federal and SLTTP information that meets DHS and IC collection requirements and priorities, and has homeland security significance.
- Develop collection and reporting contacts, identify information gaps, and produce IIRs and FIRs.
- Support the RD in the development of regional collection plans and priorities; collaborate with regional personnel on collection emphases and emergent requirements.
- Focus planning, collection, and reporting efforts on Homeland Security Standing Information Needs (HSEC SINs), DHS Chief Intelligence Officer (CINT) priorities, and validated IC requirements in a manner consistent with DHS and IC standards.
- Review and evaluate regional IIR submissions to ensure they comply with DHS/IC reporting requirements/standards and comply with Intelligence Oversight and Privacy requirements.

Homeland Security

Intelligence Analysts

- Support the RD in the development of regional analytic plans.
- Provide analytical subject matter expertise to the region.
- Research and collaborate with regional intelligence personnel and SLTTP partners in obtaining unique DHS and SLTTP data for analytic production.
- Lead analytic production, including the publication of joint seal intelligence assessments and Field Analysis Reports.

Homeland Security

Questions?

Homeland Security

Homeland Security

Attachment 4

Review of Domestic Sharing of Counterterrorism Information

Prepared by the Inspectors General of the:

INTELLIGENCE COMMUNITY
DEPARTMENT OF HOMELAND SECURITY
DEPARTMENT OF JUSTICE

MARCH 2017

OIG-17-49

At the Fundamental Stage, fusion centers across the National Network have approved plans, policies, or standard operating procedures for each of the four COCs and EC 1 (Privacy, Civil Rights, and Civil Liberties Protections). At the Emerging Stage, the National Network has the systems, mechanisms, and processes needed to implement the plans, policies, or standard operating procedures and the COCs and ECs as a whole. At the Enhanced Stage, the National Network has the operational capability to produce products and provide services to federal, state, and local customers. Finally, at the Mature Stage, the National Network has the full capability to leverage the collective resources among individual fusion centers and adjust to both the changing threat environment and evolving requirements. Based on this model, the National Network is currently halfway through the stages to achieve maturity. However, the majority of state and local officials DHS OIG interviewed said given the unpredictability of resources allocated, fusion centers are focused on sustaining rather than enhancing operations and capabilities.[47]

Need to Coordinate Granting of Security Clearances

Access to classified information, systems, and facilities is vital for the domestic sharing of counterterrorism information. State and local analysts at fusion centers require security clearances to receive classified information, and these clearances may be granted by multiple federal agencies, including DHS and the FBI. By Executive Order, all clearances granted to state and local personnel by one agency are to be accepted reciprocally by other agencies.[48] However, DHS' and the FBI's various and sometimes differing requirements for obtaining clearances and accessing classified information can complicate this reciprocity. Without full coordination, these various requirements may lead to duplication of effort in conducting background investigations or gaps in information sharing due to the inability to access classified areas and attend meetings. Currently, there are no formal agreements among the federal partners on state and local security clearance reciprocity; such agreements might mitigate the effects of varying requirements and improve information sharing.

For example, DHS OIG and DOJ OIG identified one instance at the New York State Intelligence Center (where some fusion center analysts are co-

47 Fusion centers categorize expenditures in five major areas: staff; information systems and technology; management and administration; training, technical assistance and exercise; and programmatic. In recent years, the greatest expenditure has been staff, an average of about 83 percent of total fusion center expenditures.

48 Executive Order 13549 of August 18, 2010, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities.

located with FBI personnel and systems) in which state and local representatives had difficulty accessing the FBI's "open storage areas." Specifically, in January 2015, the FBI revised its security policy to require Single Scope Background Investigations (SSBI) and Top Secret clearances for individuals to have unescorted access to the FBI's open storage areas. As a result, fusion center personnel with Secret clearances granted by DHS had to be escorted into the FBI areas. After reviewing the situation, to meet information sharing and MOU requirements, the FBI agreed to waive the SSBI requirement for the New York State Intelligence Center.

Recommendation: DHS OIG recommends that DHS:

23. Coordinate with the ODNI and FBI to develop and implement a strategy to efficiently and effectively provide security clearances and reciprocity to state and local personnel.

National Mission Cell Initiative

The National Mission Cell (NMC) concept was designed to help fusion centers fulfill their mission to support counterterrorism threat analysis and information sharing by standardizing and formalizing the processes for information collection, production, and dissemination. Personnel from the National Fusion Center Association, PM-ISE, DHS, and the FBI devised an NMC pilot program for four fusion centers, which ran from January 2014 through July 2015. NMCs were intended to be small standardized cells of intelligence analysts within a fusion center, consisting of a limited number of existing personnel from DHS, the FBI, and state and local partners. The entities involved in conceptualizing the NMC believed the concept would advance federal counterterrorism efforts; enhance information sharing; advance fusion centers' intelligence capabilities and accelerate their maturity; and increase integration, interaction, coordination, and intelligence sharing within the fusion centers and with other partners.

According to the FBI, it had witnessed significant maturation of the National Network of Fusion Centers with increased coordination, cooperation, and information sharing between FBI field offices and the fusion centers. At the same time, the threat from ISIL-inspired individuals and homegrown violent extremists had increased significantly. To address the threat, the FBI plans to enhance FBI field office engagement with fusion centers. I&A intends to remain fully engaged with and continue support to fusion centers. A new pilot phase will be conducted in six fusion centers, and the partner agencies will leverage their respective authorities and existing resources.

control related data. The use of this tool is a requirement for all field personnel and has greatly increased I&A's ability to ensure accountability, efficiently process IIRs, identify problematic process segments, and improve upon identified inefficiencies within I&A. I&A has also developed and implemented an internal SharePoint-based system for drafting, reviewing, approving, logging and tracking finished intelligence products. I&A and the clearing offices will explore expanding the scope of this system and using it as the foundation of an all-encompassing tool.

DHS clearance offices take any undue delay in production seriously, but believe that the review of intelligence products is done in a timely manner as indicated by the data provided to the OIG showing review and approval time of less than one business day. For example, the Office of Privacy and CRCL's data shows they review and approve intelligence products intended for dissemination outside the federal government within an average time of 2-5 hours. ECD: September 30, 2017.

The DHS OIG recommended that DHS:

Recommendation 9: Develop and implement a plan that will allow DHS intelligence officials in the field practical access to classified systems and infrastructure above the Secret level.

Response: Concur. I&A's Security Management Branch has created a consolidated list of all DHS Sensitive Compartmented Information Facilities (SCIFs) that are available to DHS Field personnel. Additionally, all National Guard facilities with an available SCIF are being added to the consolidated list which will be disseminated to I&A field personnel no later than March 31, 2017. I&A continues to work on the development of an interactive map overlay that can be uploaded to the I&A Web-site to allow for real time updates. ECD: October 31, 2017.

Additionally, once changes within the DHS Office of the Chief Security Officer (OCSO) have been completed, I&A; in coordination with the OCSO, Special Security Officer's Council and DHS components, will develop and implement standard procedures to ensure DHS Intelligence Enterprise personnel access to DHS Accredited SCIFs and IT Systems up to and including Top Secret/SCI both during and after normal working hours. In the interim, a POC is being provided for each SCIF location so individuals requiring access can reach out directly to the SCIF POC for assistance, when needed. ECD: October 31, 2017.

Recommendation 23: Coordinate with the ODNI and FBI to develop and implement a strategy to efficiently and effectively provide security clearances and reciprocity to state and local personnel.

Response: Concur. The OCSO will coordinate with the FBI and ODNI, which is the designated Security Executive Agent under Executive Order (E.O.) 13467, "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees and Eligibility for Access to Classified National Security Information," dated June 30, 2008, concerning this recommendation.

Rationale: Within E.O. 13467, among the authorities granted to ODNI as the Security Executive Agent in Sec. 2.3, (c) (vi) it states:

> "Shall ensure reciprocal recognition of eligibility for access to classified information among the agencies, including acting as the final authority to arbitrate and resolve disputes among the agencies involving the reciprocity of investigations and determinations of eligibility for access to classified information or eligibility to hold a sensitive position."

ECD: September 30, 2017.