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

Department of Justice
Office of the Inspector General
Audit Division Report 17-21

REVIEW OF DOMESTIC SHARING OF COUNTERTERRORISM INFORMATION

TABLE OF CONTENTS

REVIEW OF DOMESTIC SHARING OF COUNTERTERRORISM INFORMATION

EXECUTIVE SUMMARY

Fifteen years after the September 11, 2001, terrorist attacks on the United States, the terrorist threat remains in the United States and abroad, as evidenced by recent attacks in Paris, France; San Bernardino, California; Brussels, Belgium; Orlando, Florida; and Nice, France. The U.S.'s national security depends on the ability to share the right information with the right people at the right time. This requires sustained and responsible collaboration among federal, state, local, and tribal entities, as well as the private sector and international partners.

In response to a request from the Senate Select Committee on Intelligence, the Senate Homeland Security and Governmental Affairs Committee, and the Senate Judiciary Committee, the Offices of Inspector General (OIG) of the Intelligence Community (IC), Department of Homeland Security (DHS), and the Department of Justice (DOJ) conducted a review of the domestic sharing of counterterrorism information.

The OIGs concluded that the partners in the terrorism-related Information Sharing Environment – components of the Office of the Director of National Intelligence (ODNI), DHS, DOJ, and their state and local partners – are committed to sharing counterterrorism information. The partners' commitment to protecting the nation is illustrated by the actions taken before, during, and following terrorism-related incidents, as well as by programs and initiatives designed to improve sharing of counterterrorism information. However, the OIGs also identified several areas in which improvements could enhance information sharing.

To share information effectively, the federal, state, and local entities actively involved in counterterrorism efforts must understand each other's roles, responsibilities, and contributions, especially with the involvement of multiple agencies, such as the DOJ's Federal Bureau of Investigation (FBI) and DHS' U.S. Immigration and Customs Enforcement (ICE), in complex investigations. Updating or establishing new information sharing agreements among such entities should enhance coordination and collaboration, and reaffirm and formalize the roles and responsibilities of partners in the current information sharing environment. Similarly, although there is a national information sharing strategy, its implementation has been viewed to be uneven. The OIGs believe that the ODNI, DHS, and DOJ should review the interagency information sharing memorandum of understanding (MOU) and take necessary actions to update intelligence information sharing standards and processes among the departments, which we believe would result in better implementation of the strategy.

The OIGs also identified improvements in various practices and processes of the partners involved in counterterrorism. At DHS, a lack of unity in its Intelligence Enterprise, issues in the field related to staffing and access to classified systems and facilities, as well as problems with intelligence reporting processes, have made the DHS Intelligence Enterprise less effective and valuable to the IC than it could be. DOJ can improve its counterterrorism information sharing efforts by developing and implementing a consolidated internal DOJ strategy, and evaluating the continued need and most effective utilization for the United States Attorney's Offices' Anti-Terrorism Advisory Council (ATAC) meetings. Further, the FBI should spur participation associated with Joint Terrorism Task Forces (JTTF) and improve its efforts to obtain partners' input in the process of identifying and prioritizing counterterrorism threats. Within the ODNI, the Domestic DNI Representative program is hindered by large geographic regions, as well as the lack of a clear strategic vision and guidance. In addition, the National Counterterrorism Center (NCTC) Domestic Representative program, although well received in the field, has also struggled to sufficiently cover its regions. At the state and local level, due to unpredictable federal support, fusion centers are focused on sustaining operations rather than enhancing capabilities. Further, varying requirements for state and local security clearances sponsored by federal agencies can impede access to classified systems and facilities.

Our review resulted in 23 recommendations to help improve the sharing of counterterrorism information and ultimately, enhance the Nation's ability to prevent terrorist attacks. We discuss our findings in detail in the Findings and Recommendations section of the report.

INTRODUCTION

The Senate Select Committee on Intelligence, the Senate Homeland Security and Governmental Affairs Committee, and the Senate Judiciary Committee requested that the Inspectors General (IG) of the Intelligence Community (IC), Department of Homeland Security (DHS), and Department of Justice (DOJ) conduct a performance audit of federally supported entities engaged in field-based domestic counterterrorism, homeland security, intelligence, and information-sharing activities in conjunction with state and local law enforcement agencies. The oversight committees requested that the joint audit examine these entities' overall missions, specific functions, capabilities, funding, personnel costs to include full-time employees and contractors, and facility costs.

In response to this request, the Offices of the Inspector General (OIG) of the IC, DHS, and DOJ conducted a coordinated, joint review focusing on domestic sharing of counterterrorism information. The objectives of this review were to: (1) identify and examine the federally supported field-based intelligence entities engaged in counterterrorism information sharing to determine the overall missions, specific functions, capabilities, funding, and personnel and facility costs; (2) determine if counterterrorism information is being adequately and appropriately shared with all participating agencies; and (3) identify any gaps or duplication of effort among these entities.

The review was conducted by three teams from the OIGs of the IC, DHS, and DOJ. The OIGs interviewed more than 450 individuals, including senior Office of the Director of National Intelligence (ODNI), DHS, DOJ, and state and local officials. In addition, the OIGs reviewed policies, procedures, and other relevant documentation, as well as prior studies. While the OIG teams shared relevant documents, attended briefings, and participated jointly in interviews of officials and subject matter experts, each OIG team was responsible for evaluating the actions of, and information available to, its respective agencies.

Background

Post 9/11 investigations proposed sweeping change in the IC, resulting in congressional passage of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA).[1] As a result of the IRTPA, the ODNI was officially established to lead and integrate the 16 members of the Intelligence Community, and the IRTPA codified the establishment of the National

1 Intelligence Reform and Terrorism Prevention Act of 2004, PL 108–458, December 17, 2004, 118 Stat 3638.

Counterterrorism Center (NCTC) as part of the ODNI.[2] The IRTPA also directed the establishment of an Information Sharing Environment (ISE) for the sharing of terrorism information.[3] In addition, the IRTPA required the President to "designate an individual as the Program Manager (PM) for information sharing across the Federal Government," as well as an interagency Information Sharing Council (ISC) to advise the President and PM.[4]

EO 13388, Further Strengthening Terrorism-related Information Sharing, established the policy framework for the terrorism-related ISE. In particular, ISE Presidential Guideline 2 – Sharing Among and Between Federal, State, Local, Tribal, and Private Sector Entities and its Report expanded the scope of the terrorism-related ISE to crimes of national security concern and involved a step forward from initial interagency information sharing established earlier.

Under the statute, both the PM-ISE and ISC would expire after 2 years. In August 2007, the *Implementing Recommendations of the 9/11 Commission Act* permanently established the PM-ISE and ISC. The PM-ISE is responsible for facilitating the sharing of terrorism information among all appropriate federal, state, local, and tribal entities, as well as the private sector, through the use of policy guidelines and technologies. The office of the PM-ISE facilitates the development of responsible information sharing by bringing together mission partners and aligning business processes, standards and architecture, security and access controls, privacy protections, and best practices. The IRTPA mandated the PM-ISE to annually report to Congress on the ISE's progress, status of efforts, and targeted next steps.

In October 2007, the White House issued a national strategy for terrorism-related information sharing (2007 NSIS), which provided the Administration's vision for the information sharing environment.[5] In 2009, the White House established the Information Sharing and Access Interagency

---

2 IRTPA supra note 2 at § 1021, codified at 50 U.S.C. § 3056(a). President Bush initially established the NCTC by Executive Order 13354, on August 27, 2004. In July 2008, Executive Order 13354 was rescinded by Executive Order 13470 because the IRTPA codified the establishment of the NCTC.

3 ISE broadly refers to the people, projects, systems, and agencies that enable responsible information sharing for national security. This includes many different communities: law enforcement, public safety, homeland security, intelligence, defense, and foreign affairs. The people in these communities may work for federal, state, local, tribal, or territorial governments.

4 IRTPA § 1016 (f)(1), codified at 6 U.S.C. § 485(f); established the responsibilities for the ISE PM. IRTPA § 1016(g)(1); codified at 6 U.S.C. § 485(g)(1) established the responsibilities for the ISC.

5 National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing (October 2007).

Policy Committee (ISA IPC).[6] The ISA IPC is co-chaired by the National Security Staff's Senior Director for Information Sharing Policy and the PM-ISE.[7] The ISA IPC's mission is to implement the national information sharing strategy and to lead information sharing policy on national security issues across the federal government.[8] The President issued an updated national strategy in December 2012 (2012 Strategy).[9] The 2012 Strategy outlined 5 goals and 16 priority objectives for the national security information sharing environment.

Field-Based Counterterrorism Information Sharing

Various components of the ODNI, DHS, DOJ, and state and local law enforcement are among the ISE partners that contribute to the nation's field-based homeland security and counterterrorism missions and information sharing. Within the ODNI, the NCTC serves as the federal government's primary organization for analyzing and integrating all intelligence possessed or acquired pertaining to terrorism or counterterrorism (except intelligence pertaining exclusively to domestic terrorists and domestic counterterrorism). In addition, the NCTC ensures that agencies have access to and receive intelligence support needed to execute their counterterrorism plans to perform independent, alternative analysis and serves as the "central and shared knowledge bank on known and suspected terrorists and international terror groups, as well as their goals, strategies, capabilities, and networks of contacts and support."[10] The NCTC is staffed by personnel from multiple departments and agencies from across the IC, including the CIA, FBI, DHS, Department of State, Department of Defense, and other federal entities. In addition to the NCTC, the following ODNI programs and entities are involved in domestic field-based sharing of counterterrorism information.

---

6 The Executive Office of the President, establishes Interagency Policy Committees (IPC) on a variety of issues. These IPCs are the primary day-to-day forums for interagency coordination on particular issues. They provide policy analysis for consideration by senior committees and staff and ensure timely responses to decisions made by the President. The ISA IPC subsumed the role of a predecessor body, the Information Sharing Council, which was established by Executive Order 13356: Strengthening the Sharing of Terrorism Information to Protect Americans in 2004.

7 The ISA IPC consists of representatives from the ODNI; Joint Chiefs of Staff; Office of Management and Budget; Office of the Secretary of Defense; Central Intelligence Agency (CIA); National Security Agency; Federal Bureau of Investigation (FBI); and the Departments of Agriculture, Commerce, Energy, Health and Human Services, Homeland Security, Interior, Justice, State, Transportation, and Treasury.

8 In a July 2009 memorandum, the Assistant to the President for Homeland Security and Counterterrorism made clear that the Administration regarded information sharing as extending beyond terrorism-related issues to encompass the sharing of information more broadly to enhance the national security of the United States and the safety of the American people.

9 National Strategy for Information Sharing and Safeguarding (December 2012).

10 IRTPA of 2004, § 1021(d); codified at 50 U.S.C. § 3056(d).

Table 1: ODNI Programs and Entities Engaged in Field-Based Counterterrorism Information Sharing

Entity	Mission
Domestic Director of National Intelligence Representative Program	Represent the DNI within the U.S. to senior field representatives of each IC element and lead the IC effort to create a single IC enterprise that is coordinated, integrated, agile, and effective.
NCTC Domestic Representative Program	Provide tailored counterterrorism-related information and serve as the liaison for the NCTC Director with IC agencies and counterterrorism officials at the federal, state, and local levels.
Program Manager-Information Sharing Environment	Provide and facilitate the means for sharing terrorism information among all appropriate federal, state, local, and tribal entities, as well as the private sector through the use of policy guidelines and technologies.

Source: NCTC, ODNI Partner Engagement, and PM-ISE documentation

The *Homeland Security Act of 2002*, as amended, created DHS and established its primary mission to prevent terrorist attacks in the United States and enhance security. While not all DHS components have specific programs or groups dedicated to domestic field-based counterterrorism information sharing, they contribute to this mission through their areas of expertise and authorities.

The Office of Intelligence and Analysis (I&A) is one of DHS' two IC elements and is obligated and authorized to access, receive, and analyze law enforcement information, intelligence information, and other information from federal, state, and local government agencies and private sector entities, and to disseminate such information to those partners.[11] I&A's Field Operations consists of intelligence officers, reports officers, and regional directors deployed nationwide to manage DHS' role in information sharing with state and local entities. The U.S. Coast Guard is the other DHS element of the IC and has the authority to "collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence including defense and defense-related information and intelligence to support national and departmental missions" and to "conduct counterintelligence activities."[12] Other DHS components, such as the Transportation Security Administration (TSA) and U.S. Citizenship and Immigration Services (USCIS), also have intelligence programs though they are not IC elements. These programs, in addition to I&A and the U.S. Coast Guard, compose the DHS Intelligence Enterprise.

DHS components, such as U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), and Federal Protective Service (FPS), deploy representatives nationwide to leverage their law

11 6 U.S.C. § 121.

12 Executive Order No. 12333 at § 1.7(h).

enforcement authorities in counterterrorism investigations with federal, state, and local partners. For example, CBP personnel at land, air, and sea ports of entry have the authority to search people and their belongings entering the United States and collect personal information for all travelers entering or leaving the United States. ICE Homeland Security Investigations (HSI) agents across the country enforce more than 400 federal statutes focused on the illegal movement of people, goods, and currency. Table 2 lists the DHS components engaged in this review and their respective missions.

Table 2: DHS Entities Engaged in Field-Based Counterterrorism Information Sharing

Entity	Mission
I&A	Equip the Homeland Security Enterprise with the intelligence and information it needs to keep the homeland safe, secure, and resilient.
U.S. Coast Guard	Ensure the safety, security, and stewardship of the Nation's waters.
CBP	Safeguard America's borders thereby protecting the public from dangerous people and materials while enhancing the Nation's global economic competitiveness by enabling legitimate trade and travel.
Federal Emergency Management Agency	Build, sustain, and improve the Nation's capability to prepare for, protect against, respond to, recover from, and mitigate all hazards.
FPS	Prevent, protect, respond to, and recover from acts of terrorism and other hazards threatening the U.S. Government's critical infrastructure and essential services.
ICE	Promote homeland security and public safety through the criminal and civil enforcement of federal laws governing border control, customs, trade, and immigration.
National Protection and Programs Directorate	Lead the national effort to protect critical infrastructure from all hazards by managing risk and enhancing resilience through collaboration with the critical infrastructure community.
U.S. Secret Service	Protect the Nation's leaders and the financial and critical infrastructure of the United States.
TSA	Protect the nation's transportation systems to ensure freedom of movement for people and commerce.
USCIS	Determine eligibility for immigration and citizenship benefits, promote an awareness and understanding of citizenship, and ensure the integrity of the U.S. immigration system.

Source: DHS OIG compilation of DHS information

Within DOJ, there are two components that are primarily involved in the field-based sharing of counterterrorism information – the FBI and the U.S. Attorney's Offices (USAO). By law, the FBI is the lead agency within the federal government responsible for investigating crimes involving terrorist activity within the statutory jurisdiction of the United States.[13] Each U.S. Attorney is

13 18 USC 2332b(f).

the chief federal law enforcement officer within his or her particular jurisdiction. The following table shows the missions of specific entities within the FBI and USAOs that are predominantly involved in the field-based sharing of counterterrorism information.

Table 3: DOJ Entities Engaged in Field-Based Counterterrorism Information Sharing

Entity	Mission
FBI – Joint Terrorism Task Forces	Leverage the collective resources of federal, state, and local agencies for the prevention, preemption, deterrence, and investigation of terrorist acts that affect the United States' interests, and for the purpose of disrupting and preventing terrorist acts and apprehending individuals who may commit or plan to commit such acts.
FBI – Field Intelligence Groups	Coordinate, manage, and execute all functions of the intelligence cycle, including collection, analysis, production, and dissemination, for the FBI in field offices throughout the country.
U.S. Attorney's Offices – Anti-Terrorism Advisory Councils	Cross-section of federal, state, and local law enforcement, first responders, and private sector security personnel who coordinate counterterrorism efforts in their communities.

Source: FBI and Executive Office for U.S. Attorneys documentation

As acknowledged in the 2007 NSIS, state, local, and tribal governments serve as the nation's first "preventers and responders," and are critical to the nation's efforts to prevent future terrorist attacks and to respond if an attack occurs. Often, these state, local, and tribal entities are best able to identify potential threats that exist within their jurisdictions. In our review, we identified the National Network of Fusion Centers and the Regional Information Sharing Systems (RISS) as the two primary state and local counterterrorism information sharing entities. The following table provides the missions of these non-federal entities.

Table 4: Non-Federal Entities Engaged in Field-Based Counterterrorism Information Sharing

Entity	Mission
Fusion Centers	Serve as a focal point within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and state, local, tribal, territorial, and private sector partners.
Regional Information Sharing Systems	Support regional law enforcement, public safety, and homeland security efforts to combat major crimes and terrorist activity, as well as to promote officer safety by linking federal, state, local, and tribal criminal justice agencies through secure communications. In addition, provide users with information sharing resources, analytic and investigative support, and training.

Source: 2013 National Network of Fusion Centers Final Report and RISS website

FINDINGS AND RECOMMENDATIONS

INTEGRATION, COORDINATION, AND NATIONAL STRATEGY

In general, the OIGs found that federal, state, and local entities are committed to sharing counterterrorism information. The participating entities have shown their commitment to this effort by undertaking programs and initiatives that have improved information sharing, yet the participating entities were unable to quantify the significant personnel and funding resources dedicated to this effort. The OIGs also identified areas that require improvement to further strengthen the sharing of counterterrorism information.

Examples of Information Sharing and Coordination

During our review, several terrorism-related incidents occurred. We believe that many actions taken by federal, state, and local law enforcement agencies prior to, during, and following these incidents reflect their commitment to sharing counterterrorism information. For example:

- In June 2015, Ali Saleh, a resident of New York, was arrested after he systematically made multiple attempts to travel to the Middle East to join Islamic State of Iraq and the Levant (ISIL). Saleh, who allegedly was inspired by ISIL propaganda, expressed his support for ISIL online, and took steps to carry out acts encouraged in the ISIL call to arms. This arrest resulted from the efforts of the New York Joint Terrorism Task Force (JTTF) working collaboratively with its federal, state, and local task force officers.
- In June 2015, the Boston JTTF stopped and ultimately used deadly force against Usaamah Rahim, who had been under investigation and surveillance. According to an FBI affidavit, Rahim, along with co-conspirators, was initially plotting to kill a prominent blogger but had abandoned that plot and instead targeted police officers. During the course of the review, we learned that the successful disruption of this plot was based, in large part, on information shared between federal and local law enforcement authorities in Boston.
- During and following recent terrorism-related events, such as those in Chattanooga, Tennessee; Paris, France; and San Bernardino, California, fusion centers along with their federal, state, and local partners used the Homeland Security Information Network (HSIN) to share real-time updates, submit and respond to information requests, and support one another nationwide. The majority of fusion center personnel interviewed considered the use of HSIN as a best practice in information sharing across the National Network of Fusion Centers.

- Following the Paris, France; San Bernardino, California; and Brussels, Belgium, terrorist attacks, the FBI linked partner agencies using technology, including Secure Video Teleconference (SVTC), to quickly provide up-to-date threat information. For example, on the day of the Paris attacks, November 13, 2015, the FBI conducted a 3-hour conference call with representatives from all 78 Fusion Centers, DHS, executives from national law enforcement associations, the Criminal Intelligence Coordinating Council (CICC), Governor's Homeland Security Advisors, and state and local law enforcement.

In addition to these specific events, federal, state, and local partners exhibited a continued commitment to certain programs or initiatives, which further enhanced the sharing of counterterrorism information. For instance:

- The National Fusion Center Association, with federal support from DHS, DOJ, FBI, and the PM-ISE, is leading an initiative to share Real-time Open Source Analysis of Social Media (ROSM). The goal of the ROSM initiative focuses on how law enforcement agencies can and should analyze and share social media information and related criminal intelligence to help identify common indicators that can support intervention with potentially violent extremists and thereby prevent and/or disrupt attacks.
- In FY 2015, state and local partners initiated 623 terrorist watchlist nominations through I&A's Watchlisting Enterprise, 79 percent of which were accepted.
- As of FY 2014, about half of the almost 18,000 state and local law enforcement agencies in the United States had staff members who participated in their respective fusion center's Fusion Liaison Officer (FLO) Program. In FY 2014, there were a reported 40,187 FLOs, representing a 104-percent increase from about 19,700 in FY 2011.
- The FBI and DHS-led Nationwide Suspicious Activity Reporting Initiative is a collaborative effort for federal, state, and local law enforcement entities to share information on suspicious activities. Suspicious activity reporting increased by 96 percent between FY 2012 and FY 2015, with a majority of reports coming from the FBI's partners, including fusion centers.

Summary of Challenges

Although the above examples evidence positive and proactive information sharing between federal and non-federal partners, the OIGs identified several areas in which improvements could strengthen the sharing of counterterrorism information, as summarized below.

- Because both the FBI and DHS have counterterrorism-related missions and a role in gathering and disseminating counterterrorism information,

some DHS and FBI officials expressed concerns about potential overlaps in their counterterrorism missions and activities.

- Although there is a national-level information sharing strategy, the PM-ISE determined that its implementation across the information sharing environment has been uneven.
- The DHS Intelligence Enterprise is not as effective and valuable to the IC as it could be. For example, there is a lack of unity across the DHS Intelligence Enterprise, problems with I&A staffing levels in the field, issues with the internal intelligence product review and approval processes, and difficulty accessing classified systems and facilities in the field.
- DOJ can improve its counterterrorism information sharing efforts by implementing a consolidated internal DOJ strategy and evaluating the continued need and most effective utilization for the USAOs' Anti-Terrorism Advisory Council (ATAC) meetings. In addition, the FBI should spur participation associated with JTTFs and improve its efforts to obtain partners' input to the process for identifying and prioritizing counterterrorism threats.
- Within the ODNI, the Domestic DNI Representative (DDNIR) program is hindered by large geographic regions, as well as the lack of a clear strategic vision and guidance. In addition, the NCTC Domestic Representative program has also struggled to sufficiently cover its regions.
- At the state and local level, fusion centers are focused on sustaining operations rather than enhancing capabilities due to unpredictable federal support, including potential reductions in grant funding. Further, varying requirements for state and local security clearances sponsored by federal agencies can impede access to classified systems and facilities.

Based on the results of this review, the OIGs concluded that sharing of counterterrorism information among federal, state, and local partners could be strengthened. Details of the above issues are contained in the following sections, including recommended actions to further improve the sharing of counterterrorism information. We believe that implementing these recommendations will help enhance and coordinate information sharing, which, in turn, can lead to a more comprehensive picture of the terrorist threat and greater national security.

Interconnected Missions of Federal Partners

Both the FBI and DHS have counterterrorism-related missions and both have a role in gathering and disseminating counterterrorism information. The working relationships between DHS components and the FBI relating

to counterterrorism investigations reflect the challenges of these interconnected missions. During our review, some DHS and FBI officials expressed concerns about potential overlaps in law enforcement and counterterrorism missions and activities.

The FBI is the primary federal government agency responsible for handling counterterrorism investigations. However, these complex investigations often involve multiple possible violations of law, some of which may fall under another agency's primary jurisdiction, and thus, require information and expertise from different source agencies, such as travel information, nuclear regulatory information, or watchlist information. An executive within the FBI's Counterterrorism Division told the DOJ OIG that the FBI relies upon the JTTF concept to provide the coordination, information sharing, and deconfliction of investigative efforts. For example, multiple entities contributed to the investigation of the April 2013 bombing at the Boston Marathon, including the Boston JTTF, CBP, TSA, and USCIS.[14]

Although officials said that they generally understood the missions of the other partners, the involvement of multiple agencies in counterterrorism investigations increases the risk that field personnel may interpret sharing requirements and guidance differently than what is articulated in the interagency information sharing MOU.[15] The actions resulting from those differences in interpretations may contribute to a lack of trust among law enforcement agents, perpetuate negative perceptions about the other agency's ability and willingness to share information, and foster an atmosphere in which individuals rely on their personal relationships with other law enforcement partners rather than establishing standardized coordination mechanisms that remain in place despite any personnel changes.

The OIGs found that the quality of the working relationships between DHS components and the FBI varies widely in the field. For example, ICE HSI and FBI officials reported a challenging working relationship. According to the FBI, its field division leadership has consistently expressed to headquarters its concerns with ICE HSI performing work within the FBI's mission. ICE HSI has learned of these reports, which has perpetuated its negative perceptions about the FBI's willingness to work cooperatively with other law enforcement agencies. In general, ICE HSI said it believes the FBI does not sufficiently

14 Inspectors General for the Intelligence Community, Central Intelligence Agency, Department of Justice, and the Department of Homeland Security, Information Handling and Sharing Prior to the April 15, 2013, Boston Marathon Bombings, April 10, 2014.

15 The interagency information sharing MOU is discussed in the following section of this report.

understand or recognize ICE HSI's functions, capabilities, and abilities to contribute to counterterrorism investigations and information sharing. ICE HSI officials reported similar issues when discussing their involvement in the JTTFs.

However, CBP reported that it generally has good working relationships with FBI field offices and personnel. Some CBP officials suggested that this is most likely because CBP has distinct authorities and unique access to information about travelers, which is often used in counterterrorism investigations. CBP officials said their relationship with the FBI has come a long way in recent years so that it feels more like a partnership than previously when it was one-sided with CBP sharing information with the FBI but not vice versa. CBP officials added that their involvement in the JTTFs has led to better awareness by the FBI of CBP functions and capabilities.

Because agency missions are connected, it is critical that all partners understand and value the roles and contributions of its partners. The OIGs concluded that the issues cited above largely reflect struggles for this type of respect and cooperation in the counterterrorism arena. To achieve a shared vision and foster greater and more consistent cooperation, entities involved in counterterrorism should standardize practices and processes, as well as update and implement information sharing agreements. Throughout this report, the OIGs make recommendations to encourage and institutionalize such coordination through improvements to various practices and processes of the parties involved.

Strategy and Coordination in Domestic Intelligence and Information Sharing

To move away from personality-based coordination and codify interagency information sharing, the federal partners involved in counterterrorism efforts need formal agreements at the national level. The formal agreement governing information sharing, which includes priorities, requirements, and responsibilities, is outdated. The OIGs believe reviewing the interagency information sharing MOU and taking necessary actions to update intelligence information sharing standards and processes among the departments would reaffirm and formalize the roles and responsibilities of partners in the current information sharing environment. The agencies involved in counterterrorism should also establish processes to implement the overall strategy in the field. Clearly designating a capstone coordination and engagement body for the terrorism-related ISE would further assist in implementing the overall strategy and establishing field-level processes.

As previously noted, in October 2007, the White House issued the *National Strategy for* Information Sharing: Successes and Challenges in Improving Terrorism-Related Information *Sharing*, which outlined the Administration's vision for the information sharing environment. The White

House issued an updated national strategy, the *National Strategy for Information Sharing and Safeguarding* in December 2012 (2012 Strategy). The 2012 Strategy outlined goals and priority objectives for the information sharing environment. In December 2013, the PM-ISE issued its *Strategic Implementation Plan for the National Strategy for Information Sharing and Safeguarding*, which established a construct for executing the 2012 Strategy.[16] However, in its annual report to Congress for 2014, the PM-ISE reported that federal department and agency implementation of the 2012 Strategy had been uneven. The PM-ISE attributed some of the challenges in implementing the 2012 Strategy to the broad-based nature of the 2012 Strategy's priority objectives, as well as differences in department and agency prioritization, maturity, and operating environments.

In addition, although the White House updated the national strategy and the PM-ISE issued a strategic implementation plan, the *Memorandum of Understanding between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing* dates back to 2003. This MOU outlines information sharing priorities, reciprocity and transparency, sharing requirements, coordination and deconfliction, and officials responsible for information sharing. However, the MOU predates the establishment of the ODNI and NCTC.

The ODNI, DHS, and DOJ need to review the interagency MOU and determine what actions are necessary to update intelligence information sharing standards and processes among the departments. Such standards and processes should reflect the current structure, roles, and responsibilities of the ISE and the current threat environment and priorities. Based on these determinations, the NCTC, I&A, and FBI should continue to develop guidance for future intelligence information sharing, particularly in the field, that accounts for the roles and responsibilities the agencies have according to statute. Such guidance would enhance the sharing of intelligence information among federal representatives in the field and help create a unified and consistent federal contribution for state and local partners.

16 Some members of the ISE, such as DHS and the FBI, have also developed departmental and agency-level information sharing strategies to align with the national strategy.

The OIGs identified multiple entities (to include boards, committees, and councils) that are involved in the coordination and governance of domestic counterterrorism information sharing. Table 5 below provides examples of these entities and their missions.

Table 5: Examples of Information Sharing Coordinating Entities

Entity	Mission
Information Sharing and Access Interagency Policy Committee (ISA IPC)	Established by the White House to implement a national information sharing strategy and to lead information sharing policy across the federal government.
Information Sharing Council (ISC)	Advises the President and the PM-ISE in developing policies, procedures, guidelines, roles, and standards necessary to establish, implement, and maintain the ISE.
Homeland Security & Law Enforcement Partners Board	Established by the ODNI as an External Advisory Body that provides the DNI and IC leaders with external perspectives on the intelligence and information needs, equities, and capabilities of state, local, and tribal governments.
Intelligence Community Information Sharing and Safeguarding Executive	As the DNI's senior accountable officer, provides oversight and program management of all Offices of the ODNI and IC information sharing efforts; as well as leads, coordinates, facilitates, and as appropriate, manages all ODNI and IC information sharing.
Global Justice Information Sharing Initiative (Global)	Serves as a Federal Advisory Committee to advise the U.S. Attorney General on justice information sharing and integration initiatives.[17] Global supports the broad scale exchange of pertinent justice and public safety information and promotes standards-based electronic information exchange to provide the justice community with timely, accurate, complete, and accessible information in a secure and trusted environment.
Criminal Intelligence Coordinating Council (CICC)	Supports state, local, and tribal law enforcement and homeland security agencies in their ability to develop and share criminal intelligence nationwide. The CICC helps to facilitate the nationwide coordination on various efforts and initiatives to improve law enforcement's ability to share information and intelligence.
Homeland Security Advisory Council (HSAC)	Serves as a Federal Advisory Committee to provide organizationally independent, strategic, timely, specific, and actionable advice to the DHS Secretary and senior leadership on matters related to homeland security. The HSAC comprises leaders from state and local government, the private sector, and academia.

Source: OIGs' compilation of White House, ODNI, DHS, and DOJ information

17 Federal advisory committees,which may also be designated as commissions, councils, or task forces, are used to collect various viewpoints on specific policy issues. These committees are often created to help the government manage and solve complex or divisive issues. Such committees may be mandated by congressional statute, created by presidential executive order, or required by fiat of an agency head to render independent advice or make recommendations to federal agencies.

These multiple entities, with their differing roles and jurisdictions, lack an interconnectedness to facilitate collaboration, coordination, and integration of domestic information sharing. The OIGs believe that codifying an overarching engagement and coordination body for the terrorism-related ISE would help further these objectives.

Recommendations: The IC IG and DHS and DOJ OIGs recommend that the ODNI, DHS, and DOJ:

1. Review the 2003 interagency MOU on information sharing and determine what actions are necessary to update intelligence information sharing standards and processes among the departments.
2. Codify an overarching engagement and coordination body for the terrorism-related ISE.

DHS Intelligence Enterprise

The DHS Intelligence Enterprise is not as effective and valuable to the IC as it could be. For example, there is still a lack of unity among I&A and other DHS component intelligence programs, which also affects intelligence reporting. In addition, DHS OIG concluded that I&A staffing levels in the field may be making it difficult to fully support the DHS Intelligence Enterprise. Complications in its relationship with the FBI, as well as internal issues associated with the review and approval process are also negatively affecting I&A's production of intelligence reports. DHS must provide its stakeholders with information needed to disrupt and prevent terrorist threats and attacks. However, DHS intelligence personnel in the field have inconsistent access to the systems and facilities needed to receive, view, store, and share classified information above the Secret level.

Limited Cohesiveness and Coordination of Effort across the DHS Intelligence Enterprise

The DHS Intelligence Enterprise is fragmented, with elements operating independently and with few repercussions or incentives to coordinate better outside of actual events. The Under Secretary for Intelligence and Analysis, as

DHS' Chief Intelligence Officer (CINT), is responsible for integrating and standardizing DHS component intelligence program products, including products with terrorism information and national intelligence, but has not fully exerted its authority over the DHS Intelligence Enterprise. The DHS components involved have their own intelligence programs with their own cadre of intelligence professionals. Further, I&A is subject to IC directives and standards, but component intelligence programs are not, unless IC directives and standards have been institutionalized into DHS guidance.

I&A is taking several steps to help unify the DHS Intelligence Enterprise. For example, in 2014 I&A established a DHS Intelligence Rotational Assignment Program to promote a broader understanding of the various intelligence missions and functions across the intelligence enterprise and fusion centers. Efforts are also underway to ensure all intelligence products, briefings, and production plans are shared more evenly across the intelligence enterprise. However, the CINT has been unable to effectively require other DHS components to comply with its policies or to compel DHS component personnel to participate in its initiatives. Therefore, the CINT and key intelligence officials from the components should create incentives to encourage compliance and participation.

To enhance cooperation with other DHS components, I&A needs to better communicate its mission and role to component management. DHS OIG observed increased collaboration between I&A and DHS components where intelligence enterprise meetings are held regularly. This best practice builds relationships, conveys missions and roles, and enhances information sharing across DHS components. Although I&A intelligence officers are now required to hold such meetings quarterly, the differing locations of component field offices, caps on the number of I&A intelligence officers, and reshuffling of assignments have caused meetings in some areas to lose momentum.

There is also a lack of coordination between I&A and DHS components in intelligence reporting, but steps are being taken to address this issue. In 2012, DHS components established their own reporting programs, and at the same time, the Under Secretary for Intelligence and Analysis ended I&A's production of intelligence reports based on information from the components. According to officials from I&A Field Operations, some DHS components are now working with I&A on pilot programs to facilitate intelligence reporting. For example, the ICE HSI Intelligence Unit Chief sends information to an I&A senior reports officer in the field who then sends it to the region it impacts. I&A reports officers in the field then produce ICE intelligence reports for which both components receive reporting credit. CBP, TSA, and USCIS have expressed interest in developing similar pilots. Because DHS component intelligence programs have limited personnel in the field and the majority are not authorized to produce intelligence reports, these efforts could lead to more efficient and effective intelligence reporting. Rather than sending intelligence information to component headquarters to produce reports, DHS field officials

with subject matter expertise, access to information systems, and an understanding of local context could work with I&A field officials to produce reports.

Recommendations: DHS OIG recommends that I&A:

3. In conjunction with the key intelligence officials from DHS components, ensure DHS component intelligence programs comply with policies and create incentives for personnel to participate in initiatives that enhance the cohesion of the DHS Intelligence Enterprise.

4. Formalize agreements that enable I&A field officials to develop intelligence reporting with DHS components in the field, based on pilot program results.

I&A Staffing Issues

The *Intelligence Authorization Act for Fiscal Year 2014* required I&A to limit the number of intelligence officers in the field. As of December 2015, I&A had 59 intelligence officers in the field, primarily located at the nation's 78 fusion centers, serving as the IC's lead conduits to state, local, tribal, and territorial governments.[18] Nineteen of the 78 fusion centers did not have a dedicated I&A intelligence officer, although two of those centers are in the same location as fusion centers that have a dedicated intelligence officer. Nine intelligence officers and one regional director each serve two or three fusion centers; five of the nine intelligence officers serve fusion centers located more than 100 miles apart. Two regional directors are the only I&A personnel at their respective area's fusion centers. State and local entities expressed concern that recent changes to I&A Field Operations, such as the removal of some intelligence officer positions, have stretched these officers too thinly.

Because they are thinly staffed, I&A intelligence officers cannot fully support the DHS Intelligence Enterprise in the field. For example, I&A does not have intelligence officers at all the fusion centers near major DHS component field concentrations, such as along borders, including those fusion centers in El Paso and San Antonio, Texas; and San Diego, California. In addition, most DHS component intelligence program personnel are located at headquarters with few in the field, and intelligence-related work is largely a

18 I&A also has 26 reports officers in the field. However, they are trained and dedicated to producing intelligence reports, not to the additional functions performed by intelligence officers.

collateral duty for component field personnel. I&A could potentially fill this role through its intelligence officers assigned to fusion centers, but I&A does not have sufficient staffing in the field.

Insufficient Reporting of Counterterrorism Information

To develop a comprehensive and accurate threat picture, I&A field officials are expected to share information related to the missions of DHS and its components (e.g., information on homeland security, terrorism, and weapons of mass destruction) with state, local, and tribal entities. I&A field officials are also responsible for reviewing homeland security-relevant information, creating intelligence and other information products, and disseminating the products to the appropriate federal, state, local, and tribal government entities.[19] Given that DHS is largely responsible for travel-related security (e.g., borders, transportation, and immigration), DHS has unique access to information about travelers, including known or suspected terrorists, and is well-situated to intercept and identify travel by potential terrorists and foreign fighters. I&A field officials could use this information to enhance state and local information to identify and analyze trends. Although I&A has increased its focus on intelligence reporting by sending all intelligence officers and regional directors to reports officer training, converting some intelligence officer positions to reports officer positions, and developing additional reporting lines, it does not have formal guidance for field officials on the collection and coordination needed to create these reports.

In addition, none of the I&A field officials with whom DHS OIG spoke said they regularly develop intelligence reports from terrorism and counterterrorism information. I&A has a responsibility to produce intelligence reports based on counterterrorism information from state and locals for the IC, and the FBI has a responsibility to investigate terrorism-related matters and share counterterrorism information with the IC and outside agencies. Fulfilling these responsibilities can create tension because intelligence reports go to the IC while information that contributes to an investigation is generally closely held within the investigative team. Thus, I&A and the FBI may have difficulty coordinating these interrelated counterterrorism missions. Also, I&A has not asserted its reporting responsibility, leading the majority of I&A field officials to feel they needed permission from FBI field offices to develop counterterrorism reports. Without clear guidance on how to balance and coordinate these responsibilities, and with the desire to maintain good relationships with the FBI, about 43 percent of the I&A field officials interviewed said they no longer try to report on terrorism and counterterrorism information and about 21

19 6 U.S.C. § 124h.

percent have developed ad hoc arrangements with their respective FBI field office regarding reporting in general. For example, one I&A field official said he has informally agreed to write reports with information the FBI cannot or chooses not to report. Following DHS OIG's fieldwork, one I&A field official said I&A was working with the FBI to establish an agreement allowing I&A to create reports based on terrorist watchlisting.

I&A should help its field officials fulfill their responsibilities by developing and implementing guidance for intelligence reporting. In addition, better coordination with the FBI and other partners would help to create intelligence products that address investigative concerns and include terrorism- and counterterrorism-related information. Therefore, I&A should also clarify its role and improve coordination with its federal partners, including the FBI, by formalizing agreements and policies regarding intelligence reporting.

Recommendations: DHS OIG recommends that I&A:

5. Develop and implement guidance for intelligence reporting in the field.

6. Coordinate with the FBI to formalize guidance and policies for the reporting of terrorism and counterterrorism information.

Delays in I&A Intelligence Product Review and Approval

According to I&A field officials, approval and dissemination of I&A intelligence reports is often delayed, which could be the result of several factors. All I&A intelligence reports from the field must first be sent to I&A's Reporting Branch for review and approval. Then, the clearing offices - DHS Privacy Office, Civil Rights and Civil Liberties (CRCL), Office of the General Counsel-Intelligence Law Division, and I&A Intelligence Oversight – concurrently review the reports. However, reports are emailed, and there is no formal system to log and track the review process. Further, although each clearing office is supposed to complete its review reports within 2 business days, it is not clear how long it actually takes.[20] The Reporting Branch's review and approval appears to take the most time, which may be due in part to the branch's staffing levels and reviewing assignments. By the fall of 2015, the 59

20 DHS OIG requested statistics on review times from each clearing office and the Reporting Branch but did not receive comprehensive statistics from each office. The statistics received from the DHS Privacy Office, CRCL, Office of the General Counsel-Intelligence Law Division, and the I&A Intelligence Oversight indicated a review time of less than 1 business day.

I&A intelligence officers in the field completed reports officer training. In addition to the 26 reports officers in the field, these 59 intelligence officers can now produce intelligence reports, but Reporting Branch staff have not had commensurate increases. Ten senior reports officers review all reports from the field. In addition, by assigning reviews to senior reports officers based on regions, the Reporting Branch may be creating backlogs for officers responsible for regions with a greater number of reports or more complex reporting. During our review, I&A field officials also said they did not have local release authority, that is, the authority to send intelligence reports directly to the clearing offices for review and approval without first sending them to the Reporting Branch. The Under Secretary for Intelligence and Analysis recently approved granting local release authority to I&A field officials, but formal guidance had not been issued prior to the end of DHS OIG's fieldwork.

Because of the delays in I&A reporting, even though they would like to develop joint products, many fusion centers had given up on doing so. In one often cited example, a joint product with the New Jersey, New York, and New Hampshire fusion centers about homegrown violent extremists targeting military assets was in production for about 2 years. Several fusion centers said they still coordinate products with I&A field personnel who contribute informally, but without joint seals or official reporting credit. These types of timeliness issues were raised in an October 2012 Senate report and a July 2013 House report.[21]

For more flexibility and continued coordination with and support from fusion center partners, I&A has introduced new intelligence products and reports, such as Field Analysis Reports and Field Intelligence Reports. Field Analysis Reports are finished intelligence products designed to highlight analysis from the National Network of Fusion Centers on national, regional, and local issues of concern. Topics must meet I&A's statutory missions and authorities and should contain unique state, local, tribal, or territorial and/or DHS Intelligence Enterprise information or perspectives. Field Intelligence Reports are used to formally report raw, unevaluated information of potential intelligence value that responds to departmental requirements but not IC requirements. These new products have been well received by I&A stakeholders, including Congress, who had expressed concern about I&A's production levels.

---

21 United States Senate, Committee on Homeland Security and Governmental Affairs: Federal Support for and Involvement in State and Local Fusion Centers, Majority and Minority Staff Report, Permanent Subcommittee on Investigations (October 2012); and the United States House of Representatives, Committee on Homeland Security, Majority Staff Report on the National Network of Fusion Centers (July 2013).

Although I&A has taken steps to increase the timeliness and number of intelligence products, establishing formal review mechanisms and implementing formal guidance would further improve its intelligence reporting.

Recommendation: DHS OIG recommends that the DHS clearing offices:

7. Develop and implement a formal mechanism for reviewing I&A intelligence reporting from the field, including a logging and tracking process.

Recommendation: DHS OIG recommends that I&A:

8. Develop and implement guidance for field officials granting them local release authority for intelligence reporting.

DHS Lacks Consistent Access to C-LAN and SCIFs in the Field

Access to the C-LAN and Sensitive Compartmented Information Facilities (SCIF) are necessary for DHS intelligence personnel to fulfill their duties and to meet the goals of the DHS Information Sharing and Safeguarding Strategy.[22] However, while DHS I&A and other DHS Intelligence Enterprise personnel in the field have Top Secret/Sensitive Compartmented Information (TS/SCI) security clearances, they lack the supporting infrastructure to receive, view, store, and share information classified above the Secret level. Altogether, DHS components have SCIFs located at 19 sites outside of the National Capital Region that field personnel may reasonably use, such as to access the C-LAN. Of these 19, only 2 are I&A-certified SCIFs.

I&A's effectiveness as an IC member, in particular, is hampered by its limited access to classified systems and facilities. Nearly all I&A field personnel work in fusion centers, which now all have access to Secret-level classified information through the Homeland Secure Data Network (HSDN). However, counterterrorism information is often classified above the Secret level.

22 C-LAN operates as the DHS information technology network for the Top Secret/Sensitive Compartmented Information level. A SCIF is an accredited area, room, group of rooms, buildings, or installation where sensitive compartmented information may be used, stored, discussed, and/or processed.

Several DHS field personnel have brokered informal agreements through personal relationships with Department of Defense facilities and other federal field offices to gain access to the C-LAN. Some of these facilities require personnel to drive up to 3 hours, thereby limiting the frequency with which personnel may use them. Some DHS field personnel rely on the FBI for access to TS/SCI systems and space. For example, DHS task force officers have access to FBI SCIFs and systems through their participation in JTTFs, but this applies only to special agents. Of the 96 I&A field officials surveyed, about 43 percent hold active FBI badges similar to those that DHS task force officers receive and about 20 percent have access to FBI systems such as FBINet or the Top Secret/Sensitive Compartmented Information Operational Network (SCION).

To enhance the efficiency and effectiveness of counterterrorism information sharing, DHS needs to increase field personnel's access to classified systems and facilities above the Secret level. DHS should determine whether establishing more SCIFs in the field, formalizing agreements with other federal agencies, or pursuing a combination of the two, will resolve this issue and take the appropriate action.

Recommendation: DHS OIG recommends that DHS:

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.

DOJ Support of Counterterrorism Information Sharing

The DOJ OIG identified improvements that could be made to internal DOJ processes, JTTFs, and other field-based activities to enhance counterterrorism information sharing. Specifically, the DOJ OIG found that DOJ does not have a consolidated internal strategy to ensure that DOJ's counterterrorism information sharing efforts align with the President's strategic plan and that all DOJ components understand their respective roles and responsibilities. In addition, the FBI should further promote the JTTF Executive Board concept by increasing Board membership and spurring participation in Board meetings through standardization of content. Moreover, the DOJ OIG believes the ATAC meetings often duplicate other field-based counterterrorism information sharing efforts, and we believe that DOJ should evaluate the ATAC program to ensure the purpose of the ATAC meetings are not duplicative of other

counterterrorism information sharing partner initiatives. Finally, although the FBI has a well-defined process to identify and prioritize counterterrorism threats in each field division's jurisdiction, it could improve its efforts to obtain its partners' input on regional threats and mitigation strategies.

DOJ Strategy for Internal Counterterrorism Information Sharing

Based on discussions with an official from the Office of the Deputy Attorney General (ODAG), DOJ has not developed an internal strategy for counterterrorism information sharing separate from the President's strategic plan. This official stated that DOJ determined that its existing framework of policies and procedures constitutes DOJ's information sharing strategy.

The DOJ OIG believes that additional DOJ leadership is needed to ensure that DOJ's overall information sharing efforts and investments align with the 2012 Strategy and are coordinated and prioritized both within DOJ and with external partners. The DOJ OIG team discussed this issue with the DOJ Chief Information Officer (CIO) who agreed that coordination among the various DOJ components could be improved. According to the DOJ CIO, DOJ lacks an internal forum singularly dedicated to reviewing information sharing initiatives and investments across all DOJ components. The Law Enforcement Information Sharing Coordinating Committee (LCC), which was created in December 2006 by the Deputy Attorney General, was responsible for ensuring a department-wide collaborative and integrated focus on information sharing policy objectives. However, this group stopped meeting in 2009 because the group determined that it had accomplished its goal of enhancing interconnectivity with the Department's law enforcement partners following the establishment of the National Data Exchange.[23]

The lack of an internal strategy and forum for sharing information may hamper DOJ's ability to define and execute a comprehensive and unified plan for its information sharing initiatives and investments across all of DOJ's components. Officials from each DOJ component attend other information sharing working groups. For example, the DOJ CIO said that DOJ uses the Criminal Intelligence Coordinating Council (CICC) as a forum for components to discuss information sharing initiatives with external partners. The DOJ OIG is concerned that because DOJ does not have a consolidated internal strategy,

23 The National Data Exchange (N-DEx) provides criminal justice agencies with an online tool for sharing, searching, linking, and analyzing information across jurisdictional boundaries.

there is a risk that DOJ components may present or discuss initiatives that do not align with DOJ's unified vision.

The DOJ CIO said that he had recently proposed the establishment of a new council, the Law Enforcement Information Sharing Council (LEISC), that would be led by the Deputy Attorney General and help coordinate the information sharing efforts within DOJ. The proposed LEISC would provide a platform for DOJ entities to discuss and develop a unified vision regarding information sharing initiatives and investments, as well as ensure that DOJ actions are consistent with the 2012 Strategy. The DOJ CIO stated that DOJ is evaluating the LEISC, or a similar initiative, to determine how best to meet DOJ's operational and strategic planning needs. The DOJ OIG believes that the LEISC or a similar initiative could provide a valuable forum for the discussion and coordination of DOJ information sharing efforts, including overall strategy and investments. Information gleaned from this council's discussions could then be used during discussions with the PM-ISE and the CICC.

Recommendations: DOJ OIG recommends that DOJ:

10. Develop a comprehensive internal counterterrorism information sharing strategic plan based on a review of the President's strategic plan and in consultation with relevant partners.

11. Implement a council, led by a senior Department official, for the internal coordination of DOJ information sharing strategy and investments, and ensure that relevant components designate senior-level officials responsible for monitoring their component's efforts and communicating their efforts to DOJ as requested.

JTTF Executive Board Meeting Participation and Content

JTTFs, which are squads within each of the FBI's Field Divisions and select Resident Agency Offices, focus primarily on addressing terrorism threats and preventing terrorist incidents. The JTTFs leverage the resources and expertise of multiple member agencies to collect and share counterterrorism information. As of March 2016, the JTTFs were comprised of 54 federal agencies and 449 state, local, and other agencies. For example, DHS has more than 600 agents who participate on the 104 JTTFs nationwide. These DHS personnel help enhance the JTTFs' efforts through their unique expertise in areas such as immigration and customs enforcement.

In 2003, FBI field divisions were instructed to establish a JTTF Executive Board if they did not already have one. While the JTTFs conduct joint

counterterrorism investigations, JTTF Executive Boards are forums for sharing critical terrorism threat intelligence and ongoing investigative efforts to address those threats with law enforcement executives in their respective jurisdictions. As a result, the JTTF Executive Boards encompass a wider coverage of agencies within each respective jurisdiction because not all agencies are able to participate on a JTTF due to restrictions such as resources. In 2005, FBI field divisions were instructed to ensure that the JTTF Executive Board met on an as-needed basis but at least three times per year. The 2005 guidance further said that JTTF Executive Boards should be comprised of key federal, state, local, and tribal law enforcement officials, but at a minimum, include the heads of the agencies that have full-time agents and/or officers assigned to the JTTF within the respective field division's territory.

During the review, the DOJ OIG found that the JTTF Executive Board meetings in the sites the team visited were generally occurring at least quarterly. However, we are concerned with the number of agencies not represented on the JTTF Executive Boards and with the level of participation of those agencies on the JTTF Executive Boards. To assess the level of engagement and participation of executive management of the agencies that have full-time agents or officers assigned to a JTTF, the team reviewed JTTF task force officer and JTTF Executive Board member rosters and meeting attendance records maintained by the FBI for the eight FBI field divisions visited.[24]

24 The DOJ OIG requested the JTTF Executive Board member rosters and meeting attendance records for the preceding 2 years from each of the eight FBI field divisions. In reviewing the documentation provided, the total number of JTTF Executive Board meetings conducted by each site varied. Our analysis was based upon the data provided by each site.

As shown in the following table, 167 agencies assigned at least one task force officer to the JTTFs in the 8 locations reviewed. However, we found that 34, or 20 percent, of the 167 agencies did not have an agency representative on the JTTF Executive Board. For example, the FBI Boston Division's JTTF Executive Board only had representation from 40 percent of the agencies participating on the Boston JTTF.

Table 6: Analysis of JTTF Executive Board Engagement and Participation for Agencies with a Task Force Officer Assigned to a JTTF

FBI Field Location	Number of Agencies:			
	With a JTTF Task Force Officer	Without an Executive Board Member	With an Executive Board Member	Not Attending More Than Half of the Executive Board Meetings (excludes agencies without a Board Member)
Boston	20	12	8	3
Chicago	16	0	16	3
Dallas	20	2	18	3
Denver	18	1	17	7
Houston	37	7	30	19
New York	39	12	27	6
Portland	12	0	12	10
Springfield	5	0	5	1
Total	**167**	**34**	**133**	**52**

Source: DOJ OIG analysis of Federal Bureau of Investigation Data

Using the FBI-provided meeting attendance records, we found that 39 percent of the 133 agencies represented on the JTTF Executive Board did not attend at least half of the JTTF Executive Board meetings, as shown in preceding table.[25] This 39 percent included federal, state, and local agencies. The Special Agents in Charge (SAC) in two FBI field divisions we visited told us that the need to obtain appropriate security clearances prevented some state and local law enforcement representatives from attending the JTTF Executive Board meetings. Officials from federal agencies reported that they may miss meetings because of competing work demands, such as training and other meetings. While we recognize that individuals may not be able to attend every meeting, agency representation at the JTTF Executive Board meetings is

25 According to the FBI, not everyone who attends a JTTF Executive Board meeting may have signed the meeting attendance sheet. Because there was no other documentation available to confirm attendance, the DOJ OIG considered an individual to have regularly attended the meetings if she/he attended more than half of the meetings within the date ranges provided by the FBI based upon the meeting attendance sheets.

important, and we believe that the FBI and participating agencies should place greater emphasis on attendance because these meetings provide another avenue for obtaining relevant information concerning their jurisdictions that they may not obtain otherwise. To help place greater emphasis on these meetings, we believe it is essential that the FBI ensure that a management representative (and an alternate) from each agency with a task force officer assigned to the JTTF has been designated as a JTTF Executive Board member and ensure that those individuals are notified of upcoming meetings.

During the review of JTTF Executive Board data, the DOJ OIG found that representatives from agencies without full-time JTTF task force officers also attend JTTF Executive Board meetings. For example, regional representatives from the NCTC, I&A, and fusion centers attended meetings although these agencies did not have full-time JTTF task force officers.

The DOJ OIG also noted that representatives from local fire departments attended the JTTF Executive Board meetings in some FBI field divisions. The DOJ OIG discussed this issue with the Assistant Director for the FBI's Office of Partnership Engagement who said that he believed it was a "best-case scenario" to have first responders, such as fire departments, attend JTTF Executive Board meetings. He further indicated that if state and local first responders cannot participate on the JTTF Executive Board, then the first responders should be engaged with the fusion center. This official also stated that it was important to have the first responders on the JTTF so that they are aware of the threat picture and have situational awareness so they may respond appropriately in the event of a terrorist attack, such as Paris or San Bernardino. Therefore, the DOJ OIG recommends that the FBI ensure its field divisions encourage agencies that do not participate on the JTTF, including first responders, to attend JTTF Executive Board Meetings.

In addition to our concerns with the engagement and participation on the JTTF Executive Board, we believe the content of the meetings needs to be more standardized. Representatives from partner agencies who attended the JTTF Executive Board meetings reported the meetings provided valuable opportunities to share investigative and operational information, and that the meetings have improved in content and depth in recent years. The DOJ OIG attended a JTTF Executive Board meeting hosted by the FBI's Chicago Division. The meeting included an overview of the FBI's current threat environment, a roundtable discussion about emerging counterterrorism issues, and in-depth briefings on open terrorism investigations and threats, which were presented by various agencies, including the FBI, DHS, NCTC, and the area's two fusion centers -- the Illinois State Terrorism and Information Center (STIC) and the Chicago Crime Prevention and Information Center (CPIC).

However, in other locations, some partner agency officials reported that the depth to which the topics were covered varied from meeting to meeting, and that in some instances, the varying coverage coincided with changes in FBI

field division management. For example, a DHS official who attends the FBI Denver Division's JTTF Executive Board meetings said the meeting content varied in conjunction with three changes in the FBI Denver Division's leadership. This DHS official said that it would be more useful if the meetings were more consistent and provided both an overview of terrorism threats and specific cases. An official from the Colorado Division of Homeland Security and Emergency Management also said that he would like more strategic analysis of emerging threats, and that this type of information would assist him in his duties for the state of Colorado.

Although the DOJ OIG recognizes that some level of flexibility is needed to accommodate local needs, we believe the FBI should ensure that the JTTF Executive Board meetings across FBI field divisions consistently approach sharing information, which may well improve attendance at the meetings. Therefore, the DOJ OIG recommends that the FBI identify the structure and content of JTTF Executive Board meetings that would give attendees the most meaningful information on a consistent basis. The FBI should then inform field divisions to use this structure and content, perhaps as a template, at a minimum when planning their JTTF Executive Board meetings.

Recommendations: DOJ OIG recommends that the FBI:

12. Require FBI field divisions to stress to participating agencies the importance of designating an individual and an alternate to serve as their representatives to the JTTF Executive Board, as well as of regularly attending the meetings.

13. Ensure FBI field divisions encourage agencies that do not participate on the JTTF, including first responders, to attend JTTF Executive Board Meetings.

14. Identify an appropriate structure and content of JTTF Executive Board meetings that FBI field divisions should use at a minimum when conducting these meetings.

Anti-Terrorism Advisory Council (ATAC)

In 2001, the Attorney General established the ATAC program. As part of this program, each USAO designated an ATAC Coordinator to help enhance the nation's counterterrorism efforts. Each USAO also formed a committee comprised of federal, state, and local law enforcement agencies and often pertinent public health and safety and security officials from private industry. The program has three primary functions, including: (1) convening the ATAC (or committee) to facilitate counterterrorism efforts and information sharing in their communities; (2) supporting the investigative efforts of the JTTFs; and (3)

facilitating counterterrorism information sharing between DOJ field and headquarters components regarding threats, litigation, criminal enforcement, intelligence, and training. Each USAO was required to complete an ATAC Plan that defined how each office implemented the ATAC Program, and each USAO is supposed to update its plan every 6 months.[26]

Beginning at a March 2010 ATAC training event and continuing thereafter at training events, the ATAC National Program Coordinator instructed the ATAC Coordinators to coordinate their efforts with other entities within their jurisdiction to reduce duplication as it pertained to convening the committee to share counterterrorism information. For example, the USAO may not need to maintain its own distribution list for sharing counterterrorism information if the fusion center provides the primary information sharing responsibilities for national security matters within the district. Nonetheless, the USAO must remain a full-time participant with the agencies leading counterterrorism information sharing efforts and be willing to certify that the USAO is actively engaged in information sharing. Similarly, if the JTTF in the USAO's district conducts effective meetings and trainings that include the same law enforcement partners as the ATAC, then the USAO is not required to conduct duplicative ATAC meetings or trainings. However, the ATAC Coordinator should have a substantial role in developing the agenda, presenting information, and participating in the JTTF meeting or training.

To assess the USAOs' efforts to reduce the potential duplication between ATAC meetings and those of their partners, the DOJ OIG reviewed the 2006 and the most recent version of the ATAC plans for the USAOs located within eight FBI field division jurisdictions.[27] The DOJ OIG found that half of the USAOs' ATAC Plans had not been updated for nearly 10 years (from the initial submission in 2006 until the DOJ OIG requested them). As a result, the DOJ OIG was unable to determine the evolution of the ATACs and the USAOs' efforts to reduce the potentially unnecessary duplication of counterterrorism information sharing.

---

26 The ATAC Plan sets forth required objectives that must be achieved in each district. These objectives include defining the duties and responsibilities of the ATAC Coordinator and other USAO personnel who assist on counterterrorism matters, ensuring that the USAO has established a mechanism for effectively distributing time-sensitive information throughout the district, outlining collaboration between the ATAC Coordinator and DOJ's National Security Division, and ensuring the USAO has a plan for convening the ATAC.

27 We requested the most recent ATAC Plans for the USAOs located in the headquarter cities of the FBI field divisions we visited. The ATAC Plans for six of the USAOs were dated September 2015, one was dated April 2013, and one was not dated. We did not speak to the ATAC Coordinators about the plans because we were not informed of them until after our site visits.

In addition, the DOJ OIG found that several of the most recent ATAC Plans indicated fewer ATAC meetings being held or a consolidation of ATAC meetings with JTTF Executive Board meetings (the latter of which might or might not be consistent with the instructions to increase coordination and reduce duplication). Moreover, based on the review of attendance rosters, the DOJ OIG determined that, in general, representatives from the USAOs regularly attended JTTF Executive Board meetings within the eight FBI field divisions visited, and that the ATAC Coordinators said they participated in the meetings.

Given the progression of other counterterrorism information sharing efforts by other field-based entities, it is recommended that DOJ assess the ATAC program and ensure that the purpose of the ATAC meetings are not duplicative of other counterterrorism information sharing partner initiatives and are used in the most effective manner. For instance, instead of holding separate ATAC meetings, USAOs could be committed to fully participating in the JTTF Executive Board meetings and fusion center meetings, thereby standardizing the ATACs' roles and reducing possible duplication of efforts. Following this evaluation, the DOJ should ensure that each USAO updates its ATAC plan accordingly and that the plans are updated as required by the program.

Recommendation: DOJ OIG recommends that DOJ:

15. Ensure that each USAO updates its ATAC Plan as required by the program.

16. Evaluate the ATAC program to ensure the purpose of the ATAC meetings is not duplicative of other counterterrorism information sharing partner initiatives and is used in the most effective manner.

FBI Threat Review and Prioritization

The FBI Directorate of Intelligence implemented the Threat Review and Prioritization (TRP) process to assess, triage, and prioritize threats. The TRP process was designed to integrate intelligence and operations to provide a construct that synchronizes prioritization between FBI headquarters and field divisions. FBI field divisions use FBI National Threat Priorities and national-level mitigation strategies developed by FBI headquarters in completing their individual TRP process.

According to FBI policy, appropriate representatives from the USAO must be invited to participate in the TRP process. Officials from the USAOs the team visited said that USAO representatives participate in the TRP process and

believe the USAOs being involved in this process is beneficial. For example, an ATAC Coordinator from one of the USAOs visited said that she attended TRP meetings, and it helped her to understand the FBI's priorities and thought processes, which enhanced the USAO's awareness of the threat environment in the area. In addition, she said that she believes having the USAO participate in the TRP adds credibility to the TRP process and shows the FBI that the USAO cares about its issues.

Although not required by FBI policy, FBI SACs in two of the field divisions the team visited said that JTTF task force officers and other partner agencies participate in the TRP process. For example, the SAC for the FBI Denver Division said that the Denver Police Department attends the annual TRP meeting. Similarly, the SAC for the FBI Houston Division said that the USAO and JTTF task force officers participate in the TRP process. Further, he said that there would be a benefit to have even more agencies participate in the TRP process. However, some JTTF task force officers in the locations the teams visited said that they did not participate in the TRP meetings.

The DOJ OIG believes that it is important for the FBI to obtain its partners' input regarding the threats and mitigation strategies for the region. As a result, we recommend that the FBI direct FBI field divisions to identify and invite key stakeholders to TRP sessions.

The DOJ OIG also noted differences as to the individuals and entities with whom FBI field divisions shared their TRP results and, specifically, their prioritization of threats in their regions. For example, the FBI Boston Division shared its TRP outcomes with the command staff of the fusion center and the JTTF task force officer home agencies. In contrast, in the FBI Houston Division the JTTF task force officers who participate in the TRP process are responsible for providing such information to the management of their home agencies.

The results of the FBI's TRP process could provide important information to the FBI's counterterrorism information sharing partners. For example, the SAC for the FBI Houston Division said that there could be value in sharing the TRP results with JTTF Executive Board members, as well as the Texas Homeland Security Advisor. Similarly, the Homeland Security Advisor for the state of Colorado said that he believed it would be helpful to obtain the FBI Denver Division's TRP results for both the Denver area and the state of Colorado. As such, the DOJ OIG recommends that the FBI determine with whom it could share its counterterrorism-related TRP results and implement a process by which it shares counterterrorism TRP results with the appropriate partners on a systemic and regular basis.

Recommendations: DOJ OIG recommends that FBI:

17. Direct FBI field divisions to identify and invite key stakeholders to TRP sessions.

18. Determine the agencies with which it should share its counterterrorism-related TRP results and implement a process to ensure the TRP results are appropriately shared with those agencies on a systemic and regular basis.

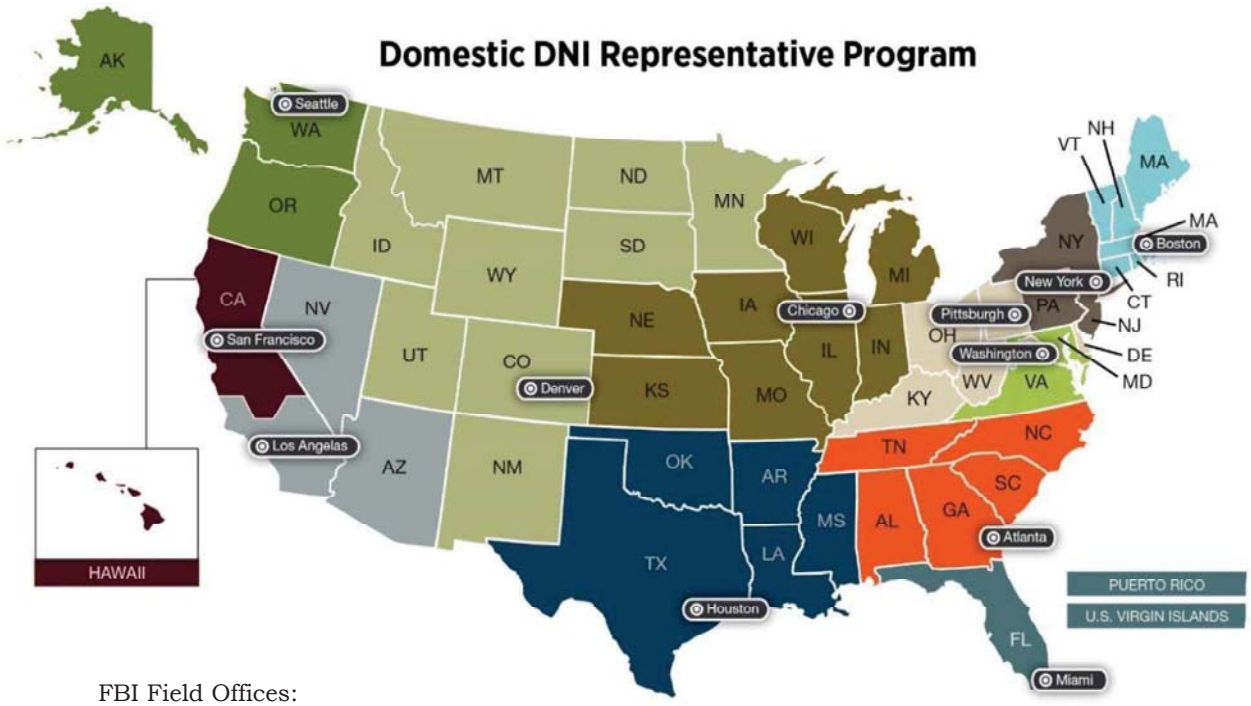
ODNI Field Based Elements Support to Counterterrorism Information Sharing

The ODNI has two programs focused on the field-based sharing of counterterrorism information: the Domestic DNI Representative (DDNIR) program and the NCTC Domestic Representative program. The OIGs found that although the DDNIR program has gained momentum and progress has been made, the program is hindered by large geographic regions, as well as the lack of a clear strategic vision and guidance for it to reach its full potential. The OIGs found that the NCTC Domestic Representative program, although well received in the field, has also struggled to sufficiently cover its regions.

The Domestic DNI Representative Program

The DDNIR program plays a role in facilitating the sharing of counterterrorism information. A November 2011 Memorandum of Agreement (MOA), "Domestic Director of National Intelligence Representatives," governs the DDNIR program between the ODNI and the FBI under Intelligence Community Directive 402, "Director of National Intelligence Representatives."

Domestic DNI Regions – The Director of National Intelligence and the FBI launched the DDNIR program in February 2012 and designated 12 FBI executives as DDNIRs. As shown in the map below, the DDNIRs are the Assistant Directors in Charge of Los Angeles, New York, and Washington DC, and the SACs of Atlanta, Boston, Chicago, Denver, Houston, Miami, Pittsburgh, San Francisco, and Seattle, with each representative being responsible for covering a designated geographic region.[28]



FBI Field Offices:

Birmingham, AL	Jacksonville, FL	Baltimore, MD	Newark, NJ	Portland, OR	Houston, TX
Anchorage, AK	Tampa, FL	Boston, MA	Albuquerque, NM	Philadelphia, PA	San Antonio, TX
Phoenix, AZ	Atlanta, GA	Detroit, MI	Albany, NY	Pittsburgh, PA	Salt Lake City, UT
Little Rock, AK	Honolulu, HI	Minneapolis, MN	Buffalo, NY	San Juan, PR	Norfolk, VA
Sacramento, CA	Chicago, IL	Jackson, MS	New York, NY	Columbia, SC	Richmond, VA
San Francisco, CA	Springfield, IL	Kansas City, MO	Charlotte, NC	Knoxville, TN	Seattle, WA
Denver, CO	Indianapolis, IN	St. Louis, MO	Cincinnati, OH	Memphis, TN	Milwaukee, WI
New Haven, CT	Louisville, KY	Omaha, NE	Cleveland, OH	Dallas, TX	
Washington, DC	New Orleans, LA	Las Vegas, NV	Oklahoma City, OK	El Paso, TX	

28 The OIGs were unable to find any documentation describing how the selection of the initial DDNIR locations were determined. However, officials familiar with the history of the program told us the regions were originally selected by identifying cities with a large presence of multiple IC elements.

The DHS Chief Intelligence Officer designated the I&A regional directors to serve as the DHS senior field representatives to the DDNIR program in specified geographic regions. I&A regional directors serve as the DHS focal point for all engagements with the DDNIR program. They maintain awareness of all DDNIR or ODNI staff visits to DHS components in their specified geographic region, coordinate actions with affected elements of the DHS Intelligence Enterprise, share program-related data, and work collaboratively with the U.S. Coast Guard national intelligence element to support its interaction with DDNIRs and ensure unity of effort and consistency in departmental messaging of DHS activities. While in some regions DHS Intelligence Enterprise field personnel participate in the program, the DDNIR is not authorized to task DHS components that are not elements of the IC. The scope of the DDNIR's authorities extends only to those DHS components that are elements of the IC: I&A and the U.S. Coast Guard's intelligence and counterintelligence elements.

Domestic DNI Quarterly Meetings – DDNIRs hold quarterly meetings with the IC representatives in their region to help foster collaboration, effective partnerships, and integration of the IC team in the domestic field. Quarterly meetings generally focus on a particular threat or issue that is of interest to the region.[29] To help ensure that the DDNIR program meetings are productive and support the primary mission of the program, the FBI has incorporated metrics into its field division performance measures. To actively participate in the DDNIR program, FBI field divisions are required to complete a combination of the following activities: serve as lead on a DDNIR region product; chair a sub-group; substantively contribute to a sub-group or region product; host a quarterly meeting; and/or complete a collaborative interagency action item.

The OIGs found that the differing sizes of some of the 12 geographic regions cause challenges for some of the DDNIRs when conducting quarterly meetings. For example, the DDNIR for the Rocky Mountain Region is responsible for the coordination of nine states in his region.[30] The Program Coordinator within that region reported challenges in identifying DDNIR meeting topics because issues and threats throughout the region differ

29 ODNI National Intelligence Managers and/or FBI Senior Intelligence Officers may travel to the quarterly meetings to provide threat briefings or relevant information.

30 The DDNIR Rocky Mountain Region encompasses nine states and four FBI field divisions, including the Minneapolis Division (Minnesota, North Dakota, and South Dakota), Salt Lake City Division (Idaho, Montana, and Utah), Denver Division (Wyoming and Colorado), and the Albuquerque Division (New Mexico). In terms of geographic territory, the Salt Lake City Division, Minneapolis Division, and the Denver Division are the 2nd, 3rd, and 4th largest territories in the FBI, respectively, trailing only the Anchorage Division (Alaska), making for an immense territory within the DDNIR Rocky Mountain Region.

considerably.[31] When her team surveyed meeting attendees for discussion topics, they often received no input.

In contrast, in the much smaller Northeast Region, the DDNIR found it easier to collaborate and plan meetings because he was close to the other SACs in his region and the field divisions have similar interests. According to the DDNIR for the Northeast Region, it is difficult for larger regions that are more geographically dispersed to collaborate and find commonality on topics.

According to officials with whom the IC IG spoke, the DNI had originally considered designating all heads of the 56 FBI field divisions as DDNIRs, which would have made the domestic program more closely resemble the overseas DNI representative program in which all CIA Chiefs of Station are designated as DNI representatives. Others with whom the team spoke, such as a former ISA-IPC chair, felt the idea had merit, stating that he never understood why some SACs are designated as representatives and others are not. In contrast, a senior FBI official currently assigned to the ODNI expressed the belief that having 56 DDNIRs may not be practical given that there are many competing priorities within the FBI.

The DHS OIG also discussed the geographical structure of the DDNIR program with I&A officials because Congress directed I&A to realign its field operations to the DDNIR Program regional construct.[32] Effective November 2014, I&A transitioned from 9 regions to the 12 DDNIR program regions. However, several I&A officials said they do not believe this structure makes sense for I&A. They expressed concern that conforming to the DDNIR regional construct hampered DHS' internal Unity of Effort message and that I&A should have realigned with other DHS regional constructs, in particular, FEMA regions. FEMA regions are well-established and already known by state and local entities that are primary customers for I&A field officials. DHS OIG concluded that should the DDNIR program modify its regional structure, I&A would likely be required to as well, thereby further impacting I&A personnel and resource allocation.

---

31 As part of the FBI implementation of the program, each of the 12 DDNIRs has designated an analyst within their office to serve as a DDNIR Program Coordinator. These Program Coordinators, who are typically located in the field division's Field Intelligence Group, are responsible for the day-to-day operation of the program to include coordinating with the other FBI field divisions and IC elements in their region to develop the agendas for the quarterly meetings, arrange speakers, and conduct a variety of other administrative and logistical tasks associated with the program. In some regions, FBI field divisions have full-time positions dedicated to the program coordinator role while in others it is a corollary duty. The role of the DDNIRs is an additional duty and DDNIRs do not receive any additional funding or personnel to execute their DDNIR responsibilities.

32 Classified Annex to the Intelligence Authorization Act for Fiscal Year 2014 (P.L. 113-126).

Per the MOA, the DNI and FBI may, through mutual agreement, add or remove ADICs or SACs as DDNIRs. While it may not be feasible to designate the heads of all 56 FBI field divisions as DDNIRs, in light of the current challenges posed by the large geographic regions, it may be feasible to designate some additional DDNIRs to help improve counterterrorism information sharing and coordination within larger existing regions. The OIGs recommend that the DNI, in coordination with the FBI, evaluate the existing DDNIR regional structure to ensure that regions are appropriately sized and defined to better align common areas of interest and geographic coordination among participating partners.

Mission and Program Guidance – The OIGs found that the DDNIR program lacks in-depth guidance and a well-defined strategy for ensuring the program is well-understood and implemented consistently across regions. All DDNIRs are required to attend a four-hour orientation at the ODNI before assuming their DDNIR role. However, we found that some of the DDNIRs want more guidance and clarification on what the DNI expects them to do. [33]

The OIGs also found that the objectives of the program had not been clearly communicated to the IC-member representatives. According to the DDNIR Southeast Region's October 2014 semi-annual report, despite messaging from ODNI and FBI leadership regarding the importance of the program, many of the participants in the region continue to express uncertainty as to the purpose of the DDNIR program and regional integration. [34] For example, one official who regularly attended meetings in the DDNIR Southeast Region stated that if the objective of the program is to "foster relationships," then the program is working well; but if the goal of the program is to collaborate on regional issues and produce a regional product, then the program is not succeeding. The DDNIR Southeast Region's October 2014 semi-annual report also noted that many of the region's partners have few or no analytic resources, and that for many, the analysis is conducted at the headquarters level.

---

33 Similarly, the Congressionally directed 9/11 Review Commission found in their March 2015 report, "The FBI: Protecting the Homeland in the 21st Century," that the DDNIR program is experiencing "growing pains," and that, "It is not well defined by the ODNI or well understood by the ADICs and SACs who serve in this capacity. Some confusion stems from the question of which functions the ADIC/SAC is performing for the DNI as opposed to performing as part of his/her FBI responsibilities, because the stakeholder groups are not the same. Most ADICs/SACs understand that the Domestic DNI Representative role is to lead coordination, but are not clear what should be coordinated, and to what end. ADICs/SACs did not believe that they had adequate guidance on how to manage the Domestic DNI Representative responsibilities beyond their own field office's geographic area, given that some of the 12 regions are quite large."

34 Each DDNIR is required to submit to the DNI semi-annual updates on the DDNIR's evaluations and recommendations of DNI policies and procedures and IC performance.

In reviewing the DDNIR quarterly meeting agendas and minutes, the DOJ OIG found that the meetings are generally maturing in structure and detail and that the depth of content covered has increased.[35] However, in some regions, the DDNIR quarterly meetings were seen primarily as networking opportunities where various officials also were invited to give topical presentations. In other regions, the DDNIRs were more involved in proactively establishing joint working groups and sub-working groups to address areas of common concern within the region ranging from border security to threats involving the oil and gas industry and ISIL.

At an annual meeting in May 2015, FBI Director Comey and DNI Clapper directed the DDNIRs to examine the Homegrown Violent Extremist (HVE) threat associated with ISIL in each of their regions in order to identify key intelligence gaps. The product was due October 31, 2015. However, specific guidance and project expectations were not provided to the DDNIRs until July 2015, which the DOJ OIG and IC IG were told resulted in significant confusion and wasted effort. According to an official from the ODNI's Office of Partner Engagement, most of the DDNIR regions produced External Intelligence Notes, which involve a much longer turn-around time due to various FBI requirements. This official said that by the time the products were available, the information was no longer valid or helpful to inform the DNI and FBI Director on emerging trends. Although this assignment provided a good opportunity to highlight interagency cooperation and further maturation of the DDNIR program in order to identify existing ISIL challenges at the regional level, the OIGs believe that this instance highlights the need for the program to have explicit and timely guidance on specific tasks. Although the DDNIR program needs to be sufficiently flexible to adapt to each region's issues and culture, clarifying guidance as to the intended outcomes of the meetings, as well as the roles and responsibilities of partners would be beneficial. Therefore, the OIGs recommend that the ODNI, in coordination with the FBI, develop and disseminate to IC-member partners more guidance and a strategy for ensuring the DDNIR program is implemented consistently across regions.

In addition to the need for more guidance, the OIGs noted that the original MOA, signed in 2011, is outdated and no longer reflects the current state of the program. Moreover, the MOA does not provide guidance on the

35 The DOJ OIG reviewed DDNIR meeting agendas and minutes for each of the DDNIR regions since the program's 2012 implementation, as well as copies of the briefings and presentations conducted during these meetings.

inclusion of non-IC members, such as state and local entities, in the DDNIR Program.[36]

In that regard, according to one regional representative, the DDNIRs should be better leveraging other partners, including fusion centers, state and local law enforcement, and the private sector. In his October 2014 semi-annual report to the ODNI, the former DDNIR for the Central Region indicated that he believed that incorporating both IC and non-IC members into the DDNIR process would encourage greater participation and exhibit trust in regional partners, which builds confidence in domestic intelligence collection, analysis, and reporting. The DDNIR for the Central Region suggested that perhaps the quarterly meetings should be expanded to two days—with one day for federal partners to meet and a second day for the DDNIR to meet with fusion center personnel. Conversely, DHS officials expressed varied opinions on the inclusion of non-IC partners in the program. The IC IG believes that non-IC partners may provide valuable information and perspective regarding the regional threat environment and recommend that the DNI, in coordination with the FBI, evaluate the regional structure and issue additional guidance, and explore the feasibility of also incorporating non-IC members into the DDNIR program in an appropriate fashion.

Recommendations: The IC IG recommends that the DNI, in coordination with the FBI:

19. Evaluate the existing DDNIR regional structure, in consultation with I&A, to ensure that regions are appropriately sized and defined to provide common areas of interest and geographic coordination among participating partners.

20. Develop and disseminate to IC-member partners additional guidance and a strategy for ensuring the DDNIR program is implemented consistently across regions and update the 2011 Memorandum of Agreement to more accurately reflect the current state of the program.

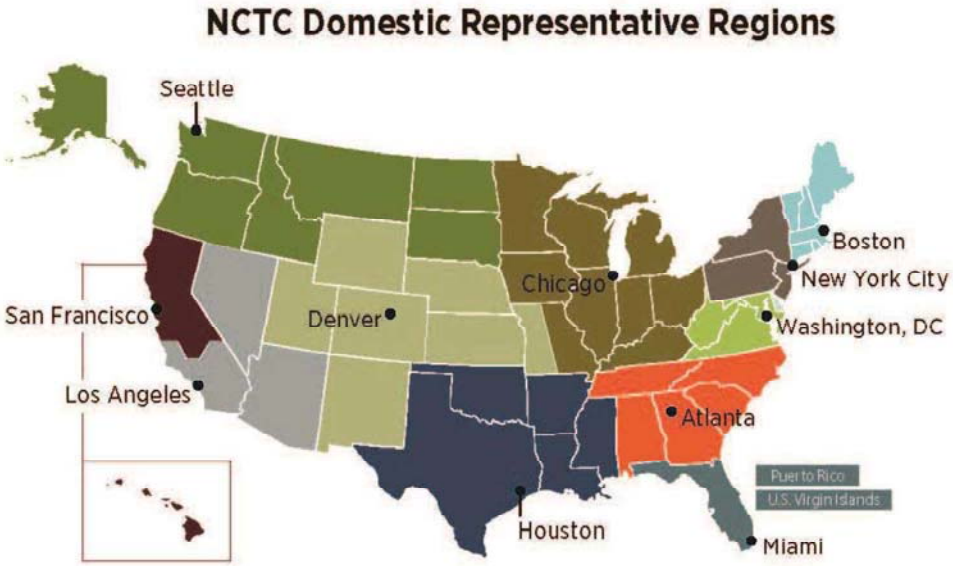
21. Evaluate the feasibility of incorporating non-IC members into the DDNIR program in an appropriate fashion.

36 The Congressionally-directed 9/11 Review Commission in their March 2015 report, "The FBI: Protecting the Homeland in the 21st Century," stated that the ODNI and FBI provide policy guidance on how state and local law enforcement and other non-Title 50 elements in the Homeland can legally and appropriately intersect with the Intelligence Community via the DDNIRs.

The NCTC Domestic Representative Program

NCTC's Domestic Representative Program was established through an MOU with the FBI. Currently, there are NCTC Domestic Representatives stationed at 11 locations across the United States. These representatives serve as the front-line liaison for the Director of NCTC with regional IC agencies and counterterrorism officials at the federal, state, and local levels. NCTC Domestic Representatives typically sit in FBI spaces and have a wide-range of job duties. One of their primary responsibilities is to deliver tailored counterterrorism-related intelligence support to a range of customers in the region, including FBI field divisions; regional FBI Field Intelligence Groups and JTTFs; DHS elements; local police; and other federal, state, and local entities. In addition, the NCTC representatives act as a liaison between NCTC and FBI field elements and between NCTC and the regional police departments by facilitating collaboration to enable the targeting, collection, processing, and reporting of targets of mutual interest. The NCTC retains primary control of the representatives and is responsible for covering the costs of all salary and official travel expenses.

The NCTC representative program has domestic representatives in 11 major cities across the country. Each representative is responsible for providing coverage to a distinct geographic region that aligns in some but not all of the regions covered by the 12 DDNIRs. DDNIRs and NCTC representatives are in the same locations, except in Pittsburgh, which has a DDNIR but not an NCTC representative. The geographic regions covered by the DDNIRs and the NCTC representatives differ in the Washington, DC, Chicago, Denver, and Seattle regions.



NCTC Representative Coverage – NCTC representatives frequently travel throughout their regions to perform their duties. Several representatives told the OIGs that they struggle to provide sufficient coverage for their region. For example, according to the NCTC representative in Los Angeles, his biggest challenge is the sheer number of customers he is responsible for supporting, which includes the FBI, DHS, fusion centers, and state and local entities dispersed across the three FBI field divisions (Los Angeles, Phoenix, and Las Vegas) that his area of responsibility encompasses. Accordingly, he must carefully pick and choose his engagements and make time to visit the more distant offices in Phoenix and Las Vegas.

Similarly, the NCTC representative in Atlanta, whose region covers five states, seven FBI field divisions, and five state fusion centers, told the OIGs that she would like to visit the major port cities—Charleston, Savannah, and Mobile—and other cities in her region, such as Memphis and Raleigh more frequently. Even the NCTC representative in Boston, whose area of responsibility includes six states relatively easy to visit by car—Connecticut, Massachusetts, Maine, New Hampshire, Rhode Island, and Vermont—stated that his principal challenge was finding the time to adequately support all six states and not wanting to turn down opportunities when asked to provide support.

In light of the regional differences between the NCTC Representative program and the DDNIR program, the DOJ OIG and IC OIG received feedback for the need for additional NCTC representatives. For instance, the DOJ OIG talked to the SAC in the FBI Pittsburgh Division who said that the NCTC representatives were an invaluable resource for their intelligence expertise and training and that having an NCTC representative would enhance collaboration in the area. The NCTC representative for New York (whose area of responsibility currently includes Pittsburgh) agreed that it might make sense to assign an NCTC representative to Pittsburgh but stated that the workload in Pittsburgh was lighter than in New York, and that NCTC might be better served by adding a representative in New York.

According to the NCTC representative for New York, the New York area generates enough work for two representatives, and one representative could stay fully occupied solely supporting the New York JTTF. If an NCTC representative were to be assigned to Pittsburgh, the NCTC representative for New York suggested that person could assume responsibility for some of the area of responsibility that currently falls within the NCTC representative for Chicago's region.

Another location that we were told should receive consideration for the assignment of an NCTC representative is Detroit. Currently, the NCTC representative for Chicago also has responsibility for Detroit but has difficulty providing adequate coverage because the area of responsibility is so large. It was suggested to the IC IG that the workload might be more manageable if

Chicago were to have its own NCTC representative and new representatives were added to cover the region outside of Chicago. An NCTC representative told the IC IG that she has heard from USAOs and other officials in the Midwest that they would like to establish closer relationships with and have more access to NCTC representatives.

As the OIGs conducted their fieldwork, they observed that some NCTC representative regions and the FBI Field divisions they support had more counterterrorism activity than others. For example, the NCTC representative for Denver explained that her region has less activity, which has impacted negatively her ability to obtain briefers from NCTC Headquarters to support her customers. Similarly, the NCTC representative for Miami estimated that she spends 85 to 90 percent of her time supporting the FBI Miami Division. Due to the FBI Miami Division's demands for her time, the NCTC representative for Miami had not yet had an opportunity to visit the FBI or state and local entities in Jacksonville, or the primary Florida Fusion Center in Tallahassee.

NCTC Representatives' Reception in the Field – During field visits, the OIGs received positive feedback on the contributions that the NCTC representatives are making to the FBI field divisions (e.g., one FBI field division stated that it would like to obtain an additional representative) and the Fusion Centers with respect to their role in furthering the sharing of counterterrorism information. NCTC representatives attend weekly FBI JTTF meetings, as well as quarterly JTTF Executive Board and DDNIR meetings where they brief on current threats and counterterrorism products. They provide case support ranging from conducting name traces through NCTC's Operations Center to arranging deeper dives on subjects of FBI investigations.

In addition, NCTC representatives request and coordinate on-site briefings and trainings by NCTC Headquarters subject matter experts on topics of interest, such as the Terrorist Screening Center and the Terrorist Identities Datamart Environment and their capabilities. NCTC representatives are highly valued for their ability to send information from the FBI field divisions directly to NCTC leadership.

NCTC representatives also work closely with I&A field personnel in their regions.[37] For example, the NCTC representative for Houston stated that his

37 I&A serves as the IC's lead conduit to state, local, tribal, and territorial governments. According to the Memorandum of Understanding between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing, no analytic conclusions of any covered entity shall be disseminated to state, local, or private sector officials, or to the public, without the prior approval of the Secretary of Homeland Security, his designee, or in accordance with approval mechanisms established by the Secretary except in exigent circumstances.

best set of customers are the I&A intelligence officers at the fusion centers. The NCTC representative for San Francisco also explained that she collaborates with the I&A intelligence officers at the Northern California Regional Intelligence Center, the State Threat Assessment Center, and Central California Intelligence Center to conduct joint briefings for the Fusion Center Terrorism Liaison Officer program.

The majority of I&A field officials the team interviewed said that the NCTC representatives serve as force-multipliers and that they complement the I&A intelligence officers as the representatives are in similar positions as themselves, "armies of one" alone in areas without field offices. Many I&A field officials conduct joint briefings with the NCTC representatives because the representatives have different access and provide greater insight into IC processes. Overall, both I&A field officials and NCTC representatives seem to value these joint briefings as they present "one government voice" to state and locals. However, there are some within I&A who are concerned about mission overlap. As the NCTC representative program continues to mature, further clarification of its roles and responsibilities and formalized coordination with I&A field officials will continue to be essential to avoid any potential duplication of effort or conflicting lines of inquiry.

Recommendation: The IC IG recommends that the Director, National Counterterrorism Center:

22. Consider assigning additional NCTC representatives to the field and/or revising the existing territorial regions, potentially to align with the DNI domestic regions, to ensure effective NCTC representation within the domestic field.

Fusion Centers

State and local entities own and operate fusion centers, but to develop and mature into the best partners, they depend on direct support and funding from federal agencies. Fusion centers also receive grant funding from FEMA indirectly; however, FEMA cannot identify how much funding fusion centers receive and spend on counterterrorism efforts. Based on self-reported data from fusion centers, direct federal expenditures for fusion centers are decreasing and state and local expenditures are increasing. Finally, the majority of state and local officials told DHS OIG that rather than enhancing and maturing their capabilities, given the unpredictability of resources, they are focused on sustaining operations.

Federal Investment and Support to Fusion Centers

According to the 2007 NSIS, state and major urban area fusion centers are vital assets to sharing terrorism-related information. Because fusion centers are state and locally owned and operated, federal influence to develop and mature fusion centers into the best potential partners depends on direct support and grant funding.

In June 2011, the PM-ISE issued the Federal Resource Allocation Criteria (RAC) Policy, which provides objective criteria for federal agencies to use when making resource allocation decisions to fusion centers. According to the RAC Policy, federal agencies will prioritize federal resource allocation in the following order: primary fusion centers, recognized fusion centers, and nodes.[38] Entities within each category must meet certain criteria for federal entities to continue their prioritization.

To guide federal resource allocation, the Federal RAC Policy Implementation Guidance, published in September 2014, offers best practices and recommendations about how to better develop, implement, and adhere to the Federal RAC Policy.

---

38 Each state, the District of Columbia, and U.S. territory may have one primary fusion center designated by the Governor or equivalent. A recognized fusion center is any designated fusion center, including major urban area fusion centers, not designated as a primary fusion center. Nodes refer to criminal intelligence units, real-time crime analysis centers, and other law enforcement or homeland security analytic centers that have not been designated as fusion centers by state governments.

I&A is required to provide the Office of Management and Budget (OMB) and the PM-ISE an annual inventory of all federal funding and personnel dedicated to the National Network of Fusion Centers. Direct federal expenditures are primarily salaries and benefits for federal personnel assigned to or directly supporting fusion centers, but also include federal information technology systems deployed to fusion centers, security clearances sponsored by federal agencies, and training and other resources specifically intended to help fusion centers build and sustain capabilities. The majority of fusion centers occupy space with other federal, state, or local agencies, resulting in commingled operating costs. Therefore, it is difficult to identify the total cost of fusion centers to the federal government because agency support serves multiple functions and purposes. For example, for the 14 fusion centers collocated with the FBI, providing access to IT systems may not be an additional cost to the FBI as their installation and maintenance would occur regardless of the presence of the fusion center. In addition, supporting a fusion center may be a part-time or collateral duty for DHS and DOJ personnel. Table 7 below provides the federal personnel support levels as reported to I&A for its annual inventory; Table 8 denotes whether those staff provided full- or part-time support to fusion centers as gathered by I&A. These numbers reflect a decline in total federal personnel support to fusion centers and of those personnel, fewer are full-time than when the reporting of such information began in FY 2011.

Table 7: Federal Personnel Support to Fusion Centers, 2011-2014

FY	DHS Personnel	DOJ Personnel	Others	Total
2011	272	125	--	397
2012	246	124	--	370
2013	258	122	10	390
2014	241	116	9	366

Source: 2011 and 2012 Federal Cost Inventory and 2013 and 2014 National Network of Fusion Centers Final Reports

Table 8: Level of Federal Personnel Supporting Fusion Centers, 2011-2014

FY	Full-Time	Part-Time	Total
2011	321 (81% of total)	76 (19% of total)	397
2012	293 (79% of total)	77 (21% of total)	370
2013	268 (69% of total)	122 (31% of total)	390
2014	266 (73% of total)	100 (27% of total)	366

Source: 2014 National Network of Fusion Centers Final Report

Within its 2014 report on the National Network of Fusion Centers, I&A identified three significant challenges associated with collecting, validating, and analyzing federal investment data:

1. Funding to support fusion centers is generally not a budget line item for most federal departments and agencies, so collecting and reporting investment data requires significant time and effort.

2. Some department and agency field offices directly support fusion centers at the field level, but the existence and extent of this support is not frequently shared with headquarters elements.

3. For those departments and agencies with organizationally separate operations and intelligence units or functions, one unit may engage with fusion centers without the knowledge of the other.

In addition to direct federal support, DHS indirectly provides grant funding to fusion centers through FEMA's Homeland Security Grant Program (HSGP).[39] However, FEMA cannot identify how much grant funding fusion centers receive and spend on counterterrorism efforts. Fusion centers do not directly receive HSGP funding but instead apply for funding and request reimbursements from the state. The governor-appointed State Administrative Agency applies for and administers HSGP funds. FEMA grant guidance simply requires that of the 25 percent of grant funding set aside for "law enforcement terrorism prevention activities," a portion must go to fund fusion centers; state and local governments determine that portion from year to year. The majority of interviewed state and local officials involved in the process said they would prefer that fusion centers be a specific line item in state and local budgets or FEMA grant requirements.

FEMA currently tracks grant funding through self-reported data received through state-submitted investment justifications and Biannual Strategy Implementation Reports. FEMA relies on states to appropriately and consistently categorize funding for all fusion center projects, but as GAO noted in a November 2014 report, this data is unreliable.[40] GAO reported cases in which projects supported broader capabilities not directly related to fusion centers, as well as some that did not specifically support center operations. For example, one grantee reported $14 million given to a fusion center for automated license plate readers and video surveillance equipment, although the fusion center was one of a number of system users.

---

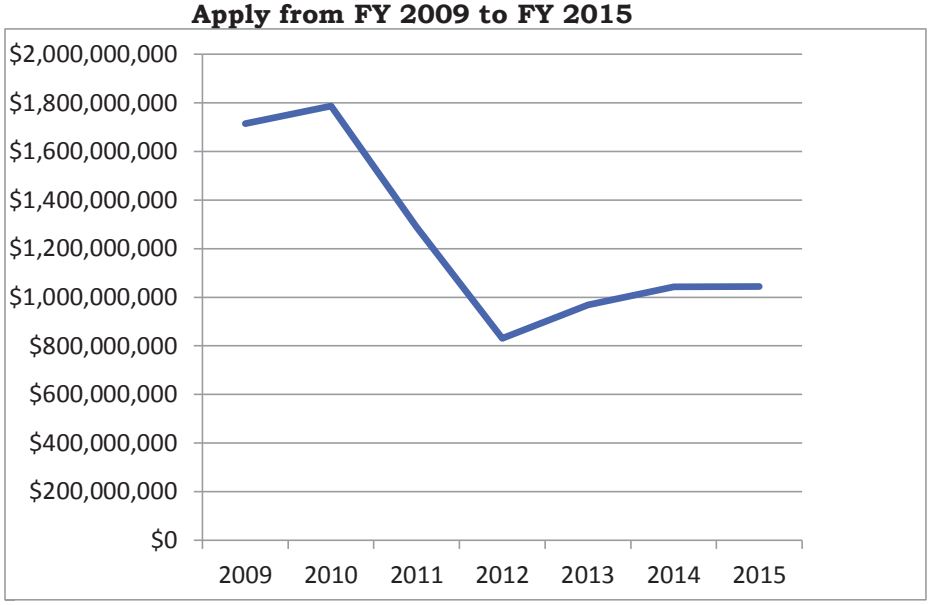
39 Fusion centers may receive HSGP funding through HSGP's State Homeland Security Program and Urban Areas Security Initiative.

40 Government Accountability Office: Information Sharing: DHS is Assessing Fusion Center Capabilities and Results, but Need to More Accurately Account for Federal Funding Provided to Centers (GAO-15-155) (November 2014).

Further complicating accurate accounting is FEMA's 3-year performance cycle under which fusion centers can spend up to 3 years of grant funding at any given time. Although the 3-year performance cycle is beneficial and welcomed by grant recipients, it makes it difficult to determine the portion of funds that has been expended each grant year. In addition, each of the 12 states DHS OIG visited operates on different fiscal year calendars than DHS; only the District of Columbia follows DHS' fiscal year calendar.

Based on self-reported data from fusion centers during the annual assessment process, direct federal expenditures for fusion centers are decreasing and state and local expenditures are increasing. In addition to decreased direct federal expenditures, the total amount of FEMA HSGP funding available for which U.S. states and territories may apply and thus may distribute to fusion centers has declined since its overall peak in FY 2010 as shown in Figure 1 below.

Figure 1: Total HSGP Funding Available for which States and Territories May Apply from FY 2009 to FY 2015



Source: DHS OIG analysis of FEMA data

Although the total level of grant funding made available by FEMA has decreased, state and local agencies reported expending about 41 percent more grant funding on fusion centers in FY 2014 than in FY 2011. This is generally indicative of state and local governments' commitment to fusion centers, which are considered valuable, worthwhile investments. As a result of this commitment by the state and local agencies that own and operate fusion centers, fusion centers are in a better position to sustain capabilities. Table 9 below displays sources of funding to fusion centers as reported by fusion centers.

Table 9: Sources of Funding to Fusion Centers, FY 2011-FY 2014[41]

Source	FY 2011[42]	FY 2012[43]	FY 2013	FY 2014
Direct Federal Expenditures	$97,456,195	$76,888,662[44]	$69,653,432	$68,216,940
Federal Grants Expended by State, Local, Territorial, and Tribal Agencies	$52,258,930	$71,219,656	$65,231,769	$73,499,366
State	$83,338,580	$90,980,473	$102,150,253	$113,297,136
Local	$34,144,222	$63,778,109	$70,304,104	$71,519,890
Tribal[45]	Data not available	$0	$100,256	$0
Territorial[46]	Data not available	$57,000	$153,658	$860,307
Private Sector	Data not available	$1,293,000	$642,770	$892,685
TOTALS	$267,197,927	$304,216,900	$308,236,242	$328,286,324

Source: DHS OIG Analysis of DHS Data

41 Data for FY 2015 was not available at the time of this draft report.

42 Federal grant, State, and local expenditure data for 60 of 72 fusion centers.

43 Federal grant, State, local, territorial, tribal, and private sector expenditure data for the 77 fusion centers designated at the time.

44 These estimates are from the 2011 Federal Cost Inventory and reflect only costs for the 72 fusion centers designated at the time; Federal staff costs are estimated.

45 SLTT Government Fiscal Year varies and may include multiple-year grant awards.

46 SLTT Government Fiscal Year varies and may include multiple-year grant awards.

Although increased state and local funding is a positive development, there are some concerns related to a decrease in federal funding. With DHS support decreasing, DHS may lose oversight and influence over fusion centers. Only fusion centers receiving FEMA grant funding must participate in DHS annual assessments of fusion centers. In recent years, Alaska, for instance, has not used FEMA grants to fund its fusion center and has declined to participate in the annual assessment process. Although DHS officials have worked with Alaska to ensure its participation in the assessment process for the time being, without a link to grant funding, DHS lacks enforcement capability.

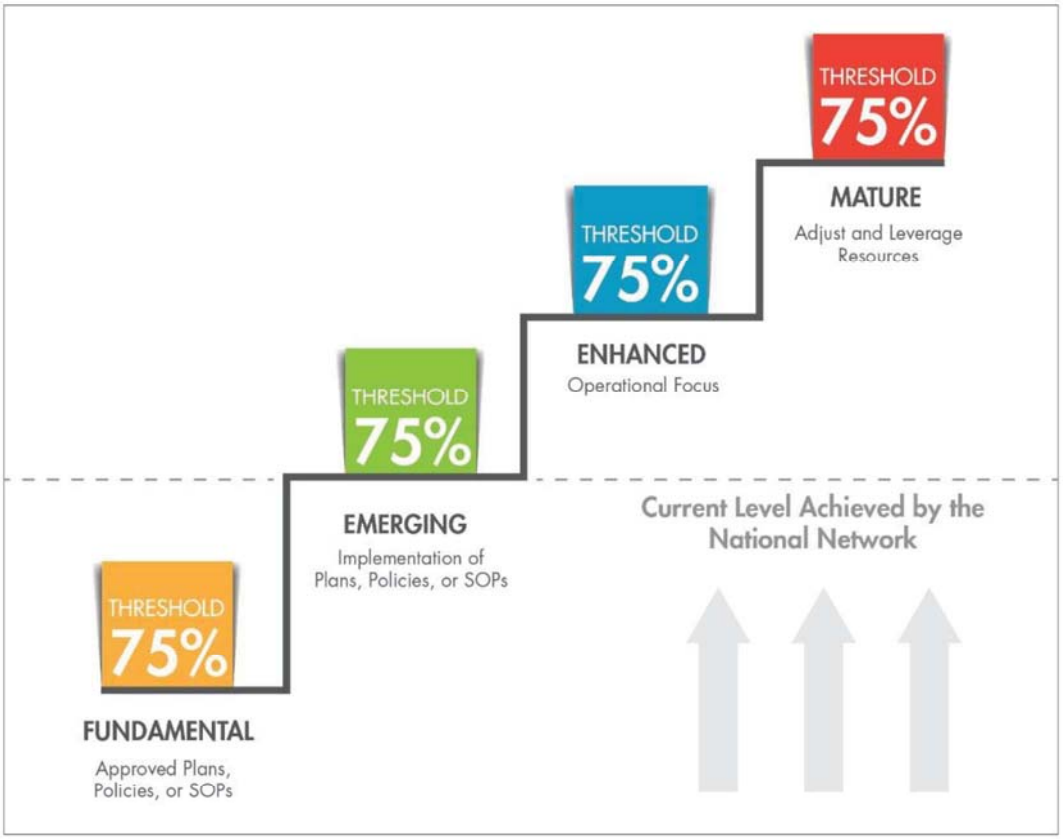
In addition, fusion centers utilizing FEMA grant funds must meet I&A requirements, such as conducting exercises and addressing resulting corrective actions, developing privacy policies, and completing annual training. These requirements establish standards for the national network and hold fusion centers more accountable to the public. Although all 78 fusion centers have complied with the requirement examples above aimed at the development and maturation of the national network, fusion centers losing or choosing not to accept FEMA grant funding may cut some of these important programs and activities to cover other mission-essential areas. Further, one fusion center director said, "if DHS has no skin in the game, the state and locals will not give them anything." Fusion centers must balance the sometimes conflicting priorities of state and local partners providing more funding with those of the federal government.

National Network Maturity Model

DHS and DOJ worked together to establish fusion center guidelines for developing and operating a fusion center within a state or region. Additionally, they worked with fusion center leadership to outline four Critical Operational Capabilities (COC), which reflect the operational priorities of the National Network of Fusion Centers, and four Enabling Capabilities (EC), which provide a programmatic foundation for the fusion process. I&A is responsible for the annual fusion center assessments, which began in 2011, to measure individual fusion center compliance with the guidelines and achievement of the COCs and ECs.

In its last annual assessment in FY 2014, I&A determined the National Network of Fusion Centers had reached the "Emerging Stage" on the National Network Maturity Model, as shown in Figure 2. The Maturity Model is a multistage framework designed to evaluate and categorize the overall progress of the national network as a whole in achieving the COCs and ECs. The Maturity Model consists of 46 attributes aligned to the four distinct stages. For each stage, the community established an outcome-oriented, qualitative definition and aligned capability attributes based on each attribute's contribution to the defined outcome for that stage. The National Network advances through each of the four stages of the maturity model when 75 percent of fusion centers achieve all of the attributes associated with that level.

Figure 2: National Network Maturity Model



Source: 2014 National Network of Fusion Centers Final Report

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.

Conclusion

Ensuring the United States is well-prepared to counter the threat of terrorism requires efficient and effective information sharing. The OIGs found that components of the ODNI, DHS, and DOJ are committed to sharing counterterrorism information. However, we also believe that the components can more fully commit to and improve their practices in this arena. The numerous partners involved in this vital endeavor must fully understand each other's missions and have clearly defined roles and responsibilities at the federal, state, and local level. Further, partners need to implement strong overall governance at the national level to ensure their field representatives fully embrace their roles according to the national strategy. Representatives in the field need to actively participate in information sharing forums, have access to information, and work in concert to leverage their resources and expertise and to expand their knowledge of national security threats. These improvements are paramount to national security partners effectively cooperating with each other to mitigate gaps and overlaps in sharing information, which is crucial to the United States' ability to prevent terrorist attacks.

APPENDIX A: OBJECTIVES, SCOPE & METHODOLOGY

The Senate Select Committee on Intelligence, the Senate Homeland Security and Governmental Affairs Committee, and the Senate Judiciary Committee requested that the Inspectors General (IG) of the Intelligence Community (IC), Department of Homeland Security (DHS), and Department of Justice (DOJ) conduct a performance audit of federally supported entities engaged in field-based domestic counterterrorism, homeland security, intelligence, and information-sharing activities in conjunction with state and local law enforcement agencies. The oversight committees requested that the joint audit examine the entities' overall missions, specific functions, capabilities, funding, personnel costs to include full-time employees and contractors, and facility costs.

In response to this request, the OIGs for the IC, DHS, and DOJ conducted a coordinated, joint review focusing on domestic sharing of counterterrorism information. The objectives of this review were to: (1) identify and examine the federally supported field-based intelligence entities engaged in counterterrorism information-sharing to determine the overall missions, specific functions, capabilities, funding, and personnel and facility costs; (2) determine if counterterrorism information is being adequately and appropriately shared with all participating agencies; and (3) identify any gaps or duplication of effort among these entities.

The review was conducted by three teams from the OIGs of the IC, DHS, and DOJ. The OIGs reviewed previous studies and conducted interviews with more than 450 individuals, including senior Office of the Director of National Intelligence (ODNI), DHS, DOJ, and state and local officials. While the review teams shared relevant documents, attended briefings, and participated jointly in interviews of certain officials and subject matter experts, each OIG was responsible for evaluating the actions of, and information available to, its respective department or agency. The teams attended, at least in part, meetings of the DNI's Homeland Security and Law Enforcement Partners' Board, interviews with DNI representatives and members of multiple JTTFs, and a teleconference with the Criminal Intelligence Coordinating Council (CCIC).

In total, the teams visited field-based domestic information sharing entities in 25 cities in 13 states and the District of Columbia:

- Massachusetts: Boston, Maynard
- California: Sacramento, Los Angeles, San Francisco
- Illinois: Chicago, Springfield
- Colorado: Denver
- Texas: Dallas, Houston, Garland, McKinney
- Missouri: Kansas City, Jefferson City, St. Louis
- New Hampshire: Concord
- Virginia: Fairfax
- New York: Albany, New York City
- New Jersey: Trenton
- Oregon: Salem, Portland
- Rhode Island: Providence
- Washington, DC
- Washington: Seattle

Of those reviews, all three teams travelled together to five cities: Denver, Colorado; Dallas, Houston, and Garland Texas; and New York, New York. Over 70 meetings were conducted by at least two of the OIGs.

The OIGs conducted their work in accordance with the Council of Inspectors General on Integrity and Efficiency's 2012 Quality Standards for Inspection and Evaluation. Those standards require an OIG plan and perform its work to obtain sufficient and appropriate evidence, provide reasonable bases for the findings, and put forth conclusions based on stated objectives. The evidence obtained in this review provides a reasonable basis for the findings and conclusions based on the objectives.

APPENDIX B: RECOMMENDATIONS

This appendix lists the report recommendations.

Recommendations: The IC IG and DHS and DOJ OIGs recommend that the ODNI, DHS, and DOJ:

1. Review the 2003 interagency MOU on information sharing and determine what actions are necessary to update intelligence information sharing standards and processes among the departments.

Joint OIG Analysis and Summary of Actions to Close Recommendation 1

Open. DHS and DOJ concurred with the recommendation as shown in Appendices D and E. ODNI provided comments on the recommendation as shown in Appendix C. The joint OIG team will continue to collaborate and monitor the actions of the components throughout the resolution phase to ensure each relevant component has taken the necessary steps to adequately address the recommendation.

2. Codify an overarching engagement and coordination body for the terrorism-related ISE.

Joint OIG Analysis and Summary of Actions to Close Recommendation 2

Open. DHS and DOJ concurred with the recommendation as shown in Appendices D and E. ODNI provided comments on the recommendation as shown in Appendix C. The joint OIG team will continue to collaborate and monitor the actions of the components throughout the resolution phase to ensure each relevant component has taken the necessary steps to adequately address the recommendation.

Recommendations: DHS OIG recommends that I&A:

3. In conjunction with the key intelligence officials from DHS components, ensure DHS component intelligence programs comply with policies and create incentives for personnel to participate in initiatives that enhance the cohesion of the DHS Intelligence Enterprise.

DHS OIG Analysis and Summary of Actions to Close Recommendation 3

Open. DHS concurred with the recommendation as shown in Appendix D. This recommendation can be closed when DHS OIG receives evidence that the DHS' Chief Intelligence Office (CINT) has implemented changes that will better integrate the DHS Intelligence Enterprise.

4. Formalize agreements that enable I&A field officials to develop intelligence reporting with DHS components in the field, based on pilot program results.

DHS OIG Analysis and Summary of Actions to Close Recommendation 4

Open. DHS concurred with the recommendation as shown in Appendix D. This recommendation can be closed when DHS OIG receives evidence, once finalized, of DHS' instruction for the process by which I&A reports officers will work with DHS Intelligence Enterprise field elements to produce Intelligence Information Reports at the local level.

Recommendations: DHS OIG recommends that I&A:

5. Develop and implement guidance for intelligence reporting in the field.

DHS OIG Analysis and Summary of Actions to Close Recommendation 5

Open. DHS concurred with the recommendation as shown in Appendix D. This recommendation can be closed when DHS OIG receives evidence of the finalized guidance for intelligence reporting in the field and documented implementation of such guidance.

6. Coordinate with the FBI to formalize guidance and policies for the reporting of terrorism and counterterrorism information.

DHS OIG Analysis and Summary of Actions to Close Recommendation 6

Open. DHS concurred with the recommendation as shown in Appendix D. This recommendation can be closed when DHS OIG receives evidence of formal, written guidance, developed in coordination with the FBI, on the reporting of terrorism and counterterrorism information.

Recommendation: DHS OIG recommends that the DHS clearing offices:

7. Develop and implement a formal mechanism for reviewing I&A intelligence reporting from the field, including a logging and tracking process.

DHS OIG Analysis and Summary of Actions to Close Recommendation 7

Open. DHS concurred with the recommendation as shown in Appendix D. This recommendation can be closed when DHS OIG receives evidence that the clearing offices – Privacy Office, Civil Rights and Civil Liberties (CRCL), Office of the General Counsel-Intelligence Law Division, and I&A Intelligence Oversight – are using this SharePoint tracking tool to document each office's review of I&A field intelligence reporting.

Recommendation: DHS OIG recommends that I&A:

8. Develop and implement guidance for field officials granting them local release authority for intelligence reporting.

DHS OIG Analysis and Summary of Actions to Close Recommendation 8

Open. DHS I&A concurred with the recommendation as shown in Appendix D. This recommendation can be closed when DHS OIG receives evidence of the final establishment and implementation of a field release capability.

Recommendation: DHS OIG recommends that DHS:

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.

DHS OIG Analysis and Summary of Actions to Close Recommendation 9

Open. DHS concurred with the recommendation as shown in Appendix D. This recommendation can be closed when DHS OIG receives evidence of the development and implementation of plans to ensure DHS intelligence officials in the field have practical access to classified systems and infrastructure above the Secret level.

Recommendations: DOJ OIG recommends that DOJ:

10. Develop a comprehensive internal counterterrorism information sharing strategic plan based on a review of the President's strategic plan and in consultation with relevant partners.

DOJ OIG Analysis and Summary of Actions to Close Recommendation 10

Open. DOJ concurred with the recommendation as shown in Appendix E. This recommendation can be closed when the DOJ OIG receives, once established, the comprehensive internal DOJ counterterrorism information sharing strategic plan.

11. Implement a council, led by a senior Department official, for the internal coordination of DOJ information sharing strategy and investments, and ensure that relevant components designate senior-level officials responsible for monitoring their component's efforts and communicating their efforts to DOJ as requested.

DOJ OIG Analysis and Summary of Actions to Close Recommendation 11

Open. DOJ concurred with the recommendation as shown in Appendix E. This recommendation can be closed when the DOJ OIG receives documentation that it implemented a council, led by a senior DOJ official, that is responsible for the internal coordination of DOJ information sharing strategy and investments. Further, DOJ OIG will need to receive evidence that each relevant component has designated senior-level officials who are responsible for monitoring their component's efforts and communicating their efforts to DOJ leadership as requested.

Recommendations: DOJ OIG recommends that the FBI:

12. Require FBI field divisions to stress to participating agencies the importance of designating an individual and an alternate to serve as their representatives to the JTTF Executive Board, as well as of regularly attending the meetings.

DOJ OIG Analysis and Summary of Actions to Close Recommendation 12

Open. The FBI concurred with the recommendation as shown in Appendix F. This recommendation can be closed when the DOJ OIG receives evidence that the FBI notified its field divisions to stress to JTTF participants the importance of designating representatives to the JTTF Executive Board, as well as regularly attending meetings. Further, the DOJ OIG will need evidence that FBI field divisions, in turn, communicated to the participating agencies the importance of the JTTF Executive Board meetings, including designating representatives and regularly attending.

13. Ensure FBI field divisions encourage agencies that do not participate on the JTTF, including first responders, to attend JTTF Executive Board Meetings.

DOJ OIG Analysis and Summary of Actions to Close Recommendation 13

Open. The FBI concurred with the recommendation as shown in Appendix F. This recommendation can be closed when the DOJ OIG receives evidence that the FBI instructed its field divisions to encourage agencies that do not participate on the JTTF, including first responders, to attend JTTF Executive Board meetings. Further, DOJ OIG will need evidence that the FBI field divisions, in turn, reached out to such agencies to encourage participation on the JTTF Executive Board.

14. Identify an appropriate structure and content of JTTF Executive Board meetings that FBI field divisions should use at a minimum when conducting these meetings.

DOJ OIG Analysis and Summary of Actions to Close Recommendation 14

Open. The FBI concurred with the recommendation as shown in Appendix F. This recommendation can be closed when the DOJ OIG receives evidence of the FBI's review and establishment of an appropriate structure and content of JTTF Executive Board meetings, and that FBI field divisions have been notified of the new structure and content.

Recommendation: DOJ OIG recommends that DOJ:

15. Ensure that each USAO updates its ATAC Plan as required by the program.

DOJ OIG Analysis and Summary of Actions to Close Recommendation 15

Open. DOJ concurred with the recommendation as shown in Appendix E. This recommendation can be closed when the DOJ OIG receives evidence that DOJ has developed a mechanism for ensuring USAOs update their ATAC Plans as required by the program.

16. Evaluate the ATAC program to ensure the purpose of the ATAC meetings is not duplicative of other counterterrorism information sharing partner initiatives and is used in the most effective manner.

DOJ OIG Analysis and Summary of Actions to Close Recommendation 16

Open. DOJ concurred with the recommendation as shown in Appendix E. This recommendation can be closed when the DOJ OIG receives the results of DOJ's evaluation of the ATAC program and whether the purpose of the ATAC meetings are not duplicative of other counterterrorism information sharing partner initiatives and are used in the most effective matter.

Recommendations: DOJ OIG recommends that FBI:

17. Direct FBI field divisions to identify and invite key stakeholders to TRP sessions.

DOJ OIG Analysis and Summary of Actions to Close Recommendation 17

Open. The FBI concurred with the recommendation as shown in Appendix F. This recommendation can be closed when the DOJ OIG receives the FBI's guidance to FBI field divisions about identifying and inviting key stakeholders to TRP sessions. Further, the DOJ OIG will need evidence that FBI field divisions, in turn, identified and invited key stakeholders to attend the TRP sessions.

18. Determine the agencies with which it should share its counterterrorism-related TRP results and implement a process to ensure the TRP results are appropriately shared with those agencies on a systemic and regular basis.

DOJ OIG Analysis and Summary of Actions to Close Recommendation 18

Open. The FBI concurred with the recommendation as shown in Appendix F. This recommendation can be closed when the DOJ OIG receives evidence of the agencies with which the FBI should share counterterrorism-related TRP results and of the process for ensuring the TRP results are shared with these agencies on a systemic and regular basis. Further, the DOJ OIG will need evidence that FBI field divisions have been notified of this process, and that FBI field divisions are sharing the TRP results with the identified agencies on a regular basis.

Recommendations: The IC IG recommends that the DNI, in coordination with the FBI:

19. Evaluate the existing DDNIR regional structure, in consultation with I&A, to ensure that regions are appropriately sized and defined to provide common areas of interest and geographic coordination among participating partners.

IC IG Analysis and Summary of Actions to Close Recommendation 19

Open. ODNI provided comments on the recommendation as shown in Appendix C. This recommendation can be closed when the IC IG receives an update on the status of their activity to meet the intent of the recommendation.

20. Develop and disseminate to IC-member partners additional guidance and a strategy for ensuring the DDNIR program is implemented consistently across regions and update the 2011 Memorandum of Agreement to more accurately reflect the current state of the program.

IC IG Analysis and Summary of Actions to Close Recommendation 20

Open. ODNI provided comments on the recommendation as shown in Appendix C. This recommendation can be closed when the IC IG receives an update on the status of their activity to meet the intent of the recommendation.

21. Evaluate the feasibility of incorporating non-IC members into the DDNIR program in an appropriate fashion.

IC IG Analysis and Summary of Actions to Close Recommendation 21

Open. ODNI provided comments on the recommendation as shown in Appendix C. This recommendation can be closed when the IC IG receives an update on the status of their activity to meet the intent of the recommendation.

Recommendation: The IC IG recommends that the Director, National Counterterrorism Center:

22. Consider assigning additional NCTC representatives to the field and/or revising the existing territorial regions, potentially to align with the DNI domestic regions, to ensure effective NCTC representation within the domestic field.

IC IG Analysis and Summary of Actions to Close Recommendation 22

Open. ODNI provided comments on the recommendation as shown in Appendix C. This recommendation can be closed when the IC IG receives an update on the status of their activity to meet the intent of the recommendation.

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.

DHS OIG Analysis and Summary of Actions to Close Recommendation 24

Open. DHS concurred with the recommendation as shown in Appendix D. This recommendation can be closed when DHS OIG receives evidence that a strategy has been developed and implemented to efficiently and effectively provide security clearances and reciprocity to state and local personnel.

APPENDIX C: THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE'S RESPONSE TO THE DRAFT REPORT

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
ASSISTANT DIRECTOR OF NATIONAL INTELLIGENCE
PARTNER ENGAGEMENT
WASHINGTON, DC 20511

PE 17-0003

MEMORANDUM FOR: Intelligence Community Inspector General

SUBJECT: Office of the Director of National Intelligence Response to the Office of the Inspector General Draft Report: "Review of Domestic Sharing of Counterterrorism Information"

The Office of the Director of National Intelligence (ODNI) appreciates the opportunity to review and respond to your report entitled, *Review of Domestic Sharing of Counterterrorism Information*. ODNI's responses to the recommendations in the report are attached for your consideration.

ODNI appreciates the time and effort required to research and draft this report and we commend your staff, along with the staff from the Offices of the Inspector General for the Department of Homeland Security and the Department of Justice, for their efforts.

JOHN D. BANSEMER
Lieutenant General, USAF

10 Nov 2017
Date

Enclosure:
Office of the Director of National Intelligence Information Paper, Response to Inspector General's Review of Domestic Sharing of Counterterrorism Information

SUBJECT: Office of the Director of National Intelligence Response to the Inspector General's Review of Domestic Sharing of Counterterrorism Information

In June 2016, the Director of National Intelligence (DNI), in consultation with the Executive Office of the President, decided to integrate the Program Manager for the Information Sharing Environment (PM-ISE) under the authority and direction of the Office of the Assistant DNI for Partner Engagement (ADNI/PE). This decision reflects the DNI's ongoing commitment to ensure our Nation and the Intelligence Community (IC) can maximize intelligence integration and government-wide information safeguarding and sharing in the most efficient and effective manner possible. The fusion of PM-ISE and PE will further strengthen, empower, and unify whole-of-government safeguarding and sharing of terrorism-related information across federal, state, local, tribal, territorial (FSLTT), private sector, and international mission partners.

While the Federal Government has made significant progress to advance terrorism-related safeguarding and sharing of intelligence and information, more work remains to ensure implementation of the best mechanisms to protect the homeland. The evolving terrorist threat highlights the critical need for strong partnerships and interoperable, and coordinated capabilities between and among FSLTT agencies. These partnerships enable appropriate information safeguarding and sharing and build trust, consistent with the missions and authorities of each agency and fully integrating the need to protect privacy, civil rights, and civil liberties.

It is important to emphasize the need for the IC's role inside the U.S. to be carefully constrained. The IC's authorities, tools, and tradecraft are properly focused on foreign threats to national security. While we must also look to their manifestations inside the country, we must carefully remain within the bounds of the limited domestic authorities and the defined roles entrusted to us. It is imperative that we continue to strengthen the national security apparatus to best protect our citizens while also protecting their privacy, civil rights, and civil liberties.

This response incorporates integrated responses from both IC and ISE authorities articulated in the Intelligence Reform and Terrorism Prevention Act of 2004, as amended (IRTPA).

Recommendation 1: Review the 2003 interagency Memorandum of Understanding (MOU) on information sharing and determine what actions are necessary to update intelligence information sharing standards and processes among the departments.

ODNI Response: A recent review by DHS in coordination with the ODNI concluded that the information sharing provisions of the MOU are overtaken by Executive Order and the IRTPA. The ODNI, in coordination with IC elements, and as a member of the Information Sharing Council, maintains ongoing discussions with ISE stakeholders to ensure domestic sharing of counterterrorism information is executed in an effective and responsible manner.

Recommendation 2: Codify an overarching engagement and coordination body for terrorism-related ISE.

ODNI Response: The Information Sharing Council is the body codified within IRTPA for the terrorism related ISE.

Recommendation 19: Evaluate the existing Domestic DNI Representative (DDNIR) regional structure, in consultation with the Office of Intelligence and Analysis (I&A), to ensure that regions are appropriately sized and defined to provide common areas of interest and geographic coordination among participating partners.

ODNI Response: ODNI, in consultation with the Federal Bureau of Investigation (FBI), believes the existing 12 regions are appropriately sized to meet the roles and responsibilities of the DDNIR program. The current structure allows for effective communication and coordination among IC organizations represented in the respective regions. A reduction in the number of regions could undermine effective communications and coordination because regionally assigned DDNIRs would see a corresponding increase in the number of IC regional offices (to include FBI Field Offices) in their regions. Conversely, increasing the number of DDNIR regions could lead to duplicative IC collaboration and increase travel costs.

Recommendation 20: Develop and disseminate to IC-member partners additional guidance and a strategy for ensuring the DDNIR program is implemented consistently across regions and update the 2011 Memorandum of Agreement to more accurately reflect the current state of the program.

ODNI Response: The IC, integrated through the Homeland Strategy Board, has already begun to address these and other identified needs. The Homeland Strategy Board has adopted a number of initiatives focused on improving the discoverability of intelligence and the transparency of activities across the Homeland domains, as well as working to enhance intelligence integration between the IC enterprise and regional levels. Strategic guidance and direction will continue through existing mechanisms to ensure IC equities are all addressed. The 2011 Memorandum of Agreement will be reviewed and revised as appropriate to ensure that it reflects existing strategic IC coordination; better defines the roles and missions of all partners involved in the DDNIR program; and is updated to capture recent changes within the ODNI and FBI.

Recommendation 21: Evaluate the feasibility of incorporating non-IC members into the DDNIR program in an appropriate fashion.

ODNI Response: The ODNI, FBI, and IC partners believe the DDNIR program is first and foremost a National Intelligence, Title 50, responsibility focused on effectively dealing with Foreign Intelligence priorities that might pose threats to the Homeland and/or those foreign and foreign-inspired threats that have a direct nexus to the Homeland. Some DDNIR regions have informally included non-IC members in quarterly meetings and working groups and found that their participation provides valuable information and perspectives regarding the regional threat environment. ODNI and FBI will consult with IC and FSLTT partners to consider the merits of appropriately formalizing this approach across the DDNIR program. Successes have been

achieved in sharing IC and Non-Title 50 (NT-50) information with regards to CT issues. The same successes have not been fully achieved in the sharing of information beyond the realm of CT. Also, including NT-50 organizations in the DDNIR program raises legal and policy issues that must be carefully addressed to ensure, among other things, that IC activities comply with policies that protect privacy, civil rights, and civil liberties.

Recommendation 22: Consider assigning additional National CT Center (NCTC) representatives to the field and/or revising the existing territorial regions, potentially to align with the DNI domestic regions, to ensure effective NCTC representation within the domestic field.

ODNI Response: NCTC recognizes the value of its representative program as it serves federal, state, local, and private industry customers in the domestic field. We strive to create and maintain the appropriate balance of domestic representatives in the field with existing personnel resources. We routinely evaluate the territorial regions assigned to each of our representatives to maximize efficiency and engagements with all partners.

APPENDIX D: THE DEPARTMENT OF HOMELAND SECURITY'S RESPONSE TO THE DRAFT REPORT

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

February 22, 2017

MEMORANDUM FOR: John Roth
Inspector General

FROM: Jim H. Crumpacker, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

SUBJECT: Management's Response to OIG Draft Report: "Review of Domestic Sharing of Counterterrorism Information" (Project No. 15-040-ISP-I&A)

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the work of the Offices of the Inspector General (OIG) for the Intelligence Community (IC), DHS, and the Department of Justice (DOJ) in planning and conducting this joint review and issuing this report.

The Department is pleased to note the OIG's positive recognition that the partners in the information sharing environment (ISE) – components of the Office of the Director of National Intelligence (ODNI), DHS, DOJ, and their state and local partners – are committed to sharing counterterrorism information. The OIGs also recognized partners' actions taken before, during, and after various recent terrorism related incidents.

The draft report contained 10 recommendations for DHS with which the Department concurs. It is important to note that DHS previously identified many of the issues highlighted in the report and has taken actions to address them. Unfortunately, not all our accomplishments are reflected in the report since the fieldwork for this review ended more than one year ago. Attached find our detailed response to each recommendation.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Attachment

Attachment: DHS Management Response to Recommendations Contained in OIG Draft Report for Project No. 15-040-ISP-I&A

The OIGs of the IC, DHS, and DOJ recommend that the ODNI, DHS, and DOJ:

Recommendation 1: Review the 2003 interagency MOU on information sharing and determine what actions are necessary to update intelligence information sharing standards and processes among the departments.

Response: Concur. DHS has conducted a review of the 2003 interagency Memorandum of Understanding (MOU) on information sharing. We believe that all key provisions of the 2003 MOU have been overtaken by statute, executive order or presidential directive, or are covered by other existing authoritative policy documents. Revision of the MOU is unnecessary to reflect these updated legal authorities and policies. Further, we did not identify any impediments to sharing that should be addressed in a new MOU. There are sections in the 2003 MOU pertaining to sharing with non-Federal stakeholders already supported by IC policy, executive order, statute, and other agreements. Any additional required provisions can be addressed by DHS, ODNI or DOJ separately through internal policies. A matrix identifying all of the places where the information from 2003 is now overcome by events or addressed in other documents has been provided to DHS OIG under separate cover. We request that DHS OIG consider this recommendation resolved and closed.

Recommendation 2: Codify an overarching engagement and coordination body for the terrorism-related ISE.

Response: Concur. DHS agrees there should be a single governance body for the terrorism-related ISE. However, DHS does not believe the Criminal Intelligence Coordinating Council (CICC) should fulfill that role as the report recommends. The CICC is a working group under the Department of Justice's Global Justice Information Sharing Initiative (Global Initiative). The Global Initiative serves as a Federal Advisory Committee to the DOJ and advises the Attorney General on justice information sharing integration initiatives. The CICC is chaired by state and local government personnel, and its charter allows the CICC to make recommendations to DOJ on criminal intelligence issues beyond the focus of just terrorism issues. Given these factors, DHS believes the existing Information Sharing and Access-Interagency Policy Committee should continue to be leveraged to fulfill this role, potentially utilizing the Program Manager for the ISEs (PM-ISE's) Information Sharing Council (ISC) as in prior years. The ISC Charter outlines the following duties for the ISC: "Pursuant to section 5(b)(i) of EO 13388, the Council shall provide advice and information concerning the establishment of an interoperable terrorism information sharing environment (ISE) to facilitate automated sharing of terrorism information among appropriate agencies to implement the policy set

forth in Section 1 of EO 13388." This language could be easily modified to provide a governance role for the ISC. DHS will support the inter-agency effort to have the ISC provide a governance role for the ISE. Estimated Completion Date (ECD): To Be Determined.

The DHS OIG recommended that I&A:

Recommendation 3: In conjunction with the key intelligence officials from DHS components, ensure DHS component intelligence programs comply with policies and create incentives for personnel to participate in initiatives that enhance the cohesion of the DHS Intelligence Enterprise.

Response: Concur. The Homeland Security Intelligence Council (HSIC) is an advisory body to the DHS Chief Intelligence Officer (CINT), and consists of Key Intelligence Officials (KIO) and other departmental representatives. KIOs represent Component Intelligence Programs (CIP), which were formally designated in 2016. The CINT worked closely with the Heads of Intelligence Components to determine CIP designations, which is important in that the CIPs that are defined in policy as the foundational elements of the DHS Intelligence Enterprise (IE).

The CINT fully supports the Intelligence Rotational Assignment Program (IRAP), which offers rotational opportunities internal to the DHS IE. In January 2016, the CINT levied a requirement for all CIPs to participate with at least two IRAP positions (inbound or outbound) by the end of 2016. The DHS Office of Intelligence and Analysis (I&A) also has sponsored reimbursable IRAP positions on the CINT's staff, one of which currently is filled by a Customs and Border Protection (CBP) Intelligence Officer serving as the DHS's Intelligence Functional Manager (IFMs) for Collection and Reporting.

In February 2016, the CINT created an IE management construct to provide both a DHS intelligence perspective on mission priorities (Intelligence Mission Managers), as well as to integrate the enabling functions for the IE (IFMs). Under the IFM construct, in coordination with the HSIC, the CINT is providing the IE with baseline standards stemming from IC policies, guidance, and standards. IFMs are overseeing progress across the IE by institutionalizing applicable IC standards in DHS Intelligence Integration Management policies. Policies and guidance that institutionalize IC standards for the DHS IE include:

- DHS Instruction 264-02-001, "DHS Tearline Process Guidance," signed January 2014, this Instruction establishes the standards for requesting, processing, and disseminating tearlines for organizations within the DHS Intelligence Enterprise and is directly associated to Intelligence Community Directive (ICD) 209, "Tearline Production and Dissemination."

- DHS Instruction 264-01-008, "IC Controlled Access Program (IC-CAP) Management, Administration, and Oversight," signed December 2015, this Instruction is directly associated to ICDs 705 "SCIFs," 501 "Discovery and Dissemination of Intelligence," and 906 "Controlled Access Programs." (Classified)
- DHS Instruction 264-01-009, "DHS Support to Domestic Director of National Intelligence Representatives," signed May 2012, this Instruction clarifies roles and responsibilities and establishes DHS processes and procedures to support the Domestic DNI Representative Program under ICD 402, "Director of National Intelligence Representatives," Annex B, December 2009.
- DHS Instruction 264-01-011, "DHS Foreign Disclosure and Release," signed June 2016, this Instruction implements and adheres to the authorities and responsibilities described in ICD 403 by establishing DHS processes and procedures for coordinating and overseeing the foreign disclosure and release of (1) classified national intelligence and (2) classified or unclassified national intelligence to foreign intelligence services. ICD 403, "Foreign Disclosure and Release of Classified National Intelligence," March 2013, as amended.
- DHS Instruction 265-05-006, "DHS SCI Access and SCIF Accreditation," signed December 2012, this Instruction establishes standards for sponsoring new access to Sensitive Compartmented Information (SCI) and accreditation of Sensitive Compartmented Information Facilities (SCIFs) and is directly related to ICD 704, "Personnel Security Standards and Procedures Governing Eligibility for Access to SCI Information and Other Controlled Access Program Information," October 2008 and ICD 705, "Sensitive Compartmented Information Facilities," May 2010.
- DHS CINT Memorandum, "Interim Guidance regarding DHS Component release of DHS Intelligence Information Reports," signed July 2015, aligns with Executive Order 12333.
- DHS CINT Memorandum, "Guidance for Accessing Intelligence Community Information (by non-Title 50 personnel in DHS, aka "isICmember attribute")," signed April 2015, this memo clarifies who within DHS may acquire access to IC information and aligns with Intelligence Community Policy Guidance 500.1, "Digital Identity."

The CINT has identified points of contact (POC) for each CIP to facilitate improved communication with the IE workforce. The CINT may now communicate directly to all IE personnel to enhance awareness of policies, standards, and rotational opportunities available to those in CIPs.

The CINT is also working with the DHS Chief Financial Officer's Program Analysis and Evaluation (PA&E) team to seek Fiscal Year (FY) 2019 funding for CINT IE initiatives that cut across Intelligence Components and fund integrative activities that benefit the analysis, collection, and operations of multiple CIPs. This would provide an incentive for CIPs to collaborate and advocate for integrated resources not prioritized by an individual

Component in order to address enterprise wide challenges. The CINT is in the process of coordinating and finalizing select requirements and submitting them as part of the Department's upcoming FY 2019 planning, programming, budgeting, and execution cycle. ECD: March 31, 2017.

Recommendation 4: Formalize agreements that enable I&A field officials to develop intelligence products with DHS components in the field, based on pilot program results.

Response: Concur. In March 2015, I&A's Field Operations Division (FOD) and the U.S. Immigration and Customs Enforcement's (ICE) Office of Intelligence (IO) coordinated a pilot wherein DHS I&A Reports Officers (ROs) would author Intelligence Information Reports (IIRs) containing ICE information, citing their own Field Reporter Numbers under the ICE Collection Reporting Code, thereby crediting both Components. For the duration of this pilot, I&A ROs drafted an average of seven ICE IIRs per month. The pilot concluded on December 15, 2016.

ICE's IO currently works with I&A ROs through two senior DHS I&A ROs identified as the primary POCs. I&A ROs then draft the applicable IIRs and submit the reports back through their POCs to ICE's IO for approval. ICE's IO releases the IIRs following pre-publication review by the I&A POCs and their ICE counterparts.

Based on the initial pilot results, ICE's IO proposed an expansion of the number of source documents they will provide to I&A ROs to increase RO production of ICE IIRs. ICE will provide a wider range of information.

Additionally, FOD and ICE's IO agreed to establish a separate pilot to embed DHS I&A ROs in ICE Special Agent in Charge (SAC) Intelligence Program offices (SIPs) by March 31, 2017. The ICE RO program agreed to identify approximately 10 offices in major metropolitan areas where the SIP is actively seeking to increase IIR production and/or the ICE RO program is receiving significant material for IIR production. ICE and I&A will evaluate this program by June 30, 2017, to determine what adjustments might be needed and establish a plan for future phases of the program.

Two Homeland Security Investigations SAC offices and two CBP facilities have conducted limited independent pilots where I&A ROs directly engaged with their Component partners to write IIRs on ICE and CBP information. The success of these engagements on IIRs proved the concept of field-level collaboration on intelligence information reporting, and highlighted the benefits of the I&A ROs being able to rapidly consult with their ICE and CBP colleagues.

In addition, FOD is working on a DHS Instruction institutionalizing the process wherein DHS I&A ROs will work with DHS IE field elements to access intelligence information,

gain an understanding of local context, deconflict reporting, and produce IIRs at the local level. ECD: September 30, 2017.

Recommendation 5: Develop and implement guidance for producing intelligence reports in the field.

Response: Concur. I&A has made significant headway in codifying and implementing guidance for intelligence reporting. I&A has coordinated with the Federal Bureau of Investigation (FBI) to publish Standard Operating Procedure (SOP) FO-003, which established guidance for the development, production, and coordination of I&A Terrorism Watchlist IIRs.

The Under Secretary for I&A (USIA) also issued an October 20, 2015 memorandum to all I&A and its field personnel approving them to "continue publishing IIRs on individuals that have records within the Terrorist Screening Database ("Terrorist Watchlist") and/or the Terrorist Identities Datamart Environment (TIDE).[1] The SOP and memorandum provide I&A field personnel clear guidance and authority to report terrorism and counterterrorism information as it applies to the Terrorist Watchlist and TIDE.

On June 24, 2016, I&A issued Policy Instruction IA-907, "Overt Human Intelligence Collection Program," which established the responsibilities, procedures, and requirements for the I&A Overt Human Intelligence (HUMINT) Collection (OHIC) Program. The key elements and responsibilities of IA-907 were to establish governance, training, and oversight of the OHIC program; define the authorized activities, eligible source types, and pre- and post-engagement processes; and describe I&A's source management storage, identification, and reporting processes. IA-907 codifies guidance for I&A personnel in the field to conduct overt human intelligence collection.

I&A, through the HSIC, also worked with DHS Intelligence Enterprise Components and updated existing DHS Policy Instruction 264-01-006, which articulates and streamlines processes for the production of IIRs throughout the Department. IIRs are the standard raw intelligence report through which terrorism and counterterrorism information is reported to the Intelligence Community. The Instruction was signed January 19, 2017. I&A is working on Policy Instruction IA-905, "Field Intelligence Report Program," which will codify processes pursuant to releasing intelligence and information reports relevant to DHS Component requirements and Departmental priorities. ECD: March 31, 2017.

---

[1], Memorandum from the Under Secretary for Intelligence and Analysis, "DHS Office of Intelligence and Analysis Publication of Terrorism Watchlist Intelligence Information Reports," October 20, 2015.

In addition, I&A is working on a DHS Instruction institutionalizing the process wherein DHS I&A ROs will work with DHS IE field elements to access intelligence information, gain an understanding of local context, deconflict reporting, and produce IIRs at the local level. ECD: September 30, 2017.

I&A will continue to explore additional guidance for intelligence reporting as necessary. I&A also continues to work with the FBI – both at the headquarters and field levels – to better coordinate intelligence reporting.

The DHS IFM for Collection and Reporting oversees an IE Board on behalf of the CINT that serves as the focal point for preparing IIM directives related to policies, procedures, and standards on integration of priority intelligence requirements, standardized intelligence reporting, and identifying appropriate training and certification for DHS field personnel.

Additionally, this integrated Board and subordinate working groups are standardizing training and procedures for RO which will enable Intelligence Components to quickly onboard ROs who can translate data of significant intelligence value into IIRs for release to the IC.

On August 26, 2016, the CINT signed a Departmental Intelligence, Surveillance and Reconnaissance (ISR) Plan, the implementation of which will establish ISR processes for tracking collection aligned to priority intelligence requirements focused on intelligence problems, gaps, targets, and essential elements of information. ECD: September 30, 2017.

Recommendation 6: Coordinate with the FBI to formalize guidance and policies for the reporting of terrorism and counterterrorism information.

Response: Concur. IA-507, "I&A Field Personnel," June 9, 2015, specifically authorizes I&A field personnel to provide operational support, incident response, outreach, and information sharing of terrorism and counterterrorism (CT) information with other federal partners across the country (e.g., FBI). DHS exchanges counterterrorism operational information and intelligence in several forms, including through FBI's embedded Liaisons in I&A. The FBI Liaisons participate in all intelligence briefings to the USIA and the Secretary, CT weekly meetings with the Secretary and senior staff and the CT Coordinator, and additionally has a seat at all DHS Counterterrorism Advisory Board meetings. When threat reporting warrants, DHS I&A and FBI schedule classified and unclassified calls and teleconferences with Joint Terrorism Task Forces, Field Offices, and Fusion Centers to disseminate the threat information and answer any questions from those entities.

Additionally, DHS coordinates with the National Counterterrorism Center and FBI through an interagency approved process regarding the issuance of National Terrorism Advisory System advisories. I&A and FBI coordinate on Joint Intelligence Bulletins to state, local, tribal and territorial partners. There is a need for more formal, written guidance for field personnel engaging between I&A and FBI field offices as it pertains to IIR production and dissemination. The I&A Field Operations Regional Directors now routinely engage with their respective Domestic Director of National Intelligence Representatives to discuss IIR production and dissemination in each region. I&A will also engage the DOJ and its FBI field offices to develop more formal, written guidance for I&A's field personnel engaging with their FBI counterparts as it pertains to IIR production and dissemination. ECD: September 30, 2017.

Recommendation 8: Develop and implement guidance for field officials granting them local release authority for intelligence products.

Response: Concur. On July 20, 2015, the USIA signed a decision memorandum titled "Interim Guidance Regarding Component Intelligence Program Release of Department of Homeland Security Intelligence Information Reports." The memorandum established the need and authority for establishing a field release capability, the criteria for nominating personnel to be releasers, and the processes for approving the nominated personnel.

Since the aforementioned memorandum, I&A has granted interim release authority to five individuals in FOD. Interim release authority has allowed personnel in the field to review, edit, and release IIRs in a more timely and efficient manner. Since January 2016, FOD has released all IIRs internally and without review by the I&A Reporting Branch. As of September of 2016, FOD releasers have released a total of 698 IIRs. We request that DHS OIG consider this recommendation resolved and closed.

The DHS OIG recommended that the DHS clearing offices:

Recommendation 7: Develop and implement a formal mechanism for reviewing and approving I&A intelligence products, including a process for logging and tracking products.

Response: Concur. I&A believes there is already a robust process in place for reviewing and approving its intelligence products, including systems for logging and tracking products. The review process has been in place since 2009. Several of the clearance offices also log and track products. For example, the Office of Privacy has tracked product review statistics since 2010 and the Office for Civil Rights and Civil Liberties (CRCL) has had a tracking system in place since October 2014. Furthermore, FOD has developed and hosted a tracking tool on an ODNI SharePoint platform for use by I&A personnel. The tool allows the FOD to track its IIRs, including the amount of time taken to process IIRs, the amount of time it takes for I&A to clear on IIRs, and other quality

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.

APPENDIX E: THE DEPARTMENT OF JUSTICE'S RESPONSE TO THE DRAFT REPORT[49]

U.S. Department of Justice

Washington, D.C. 20530

September 22, 2016

MEMORANDUM

TO: Michael Horowitz
Inspector General
U.S. Department of Justice

FROM: Carlos Felipe Uriarte
Associate Deputy Attorney General
Office of the Deputy Attorney General

John P. Carlin
Assistant Attorney General
National Security Division

Monty Wilkinson
Director
Executive Office for United States Attorneys

SUBJECT: Response: Joint Review of Domestic Sharing of Counterterrorism Information

The Department of Justice (DOJ or Department) appreciates the joint review undertaken by the Department's Office of the Inspector General (OIG), with the Inspectors General of the Intelligence Community and the Department of Homeland Security regarding the domestic sharing of counterterrorism information. Although this review included the Federal Bureau of Investigation (FBI), this response will not cover recommendations to the FBI. The report makes seven additional recommendations to the DOJ. We address these recommendations below, and concur with all seven.

49 Subsequent to DOJ's formal response, the language for recommendation #2 was revised as reflected in the body of the report. DOJ OIG discussed the revised language with DOJ. DOJ stated that it concurred with the revised recommendation and did not submit a new formal response.

Recommendation No. 1: The IC, DHS, and DOJ OIGs recommend that the ODNI, DHS, and DOJ: *(U//FOUO) Review the 2003 interagency Memorandum of Understanding (MOU) and determine what actions are necessary to update intelligence information sharing standards and processes among the departments.*

Response: Concur. The Department agrees to work through the interagency to review the 2003 interagency MOU and determine whether any actions are necessary to update intelligence information standards and processes among the departments as well as to consider potential updates to the 2003 interagency MOU.

Recommendation No. 2: The IC, DHS, and DOJ OIGs recommend that the ODNI, DHS, and DOJ: *(U//FOUO) Codify the designation of a single governance body for the terrorism-related Information Sharing Environment (ISE).*

Response: Concur. The Department agrees to work with the interagency to designate a single governance body for terrorism-related ISE.

Recommendation No. 10: The DOJ OIG recommends that DOJ: *(U//FOUO) Develop a comprehensive internal counterterrorism information sharing strategic plan based on a review of the President's strategic plan and in consultation with the relevant partners.*

Response: Concur. The Department agrees to develop a comprehensive internal counterterrorism information sharing strategic plan. As part of this process, the Department will review the President's strategic plan for counterterrorism information sharing and will consult will all relevant partners. In developing such a plan, the Department will rely on experts in the National Security Division, the U.S. Attorneys' offices (USAO), and the FBI, as well as the Department's Chief Information Officer.

Recommendation No. 11: The DOJ OIG recommends that DOJ: *(U//FOUO) Implement a council, led by a senior Department official, for the internal coordination of DOJ information sharing strategy and investments, and ensure that relevant components designate senior-level officials responsible for monitoring their component's efforts and communicating their efforts to DOJ as requested.*

Response: Concur. The Department agrees to implement a council, led by a senior Department official, for the internal coordination of DOJ information sharing strategy and investments, and ensure that relevant components designate senior-level officials responsible for monitoring their component's efforts and communicating their efforts to DOJ leadership as requested.

Recommendation No. 15: The DOJ OIG recommends that DOJ: *(U) Ensure that each USAO updates its ATAC Plan as required by the ATAC program.*

Response: Concur. As part of its evaluation of the ATAC program, DOJ will assess how frequently plans should be updated in the future and will ensure that ATAC plans are modified accordingly.

Recommendation No. 16: The DOJ OIG recommends that DOJ: *(U//FOUO) Evaluate the ATAC program to ensure the purpose of the ATAC meetings are not duplicative of other counterterrorism information sharing partner initiatives and are used in the most effective manner.*

Response: Concur. DOJ will evaluate the ATAC program to ensure the purpose of the ATAC meetings are not duplicative of other counterterrorism information sharing partner initiatives and are used in the most effective manner.

cc: Andrew McCabe, Deputy Director, Federal Bureau of Investigation
Lee Lofthus, Assistant Attorney General, Justice Management Division

APPENDIX F: THE FEDERAL BUREAU OF INVESTIGATION'S RESPONSE TO THE DRAFT REPORT

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

September 15, 2016

The Honorable Michael E. Horowitz
Inspector General
Office of the Inspector General
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530

Dear Mr. Horowitz:

The Federal Bureau of Investigation (FBI) appreciates the opportunity to review and respond to your office's report entitled, *Review of Domestic Sharing of Counterterrorism Information.*

We agree that it is important to provide additional guidance to field divisions and participating agencies regarding attendance at and the structure of JTTF Executive Board meetings. We also agree it is important to provide guidance to the field in regards to counterterrorism-related TRP sessions. In that regard, we concur with your five recommendations for the FBI.

Should you have any questions, feel free to contact me. We greatly appreciate the professionalism of your audit staff throughout this matter.

Sincerely,

James C. Langenberg
Section Chief
External Audit and Compliance Section
Inspection Division

Enclosure

The Federal Bureau of Investigation's Response to the Joint Review of Domestic Sharing of Counterterrorism Information

Report Recommendation #12: Require FBI field divisions to stress to participating agencies the importance of designating an individual and an alternate to serve as their representatives to the JTTF Executive Board, as well as of regularly attending the meetings.

FBI Response to Recommendation #12: Concur. The FBI will instruct FBI field divisions to emphasize to participating agencies the importance of designating an individual and an alternate to serve as their representatives to the JTTF Executive Board, as well as of regularly attending meetings.

Report Recommendation #13: Ensure FBI field divisions encourage agencies that do not participate on the JTTF, including first responders, to attend JTTF Executive Board meetings.

FBI Response to Recommendation #13: Concur. Consistent with security policy requirements, the FBI will work with the FBI field divisions to encourage agencies that do not participate on the JTTF, including first responders, to attend JTTF Executive Board meetings.

Report Recommendation #14: Identify an appropriate structure and content of JTTF Executive Board meetings that FBI field divisions should use at minimum when conducting these meetings.

FBI Response to Recommendation #14: Concur. The FBI will review and determine how to refine the general structure of the JTTF Executive Board meetings that FBI field divisions should use at minimum when conducting meetings.

Report Recommendation #17: We recommend that the FBI direct FBI field divisions to identify and invite key stakeholders to TRP sessions.

FBI Response to Recommendation #17: Concur. The FBI will create guidance instructing FBI field divisions to identify and invite key stakeholders to counterterrorism TRP sessions.

Report Recommendation #18: Determine the agencies with which it should share its counterterrorism-related TRP results and implement a process to ensure the TRP results are appropriately shared with those agencies on a systemic and regular basis.

FBI Response to Recommendation #18: Concur. The FBI will create guidance to determine which agencies it will share the counterterrorism-related TRP results and will establish a process to ensure the TRP results are appropriately shared with those agencies on a systemic and regular basis.