



THE FEDERAL BUREAU OF INVESTIGATION'S FOREIGN TERRORIST TRACKING TASK FORCE

U.S. Department of Justice
Office of the Inspector General
Audit Division

Audit Report 13-18
March 2013

REDACTED – FOR PUBLIC RELEASE

AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S FOREIGN TERRORIST TRACKING TASK FORCE

EXECUTIVE SUMMARY*

The Federal Bureau of Investigation's (FBI) Foreign Terrorist Tracking Task Force (FTTTF) supports the FBI's National Security Branch in the detection, identification, tracking, and assessment of individuals and entities that pose threats to the United States and its interests. The FTTTF conducts in-depth analyses using various government and public source datasets to identify and track terrorist and national security threats and provides intelligence on these threats to FBI field offices, headquarters sections, and intelligence community partners. As of the end of fiscal year (FY) 2011, the FTTTF had access to [REDACTED] different datasets containing [REDACTED] records. In FY 2011 the FTTTF examined information relating to [REDACTED] individuals, resulting in the dissemination of [REDACTED] leads on potential national security threats.

The OIG performed this audit to determine if the FBI: (1) has implemented a viable FTTTF strategy to locate and track suspected terrorists and their supporters, including coordination with FBI headquarters and field offices to enhance national security investigations; and (2) is following Department of Justice (DOJ) privacy policies in its management of information.

We determined that the FBI has implemented a strategy that provides significant value to the FBI by performing in-depth analyses that proactively identify national security threats and assist ongoing national security investigations. For example, the FTTTF has assisted the Counterterrorism Division in locating and tracking suspected terrorists and their supporters. Many agents and analysts described the FTTTF's information as valuable and stated that FBI field offices do not have resources available to conduct that level of detailed and thorough analysis on large amounts of data. In addition, the FTTTF partners with other government agencies to obtain data, conduct analysis, and provide investigative information to assist these agencies in detecting national security threats.

We found limited coordination between the FTTTF and National Security Branch operational divisions prior to FY 2011. However, the FTTTF

* The FBI identified within the full version of this report classified and other information that if released publicly could compromise national security interests and the FBI's operations. To create this public version of the report, the Office of the Inspector General redacted (blacked out) these portions of the full report.

has worked to improve its coordination with the entire National Security Branch, especially within the Counterterrorism Division. Specifically, FTTTF personnel have been assigned to one of the Counterterrorism Division's operational sections, which has enhanced communication and helped the FTTTF provide more valuable support to assist the FBI's counterterrorism efforts. Working side-by-side with their operational counterparts, the FTTTF assignees become aware of the Counterterrorism Division's intelligence gaps and the latest information on emerging threats and are, in turn, able to suggest how the FTTTF can help address those threats and gaps. The FTTTF assignees also initiated the updating of threat assessment criteria used on an existing FTTTF project, the criteria for which had not been updated for an extended period of time. Thus, these FTTTF assignees have proven valuable in supporting this Counterterrorism Division section's national security activities. We believe that the FBI could benefit from additional FTTTF personnel serving as liaisons to other National Security Branch operational divisions.

However, we identified areas for which we believe the FTTTF can improve its operations. We found that due to various contributing factors, the FTTTF did not always provide FBI field offices with timely and relevant information. For instance, FTTTF officials stated that one project was hindered in its ability to provide timely information to field offices. [REDACTED]

Further, field office personnel told us that they believed that some leads received from the FTTTF contained [REDACTED] information that may not assist them in their investigations. This could occur because FTTTF analysis includes searching data within the FBI case management system and this information may have been originally developed by field offices. We understand that the FTTTF cannot assume that a field office is aware of all the information relating to a specific subject, and that it is better to have instances of [REDACTED] information than to assume that a field office is aware of the threat. To minimize the potential of the FTTTF providing [REDACTED] information, one suggestion from field office personnel was for the FTTTF to add investigative context to its leads, such as why FTTTF analysts believe the link between information already contained in FBI systems might enhance an ongoing investigation. Another suggestion was to assign to the FTTTF additional agents who understand the type of information that is most useful to field offices. The FTTTF workforce primarily consists of analysts and contractors, and as acknowledged by FTTTF personnel, these individuals are subject-matter experts on analyzing data, not investigating cases. Nonetheless, time and resources are not used

optimally when field offices address [REDACTED] leads. We believe the FTTTF should take additional measures to ensure that information provided to field offices is timely, relevant, and valuable.

In addition, we determined that the FTTTF's outreach efforts to the field offices can be improved, as many field office agents and analysts in the three field offices we visited were not fully aware of the FTTTF's capabilities. These agents and analysts respond to information and leads disseminated by the FTTTF. However, because these individuals do not have a comprehensive understanding of the FTTTF's support role and its potential use by field offices, the FTTTF's valuable analytical capabilities may not be used to the fullest extent possible to help further the FBI's national security mission. In the past, the FTTTF provided on-site capabilities briefings to field offices. Limited funding and other resources have prevented the FTTTF from traveling to conduct these briefings. While we understand that the FTTTF may not be able to travel to every field office to brief FBI personnel on its capabilities, we believe the FTTTF should develop other methods to provide field offices with information about the FTTTF's capabilities and resources.

We found that the FTTTF has difficulty tracking investigations opened as a result of FTTTF support and that the FTTTF's process for assessing the utility of information disseminated to field offices can be improved. FTTTF officials explained that while the FTTTF requests a response to the information provided to field offices, in some instances no feedback is provided and FTTTF personnel often spend additional time and resources to determine the value of the information and assistance provided. The FTTTF cannot ensure that field offices review information sent if a response is not provided. We believe the FTTTF should meet with National Security Branch officials to determine how field offices can respond to FTTTF leads in an efficient manner that is not burdensome for field office personnel. Additionally, responses from field office personnel do not always indicate the usefulness or effectiveness of FTTTF analysis. We believe the FTTTF should develop a method by which to help understand the utility of information provided to field offices to determine its effectiveness in supporting the mission of the National Security Branch.

The FTTTF has implemented many privacy-related policies and procedures to ensure it meets DOJ's requirements for handling information. The FTTTF's privacy oversight and management is strengthened by the utilization of an assigned Office of General Counsel attorney. This representative ensures FTTTF personnel complete annual privacy training, validates FTTTF's adherence to privacy policies for conducting searches, and verifies compliance of FTTTF programs and datasets with DOJ and FBI

privacy policies. Both the former FTTTF Director and the Office of General Counsel attorney stated that the FTTTF has not encountered any privacy-related issues or problems.

According to officials in DOJ's Office of Privacy and Civil Liberties (OPCL), in FY 2008 the Acting DOJ Chief Privacy and Civil Liberties Officer gave the FTTTF conditional approval of its Privacy Impact Assessment. However, the FBI was informed by the Acting DOJ Chief Privacy and Civil Liberties Officer that in order to increase transparency, the FTTTF needed to submit a System of Records Notice for its FTTTF information systems in order for the Privacy Impact Assessment to be fully approved. According to the FBI and OPCL, officials disagreed about the approach to be taken in responding to this requirement. As a result, the FBI and OPCL continued to hold discussions throughout FY 2009 regarding this requirement, and the FBI did not submit a System of Records Notice for FTTTF systems at that time. In FY 2011 the FBI submitted the System of Records Notice, which received final approval in July 2012.

Our audit resulted in seven recommendations to improve FTTTF support provided to field offices and the National Security Branch, including assigning additional FTTTF liaisons throughout the Counterterrorism Division; ensuring FTTTF information provided to field offices is timely and relevant; and establishing increased communication and coordination options between the FTTTF, field offices, and the National Security Branch.

**AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S
FOREIGN TERRORIST TRACKING TASK FORCE**

TABLE OF CONTENTS

INTRODUCTION.....	1
FTTTF History	1
FTTTF Organizational Structure.....	2
FTTTF Datamart.....	3
FTTTF Projects.....	4
OIG Audit Approach	7
FINDINGS AND RECOMMENDATIONS	9
I. Strategy Implementation.....	9
Supporting the FBI's National Security Mission	9
Effectiveness of FTTTF Information	11
FTTTF Awareness and Coordination	15
Tracking FTTTF Performance	20
Recommendations	24
II. Information and Privacy Management.....	26
FTTTF Information Management	26
Privacy Requirements for the FBI's Information Systems	28
Recommendation	30
STATEMENT ON INTERNAL CONTROLS	31
STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS	32
APPENDIX I: OBJECTIVES, SCOPE, AND METHODOLOGY	33
APPENDIX II: FTTTF UNITS	35
APPENDIX III: FEDERAL BUREAU OF INVESTIGATION RESPONSE..	37
APPENDIX IV: OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE REPORT	41

INTRODUCTION

The Federal Bureau of Investigation's (FBI) Foreign Terrorist Tracking Task Force (FTTTF) identifies and tracks terrorist and national security threats against the United States by conducting in-depth analyses using various datasets. These datasets generally are stored in the FTTTF Datamart, a collection of data gathered from multiple government and non-government sources. The Datamart includes information obtained from the FBI's Investigative Data Warehouse, the primary analytic data repository containing FBI case file and investigative data. The FTTTF provides the results of its in-depth analyses to FBI field offices and headquarters sections to help locate and track suspected terrorists and their supporters, as well as national security threats. Field offices and headquarters sections have the discretion to use the FTTTF's information to initiate or advance on-going national security-related investigations.

FTTTF History

The FTTTF was established by Homeland Security Presidential Directive-2 (HSPD-2), which was signed on October 29, 2001. Specifically, HSPD-2 directed the Attorney General with assistance from other officers of the government, as appropriate, to establish the FTTTF to ensure that federal agencies coordinate programs to: (1) deny entry into the United States of aliens associated with, suspected of being engaged in, or supporting terrorist activity; and (2) locate, detain, prosecute, or deport any such aliens already present in the United States.

In 2002, the Attorney General signed a memorandum that ordered the FBI to assume responsibility of the FTTTF within the Counterterrorism Division. While the FBI maintains exclusive responsibility for the FTTTF, it still utilizes a multi-agency operating environment similar to what existed prior to the Attorney General assigning authority of the FTTTF to the FBI. In addition to partnering with intelligence community agencies to coordinate data sharing, the FTTTF maintains relationships with other government agencies to develop projects that address common threats and identify gaps in intelligence gathering. Moreover, liaisons from the Department of Defense (DoD), Department of Homeland Security (DHS), the National Geospatial Intelligence Agency, and the Central Intelligence Agency work on-site at the FTTTF to assist in data analysis, which helps the FTTTF to better understand the non-FBI data and facilitates access to additional datasets maintained outside the FBI.

In 2006, the FBI identified unmet analytical and technical needs within its National Security Branch and determined that the FTTTF could fill this gap

by establishing the National Security Analysis Center. As a result, the FTTTF incorporated the National Security Analysis Center and expanded its role to support the other National Security Branch operational divisions in the detection, identification, and tracking of individuals or entities that pose threats to the United States and its interests. The FTTTF now coordinates with not only the Counterterrorism Division but also with the FBI's Counterintelligence Division and the Weapons of Mass Destruction Directorate.

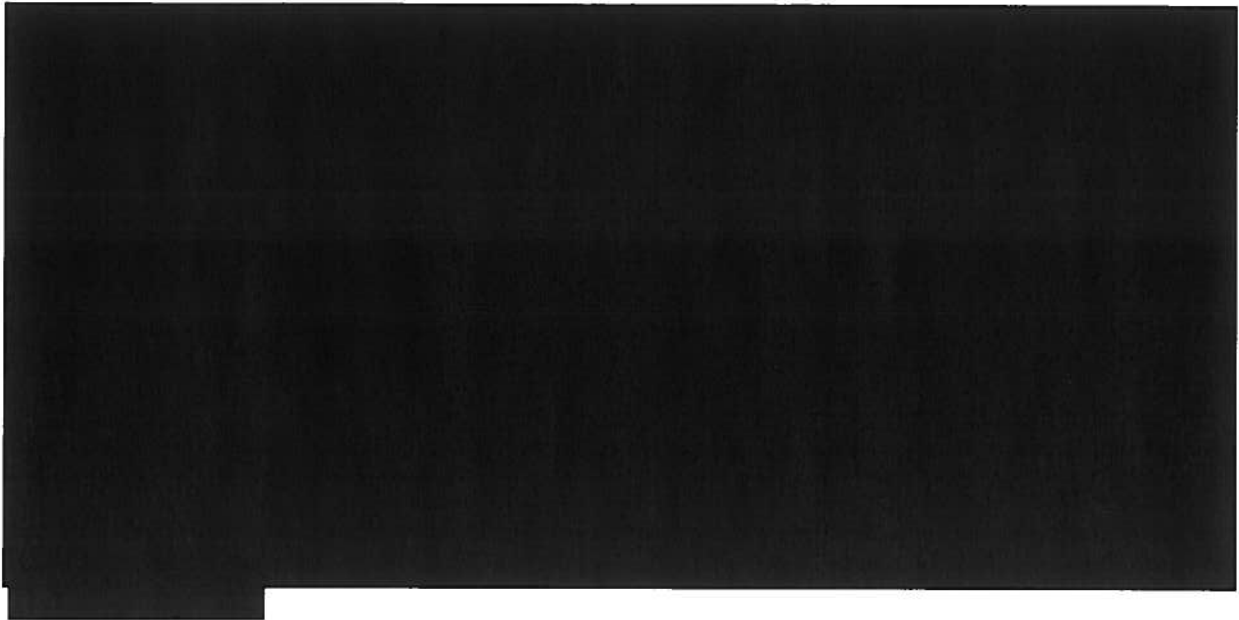
FTTTF Organizational Structure

The FTTTF is led by a Director at the Section Chief-level who reports to the Assistant Director of the FBI's Counterterrorism Division through the Deputy Assistant Director for the Operational Support Branch. The FTTTF has approximately 360 staff members comprised of FBI personnel, intelligence community employees, and contractors. In FY 2012, the FTTTF's budget was \$54.4 million.

The FTTTF is divided into two components – Operations and Operational Support.

The Operational Support component is comprised of three

EXHIBIT I-1
FTTTF ORGANIZATIONAL CHART



FTTTF Datamart

The FTTTF analyzes large sets of data and then provides resulting detailed information in a manageable and useful format to FBI field offices and headquarters units, as well as intelligence community partners, to assist in national security operations. The FTTTF's Datamart contains data from FBI systems, intelligence community partner databases, and public source datasets. According to the FTTTF, utilizing data from many sources helps the FTTTF to "follow terrorists' electronic footprints."

Since its inception and in coordination with intelligence community partners, the FTTTF has gained access to and utilizes [REDACTED] different datasets totaling [REDACTED] records. [REDACTED]

1

1

FTTTF Projects

The FTTTF conducts analyses on counterterrorism subjects and national security threats through the use of over 40 unique projects, as well as ad hoc projects based on requests from headquarters sections and field offices. On each of these projects, the FTTTF primarily initiates Type III Threat Assessments prior to conducting analysis. According to the FBI's Domestic Investigations and Operations Guide, Type III Threat Assessments are used to perform analysis with the intent to identify, obtain, and utilize information about actual or potential national security threats or federal criminal activities, or the vulnerability to such threats or activities. A Type III Assessment allows the FBI to collect information, often based on a predicated threat, that may lead to potential targets, threats, or vulnerabilities. According to FTTTF officials, the FTTTF operational units are responsible for updating the respective threat assessment files for each of their projects because FTTTF analysts are conducting the searches on the FTTTF Datamart and disseminating leads and targeting packages to field offices and headquarters sections. The general process followed by FTTTF operational units for each project is depicted below in Exhibit I-2.

EXHIBIT I-2
OVERVIEW OF THE FTTTF GENERAL PROJECT PROCESS



Source: OIG Analysis of FBI Information

For this audit, we selected four specific FTTTF projects to review in detail: (1) the Traveler Assessment project, (2) the Finding Terrorists in the United States (FINDUS) project, (3) the Scarecrow project, and (4) the Amon project, all of which are discussed in detail in the following sections. These projects are managed by different FTTTF operational units and have unique focuses, such as one project pertaining to the identification of unknown counterterrorism subjects and another concentrating on domestic terrorism threats. [REDACTED]

Traveler Assessment Project

The FTTTF established the Traveler Assessment Project in 2005 to help identify and assess unknown individuals who may have links to terrorism. [REDACTED]

3

4

3

4

FINDUS Project

The FTTTF [redacted] Unit manages the FINDUS project, which is used to determine the undetected presence of known or suspected terrorists [redacted]

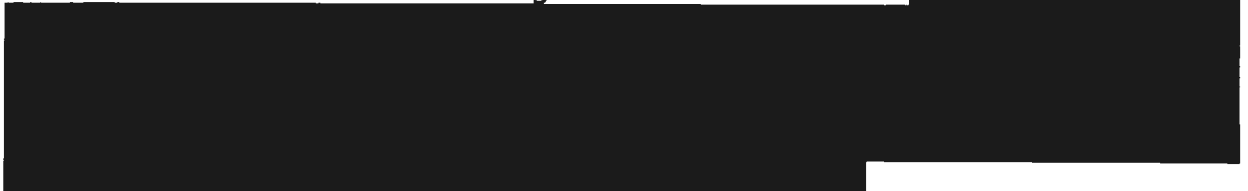


Scarecrow Project

FTTTF's National Security Analysis Center runs the Scarecrow project.



The Sovereign Citizen Movement in the United States is comprised of United States citizens who openly reject their United States citizenship status and claim to exist beyond the realm of government authority, including courts, taxing entities, motor vehicle departments, and law enforcement. Affiliates may use this self-appointed status to justify threats, violence, or crime, including theft and fraud. The National Security Analysis Center's Scarecrow project focuses solely on the financial schemes of the Sovereign Citizen movement.



Amon Project

In 2009, the FTTTF's National Security Analysis Center developed a centralized process to enhance the FBI's response to national counterintelligence security threats [REDACTED]

5

OIG Audit Approach

The objectives of this audit were to determine if the FBI: (1) has implemented a viable FTTTF strategy to locate and track suspected terrorists and their supporters, including coordination with FBI headquarters and field offices to enhance national security investigations; and (2) is following DOJ privacy policies in its management of information.

To accomplish these objectives, we interviewed 41 individuals from within the FTTTF, the Counterterrorism Division, the Counterintelligence Division, the Weapons of Mass Destruction Directorate, and the Office of General Counsel. We also interviewed officials from the DOJ Office of Privacy and Civil Liberties about DOJ's privacy policies and procedures.

As previously mentioned, we selected four FTTTF projects on which to focus our review. We observed the processes to determine how FTTTF personnel conduct analyses on each of these projects. We also conducted site visits at FBI field offices in Chicago, Illinois; New York, New York; and Phoenix, Arizona, to determine field office awareness of the FTTTF, as well as their communication and coordination with the FTTTF on the associated projects.

The results of our review are detailed in Findings I and II. Finding I provides our analysis of the FTTTF's strategic goals and performance

measures, as well as our assessment of the FTTTF's coordination and outreach with FBI field offices and headquarters sections. Finding II details the FTTTF's privacy policies and adherence to the DOJ's privacy regulations pertaining to the Privacy Act and E-Government Act. Further information on the audit objectives, scope, and methodology is contained in Appendix I.

FINDINGS AND RECOMMENDATIONS

I. Strategy Implementation

We believe the FTTTF has implemented a strategy that provides significant value to the FBI by performing in-depth analyses that proactively identify national security threats and assist ongoing national security investigations. In FY 2011, the FTTTF reviewed over [REDACTED] individuals to provide [REDACTED] leads to field offices, headquarters entities, and intelligence community partners. However, FTTTF officials described a [REDACTED] in some of the data it analyzes, and field office personnel explained instances of receiving [REDACTED] or what appeared to be [REDACTED] information from the FTTTF. Although the FTTTF has taken many steps to coordinate with National Security Branch components, we believe certain components, such as the Counterintelligence Division and the Weapons of Mass Destruction Directorate, could benefit from increased communication and coordination from the FTTTF in the form of having FTTTF assignees similar to those assigned to the Counterterrorism Division. We also found field office personnel lacked awareness of the FTTTF's capabilities, and we believe these employees could better utilize FTTTF assistance with an increased awareness of the FTTTF's capabilities to support investigations and identify unknown national security threats. Moreover, we determined that the FTTTF's process for assessing the utility of information disseminated to field offices can be improved.

Supporting the FBI's National Security Mission

When the FTTTF was established within the FBI's Counterterrorism Division in 2002, its strategy was solely focused on assisting counterterrorism efforts to detect and track foreign terrorists and their supporters in the United States. Therefore, the FTTTF only provided support to the FBI's international terrorism program. In 2006, the FBI, with legal assistance from DOJ, conducted an assessment to determine how the FTTTF's services could be expanded to support the entire National Security Branch, with particular interest as to how current FTTTF operations, expertise, and technology efforts could be leveraged in this regard. It was determined that the National Security Branch could utilize the FTTTF's successful data exploitation and bulk data analysis techniques to support all National Security Branch components in the detection, identification, tracking, and assessment of individuals and entities that pose threats to the

United States and its interests. FTTTF operations now support the FBI's counterterrorism efforts (both international and domestic terrorism), as well as counterintelligence and weapons of mass destruction efforts. The National Security Branch benefits from the implementation and utilization of FTTTF tools, data, projects, and practices, including domain mapping and geospatial analysis.

We found that the FTTTF provides the FBI's National Security Branch with in-depth and comprehensive data analysis, which allows operational personnel to devote their time and resources to conducting investigations. According to the FBI, since [REDACTED] [REDACTED] different datasets containing [REDACTED] records. In FY 2011, the FTTTF reported that it examined information relating to [REDACTED] individuals, resulting in the dissemination of [REDACTED] leads to FBI field offices, headquarters sections, and intelligence community partners. Additionally, through the information provided in these leads the FBI opened [REDACTED] national security investigations.

Counterterrorism Division personnel stated that the FTTTF has an expertise that assists the Counterterrorism Division in fulfilling its mission by providing a wealth of information to FBI headquarters sections, field offices, and intelligence community partners. Also, many field office agents and analysts expressed praise for the information provided by the FTTTF, stating that this information is worthwhile and relevant. For example, the Chicago Field Office used information from an FTTTF Scarecrow lead that resulted in the identification of another individual associated with the Sovereign Citizen movement. Further, field office personnel acknowledged that the FTTTF is able to perform FBI-wide searches and analyses that field offices generally do not conduct. For example, a New York City Field Office case agent described an instance in which the FTTTF linked a subject within the New York City Field Office's jurisdiction to an ongoing investigation in another field office. This case agent stated that this connection would not have been made without the FTTTF's support.

Of the four projects we reviewed, the Amon project was the most widely praised among FBI personnel. Many field office agents and analysts explained that National Security Analysis Center was open to new ideas and described a good working relationship between the field offices and the FTTTF. According to FTTTF personnel, the Amon project efficiently and effectively analyzes large datasets on multiple individuals and saves field office personnel valuable time and resources. Documentation provided by the National Security Analysis Center indicated that it takes approximately 1 week for 4 to 5 FTTTF analysts to perform the Amon project analyses on thousands of individuals for 32 field offices every month using its batched

data processing techniques. This unit estimated that it would have taken 25 field office analysts over 6 months to perform these same analyses individually. Field office analysts explained that the value of the FTTTF comes not only in the information provided but also in the time and resources saved at the field office level, as analysts would not be able to perform the high volume of searches without assistance from the FTTTF.

The FTTTF also partners with other government agencies to coordinate data sharing and to develop projects that address common threats and identify intelligence gaps. [REDACTED]

[REDACTED] The project also assists the National Joint Terrorism Task Force by providing leads on possible subjects of interest.⁶ We believe the FTTTF's ability to coordinate its efforts not only with internal FBI entities but also with intelligence community partners to track and detect national security threats provides significant value to the FBI.

Effectiveness of FTTTF Information

During our review we found that although the FTTTF provides valuable information to field offices and headquarters entities, the effectiveness of this information is diminished when it is not new or timely. There have been contributing factors, including instances of [REDACTED] and the availability of relevant information, that have hindered the FTTTF's ability to provide timely information to field offices. Further, field offices believe to have received [REDACTED] that did not assist them in their investigations.

[REDACTED]

We found that the FTTTF did not always provide FBI field offices with timely and relevant information. Sending field offices leads that contain

⁶ The National Joint Terrorism Task Force was established in 2002 to manage the FBI's Joint Terrorism Task Forces through which local, state, and federal agencies work together to combat terrorism on a regional scale.

[REDACTED] information can result in an inefficient use of field office resources. For example, the FBI may miss the opportunity to open an investigation on a known or suspected terrorist residing in the United States or to further help field offices deter threats against national security because the individual departed the United States before or soon after the FTTTF completed its analysis and forwarded the lead to the field office.

FTTTF officials stated that certain projects were operating with [REDACTED] This contributed to the FTTTF disseminating [REDACTED] information for the Traveler Assessment project. [REDACTED]

In addition, as of [REDACTED] the Amon project operated with a [REDACTED] time and was analyzing records from [REDACTED].

According to FBI officials, the Amon project intentionally [REDACTED] on its analysis based on consultation with the Counterintelligence Division. Because the Amon project evaluates [REDACTED] in the United States.

FTTTF officials explained that the [REDACTED] on the Traveler Assessment project is due, in part, to competing priorities and circumstances that [REDACTED], such as when special requests or new threats arise. If a special project is initiated based on an immediate threat to national security, FTTTF analysts are pulled from their daily workload to assist on the special project.

[REDACTED] For example, [REDACTED] the Traveler Assessment project began conducting analyses on [REDACTED]. As part of this process, the analysts performed [REDACTED]

[REDACTED] As a result, the analyses of [REDACTED] We recognize that resources must be redirected to address immediate threats and special projects. However, the FTTTF must ensure that [REDACTED] are monitored and kept at a manageable level. We believe that the FTTTF cannot provide optimal support to field offices and headquarters sections while [REDACTED]

While onsite at the Chicago Field Office, we learned of a lead that [REDACTED]
Through its Traveler Assessment project, the [REDACTED]
Unit conducted analysis on [REDACTED]
[REDACTED] The [REDACTED] Unit provided
the resulting lead to the Chicago Field Office on [REDACTED]. The
Chicago Field Office began addressing the lead on [REDACTED], and
found that the subject had left the United States on [REDACTED]. We
believe that if the [REDACTED] Unit had been
[REDACTED], the Chicago Field Office would have received
the information [REDACTED]

Another contributing factor to the FTTTF providing [REDACTED]
[REDACTED] is the availability of [REDACTED] FTTTF
officials explained that individuals [REDACTED]
[REDACTED] As a result,
[REDACTED]
used at the time of the FTTTF's analysis.

While at the Phoenix Field Office, we learned about another instance in
which the FTTTF provided a field office with [REDACTED]
[REDACTED], to the Phoenix
Field Office indicating that [REDACTED] in the Phoenix Field Office's
area of responsibility. However, when the Phoenix Field Office addressed
the lead on [REDACTED], additional research by a field agent revealed
[REDACTED].
Therefore, the FTTTF lead contained [REDACTED],
and the Phoenix Field Office was unable to determine the individual's nexus
to terrorism.

While we understand that some [REDACTED] is necessary to conduct
worthwhile and relevant analysis, such as on the Amon project, the work
performed by the FTTTF becomes [REDACTED]
[REDACTED] As previously mentioned, in [REDACTED], FTTTF officials
stated that the Traveler Assessment project had a [REDACTED] and
was [REDACTED]. The FTTTF is looking for ways
to [REDACTED], such as adding [REDACTED], thereby
decreasing the [REDACTED]. We believe the FTTTF
should continue to work on minimizing the dissemination of [REDACTED]

[REDACTED], including implementing a strategy and procedures [REDACTED]
[REDACTED]
[REDACTED]

We also found instances of field offices receiving [REDACTED]. An FTTTF Unit Chief explained that FBI case agents are responsible for tracking and updating case file information in the FBI's case management system and in Guardian, the FBI's threat tracking system. Because the FTTTF Datamart searches these FBI systems, FTTTF analysts may include field office-generated investigative information in the leads developed and sent to a field office. However, this official further stated that the FTTTF cannot assume a field office is already aware of all the information relating to that individual. Moreover, an FTTTF official explained that the lead document includes a paragraph discussing the potential for the lead to include [REDACTED].

Field agents believed that some FTTTF leads can be [REDACTED] in nature. Three Supervisory Special Agents stated that they have received information from the FTTTF of which their field office was already aware. For example, the Phoenix Field Office received an FTTTF lead based on detailed telephone records. However, according to a field office manager, the Phoenix Field Office had input that telephone record information into an FBI system, which the FTTTF then analyzed. This field office manager believed that, as a result, the FTTTF provided a lead to the Phoenix Field Office based upon analysis the field office had performed and for which the field office was already aware.

To minimize the potential of the FTTTF providing [REDACTED], field office personnel recommended that the FTTTF run a final check to see if there are any changes to the information before sending the leads to field offices. In addition, field office supervisors proposed that the FTTTF add investigative context to information in its leads, such as why FTTTF analysts believe the link between information already contained in FBI systems might enhance an ongoing investigation, to help prevent the receipt of [REDACTED]. One suggestion was to assign to the FTTTF additional agents who are familiar with conducting FBI investigations and who understand the type of information that is most useful. The FTTTF workforce primarily consists of analysts and contractors, and as acknowledged by FTTTF personnel, these individuals are subject-matter experts on analyzing data, not investigating cases.

We understand that the FTTTF cannot assume that a field office is aware of all the information relating to a specific subject, and that it is better

to have instances of [REDACTED] than to assume that a field office is aware of the threat. However, we believe the FTTTF could take additional measures to ensure that information provided to field offices is timely, relevant, and valuable. Therefore, we recommend that the FTTTF evaluate its procedures and determine a more effective way to ensure that information provided is not [REDACTED].

FTTTF Awareness and Coordination

For the FTTTF to continue to provide effective assistance in addressing national security threats, we believe it is important for the FBI's National Security Branch operational divisions and field offices to be aware of the FTTTF's capabilities and for the FTTTF to coordinate with these components. At the headquarters level, Counterterrorism Division, Counterintelligence Division, and Weapons of Mass Destruction Directorate officials were aware of the FTTTF and its capabilities and described various coordination efforts. However, field offices were less aware of the full extent of the FTTTF's support functions.

Headquarters Outreach

As part of the FTTTF's strategy to coordinate efforts within the FBI, we found that it maintains a close working relationship with the National Security Branch's operational divisions, particularly the Counterterrorism Division. FTTTF personnel are subject-matter experts on obtaining and examining data, but they do not have the appropriate operational expertise to determine whether accurate and up-to-date search criteria are used in analyzing information on particular threats. Therefore, FTTTF personnel must coordinate with the subject-matter experts in the FBI's operational divisions to identify intelligence gaps, establish search criteria, and ensure it is effectively supporting national security investigations.

In FY 2011, the Counterterrorism Division enhanced the coordination between these operational subject-matter experts and the FTTTF through the assignment of FTTTF personnel to the Counterterrorism Division Strategic Operations Section's fusion cells.⁷ According to the former FTTTF Director, the assignees serve to translate Counterterrorism Division needs into FTTTF analytical capabilities and fill investigative and intelligence gaps. The operational subject-matter experts, in turn, advise the FTTTF assignees

⁷ [REDACTED]

of the changing national security threats. For example, fusion cell assignees have assisted with updating the threat assessment criteria used in FTTTF analyses to be timely and relevant.

The Unit Chief of the [REDACTED] Unit explained that the threat assessment for the Traveler Assessment project is updated every 90 days in accordance with the FBI's Domestic Investigations and Operations Guide. We found that threat assessment updates reflected project statistics and successes, as well as action items for the Counterterrorism Division to review the current [REDACTED] and provide changes to the [REDACTED] Unit, as needed. However, we also found that changes or updates to the threat criteria were rarely made by the Counterterrorism Division. In fact, the [REDACTED] on which the Traveler Assessment project conducted analyses, as well as the [REDACTED], had not been updated for an extended period of time. As a result of the lack of updates to the threat assessment criteria, the FTTTF may have been performing searches based on extraneous criteria.

Within months of FTTTF personnel being assigned to the fusion cells, an initiative was completed to update the threat assessment and search criteria for the Traveler Assessment project. [REDACTED]

[REDACTED] According to a FTTTF official, without the coordination in the fusion cells, the Counterterrorism Division did not update the criteria used to conduct searches within the Traveler Assessment project, and therefore, we believe that the FTTTF may have been providing field offices with traveler threat information that was not consistent with the FBI's current threat picture. We believe the FTTTF should establish a system or procedure to ensure the Counterterrorism Division and the FTTTF coordinate to update threat criteria in a timely manner for all applicable projects.

In addition to providing FTTTF assignees to the Counterterrorism Division's fusion cells, the FTTTF Director attends daily and weekly meetings with Counterterrorism Division senior management to promote the FTTTF's support capabilities and to gain insight into the FBI's current terrorism-related threats and intelligence gaps. At times, these meetings result in the FTTTF being tasked with a specific assignment, while at other times the FTTTF Director might suggest or initiate additional tasks to further support the FBI's national security efforts based on information presented during these meetings.

The FTTTF Assistant Section Chief of Operations also participates in a daily meeting with managers of the Counterterrorism Division's operational units. These meetings afford the FTTTF the ability to obtain relevant threat information and, in turn, ensure the FTTTF's projects are focusing on the most relevant threats. The FTTTF also provides reports to Counterterrorism Division headquarters sections to highlight FTTTF capabilities and successes, including leads generated, investigations initiated, and project descriptions.

Despite having personnel assigned to the fusion cells and communication between the FTTTF and Counterterrorism Division management, we believe more communication and routine discussions on threats and intelligence needs can further the FBI's counterterrorism mission. As previously stated, the Counterterrorism Division had not updated search criteria for threat assessments for a significant period of time prior to the assignment of FTTTF employees to the fusion cells. We believe increased communication between the FTTTF and other Counterterrorism Division operational units could help ensure the FTTTF's projects address relevant national security threats. Further, FTTTF personnel have not been assigned to any other Counterterrorism Division sections. We believe that the FTTTF and other Counterterrorism Division sections can benefit from additional FTTTF personnel serving in a liaison role to improve communication and coordination. Counterterrorism Division officials agreed with our view on the benefit of assigning FTTTF personnel to Counterterrorism Division operational units to further expand FTTTF's support capabilities.

As previously stated, the FTTTF is organizationally aligned within the Counterterrorism Division. While the FTTTF provides support to the Counterintelligence Division and Weapons of Mass Destruction Directorate, these components do not have authority over the FTTTF to direct its projects or practices. While these components are not staffed with FTTTF assignees, Counterintelligence Division and Weapons of Mass Destruction Directorate officials stated that they have a good working relationship with the FTTTF and are pleased with the support it provides. For example, according to a Counterintelligence Division Unit Chief, the Counterintelligence Division works with the FTTTF as new threats emerge to update the Amon project's [REDACTED]

However, we believe the Counterintelligence Division and the Weapons of Mass Destruction Directorate would further benefit from increased, direct coordination with the FTTTF, similar to the FTTTF's coordination within the Counterterrorism Division through the fusion cell assignees and daily management meetings. This coordination would allow the Counterintelligence Division and Weapons of Mass Destruction Directorate to

provide a better opportunity for the FTTTF to meet those components' needs, as assignees would advise these components on how FTTTF analytic capabilities can help fill counterintelligence and weapons of mass destruction investigative and intelligence gaps. The success of the FTTTF assignees to the Counterterrorism Division's fusion cells has shown that daily interaction with FTTTF personnel can help close intelligence gaps, such as maintaining and updating threat assessment criteria. We believe the FBI should consider additional means to enhance routine, operational-level interaction to help ensure that the FTTTF is providing optimal support to these other components' efforts on addressing national security matters. According to the FBI, the FTTTF currently does not have sufficient resources to use in this way. However, the FBI is interested in expanding its use of FTTTF assignees.

Field Office Outreach

[REDACTED]

The FTTTF has a dedicated unit to promote the FTTTF's capabilities and assess the performance of the FTTTF. The [REDACTED] Unit facilitates internal coordination between FTTTF units and manages and develops external communication and collaboration with field offices, other FBI divisions, and the intelligence community. [REDACTED] Unit collects and reports on FTTTF operational metrics, such as the number of leads sent to field offices.

One method used by the [REDACTED] Unit to inform the field offices of FTTTF capabilities is to provide information briefings about the FTTTF.⁸ Staff from the [REDACTED] Unit originally traveled to field offices to provide these information

⁸ In addition to field offices, the [REDACTED] Unit provides information briefings to FBI headquarters entities.

briefings. However, recent budget constraints and staffing shortfalls have limited the [REDACTED] Unit's ability to travel and provide briefings to field offices, which was acknowledged by various FTTTF personnel. As a result, the [REDACTED] Unit provides briefings at local conferences in the Washington, D.C., area, such as FBI supervisor conferences. Further, the [REDACTED] Unit provides the FTTTF capabilities briefing to each incoming Special Agents in Charge. The [REDACTED] Unit plans to increase its outreach efforts, particularly with on-site FTTTF capabilities briefings at field offices, if additional funding is received.

We found that field office personnel had a better understanding of the FTTTF when provided with a briefing. Specifically, National Security Analysis Center personnel conducted briefings at each field office using the Amon project before implementation. The briefings help field analysts gain an understanding of the project's mission, the analysis conducted, and the output provided to field offices. The Amon project briefing also gave field personnel a forum to provide specific search criteria that would benefit their location-specific investigative needs. We believe the Amon project briefings increased field analysts' coordination and understanding of the Amon project.

In addition to conducting capabilities briefings, the [REDACTED] Unit promotes the FTTTF's work through the dissemination of a monthly report to Special Agents in Charge and National Security Branch officials. According to the former FTTTF Director, the reports publicize the FTTTF's support role in national security investigations and the benefits of the FTTTF's analytical capabilities.

However, we found that the monthly report might not be utilized to the extent that the FTTTF intends. In general, the Special Agents in Charge we interviewed stated that either they do not receive any reports from the FTTTF, or that they receive the monthly FTTTF report but do not read it. Further, we found that senior field office managers generally do not interact with the FTTTF. Instead, squad supervisors, agents, and intelligence analysts coordinate with FTTTF personnel and address FTTTF leads. Therefore, we believe the FTTTF may find more benefit by also sending the reports to this cadre of FBI personnel to make them more aware of the FTTTF's capabilities.

While knowledge of the FTTTF is not necessary to address the FTTTF's leads, an increased knowledge of the FTTTF would allow field agents and analysts to understand the full capabilities of the FTTTF and to contact the FTTTF for additional support services to further national security

investigations. Therefore, we believe the FTTTF should explore new options to communicate its capabilities to field offices and headquarters sections, such as using secure video teleconference equipment to brief field offices and sending monthly report packages to operational personnel.

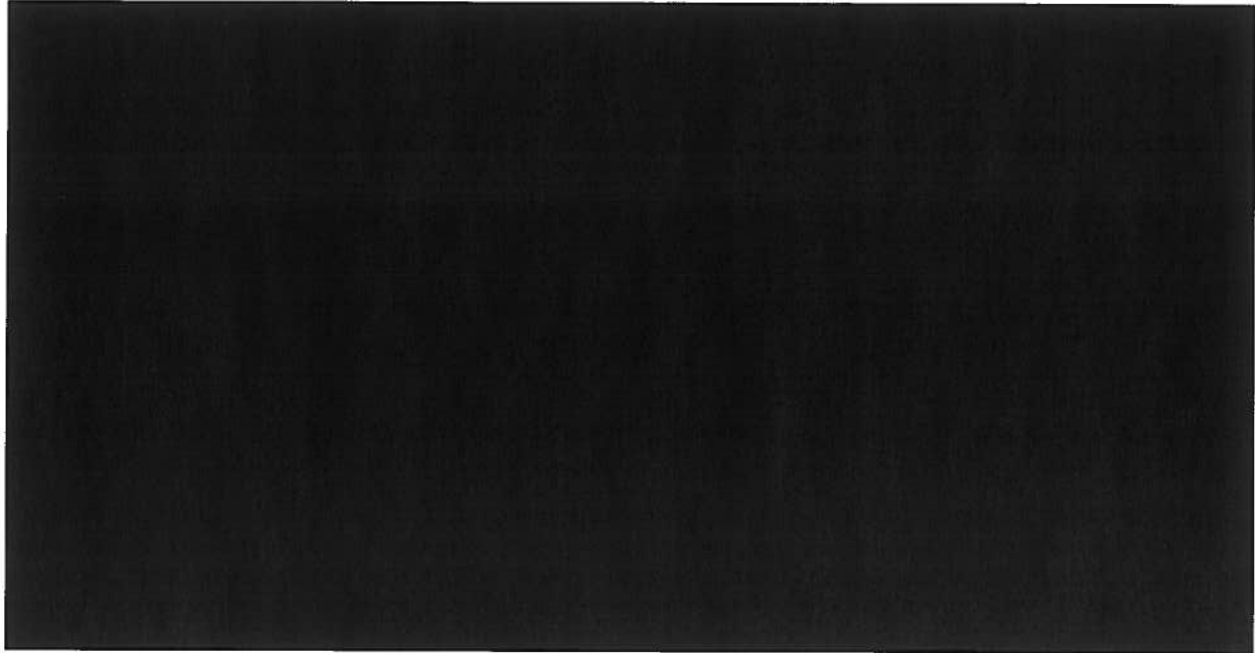
Tracking FTTTF Performance

To measure the support provided to the FBI's National Security Branch, the FTTTF identified various objectives to assist in accomplishing its goal of protecting the United States from national security threats. Specifically, the FTTTF determines its success through its ability to track and detect known and unknown subjects who pose a threat to U.S. national security; identify common subjects of interest from emerging, non-traditional national security threats; develop new methodologies and processes to support National Security Branch mission requirements; and provide actionable intelligence to FBI field offices that lead to the opening of investigations. To ensure these objectives are accomplished, the FTTTF's [REDACTED] Unit examines various statistics, including the number of leads sent to field offices and other FBI entities, such as headquarters sections, field intelligence groups, and FBI Legal Attachés located in foreign countries. The [REDACTED] [REDACTED] Unit then creates FTTTF statistical reports to provide metrics used to determine whether the FTTTF is accomplishing its mission.

We obtained the number of FTTTF leads sent to field offices from FY 2009 to FY 2011, as shown in Exhibit 1-1.⁹ According to the FBI, during this 3-year timeframe the FTTTF disseminated [REDACTED] leads to field offices, with an additional [REDACTED] leads sent to other FBI entities.

⁹ This chart does not incorporate information sent to field offices that is not in the form of leads, such as analysis from the Amon project provided to field offices in the form of a spreadsheet.

EXHIBIT I-1
LEADS DISSEMINATED BY THE FTTTF
FY 2009 – FY 2011



The former FTTTF Director also stated that the FTTTF operational units monitor their output to ensure leads are addressed and to gauge their achievement towards the following two objectives: (1) tracking and detecting known and unknown subjects who pose a threat to U.S. national security, and (2) providing actionable intelligence to FBI field offices that lead to the opening of investigations. However, the former FTTTF Director also stated that measuring the number of investigations opened as a result of an FTTTF lead is difficult because field offices may already be aware of the threat. Thus, field offices' actions may not have directly, or at least solely, resulted from the FTTTF's leads. Because the FTTTF could not provide definitive information on the number of investigations opened as a result of FTTTF analysis, the FTTTF provided information on the number of leads generated through the Traveler Assessment, FINDUS, and Scarecrow projects, depicted in Exhibit 1-2. Because the analysis through the Amon project does not result in leads, the FTTTF identified information on the number of [REDACTED] through this project.

EXHIBIT 1-2
FTTTF LEADS SENT TO FIELD OFFICES AND HEADQUARTERS
ENTITIES, BY PROJECT

PROJECT	FY 2011	JUNE 2012
Traveler Assessment		
FINDUS		
Scarecrow		
Amon		

FTTTF Operational Unit Performance Measures

Tracking leads alone cannot determine the FTTTF's progress towards its strategic goals. To help assess FTTTF operational performance, field offices are required to address the FTTTF's actionable leads by responding to the respective FTTTF operational unit responsible for sending the lead. The FTTTF established this reporting requirement to ensure that field offices review information sent and take appropriate actions that the field offices deem necessary.

Each FTTTF operational unit is responsible for ensuring field offices follow up on these leads and has discretion on how it monitors and tracks the field offices' actions. Officials from the operational units explained that some field offices often do not indicate whether the lead was addressed or what actions were taken, such as if the lead resulted in the identification of a suspect. As a result, these FTTTF units often must reach out to field offices to obtain the results of the leads provided by the FTTTF, a process requiring time and resources of the FTTTF staff that could instead be spent performing other analyses.

When field office personnel receive a lead in the FBI's case management system from the [REDACTED] Unit's Traveler Assessment project, they are instructed to send the [REDACTED] Unit an electronic communication that provides a narrative description of the actions the field office took to address the lead, as required by the FBI. The [REDACTED] Unit established an automated system to notify its Supervisory Special Agents if a field office response is past due. However, the [REDACTED] Unit's Supervisory Special Agents will also check Guardian to determine if a field office opened a threat assessment but did not directly alert the [REDACTED] Unit of its actions through an electronic communication.

During fieldwork at the Phoenix Field Office, we were informed about concerns with the format of how field offices are expected to respond to Traveler Assessment project leads. A field office manager explained that the field office did not respond to the [REDACTED] Unit via an electronic communication on [REDACTED], but instead only indicated in the FBI's case management system that these leads were addressed. In this official's opinion, responding via the FBI's case management system should be sufficient for noting a lead was addressed. The [REDACTED] Unit officials, in turn, explained that while they do not want to create extra work for the field offices, a narrative response in electronic communication format assists the FTTTF in determining whether the information provided was useful and relevant. The Unit Chief reiterated that the [REDACTED] Unit does not direct the field offices to open a case or create a source based on the leads provided, but rather the Supervisory Special Agents follow up to ensure that field offices reviewed the information sent and took appropriate actions that the field offices deem necessary.

The [REDACTED] Unit sends leads for the FINDUS project to field offices through Guardian. Leads disseminated through Guardian require field agents to respond within [REDACTED] days. Similar to the [REDACTED] Unit, the [REDACTED] Unit uses an automated system to track the status of FINDUS leads to ensure the leads have been addressed by the field office and will update the internal automated system when appropriate. An agent at the Chicago Field Office verified this process and explained that any response to a FINDUS lead is provided in the comments section of Guardian. If a lead has not been addressed, a [REDACTED] Unit analyst will reach out to the field office to determine what actions, if any, were taken to address the lead. The Unit Chief of the [REDACTED] Unit stated that receiving responses from the field offices on FINDUS leads had been a challenge for the unit prior to the [REDACTED] Unit providing leads in Guardian. This official also stated that larger field offices do not have time to notify the FTTTF whether it addressed leads, as the volume of leads and cases in those field offices does not allow sufficient time for agents to update the actions taken on every lead. However, since leads have been provided to field offices in Guardian, this official said that tracking the actions of the field offices has been much easier, as every investigative action is updated in Guardian. Responses in Guardian do not require an electronic communication to the FTTTF, therefore eliminating the burden of agents spending time to follow up on FTTTF leads.

It is important for the FTTTF to know what actions were taken on its disseminated leads. Without this information, the FTTTF cannot ensure that

field offices reviewed information sent and addressed the lead. We believe the FTTTF should meet with National Security Branch officials to come to agreement on how field offices can respond to FTTTF leads in an efficient manner that is not cumbersome for field office staff.

The FTTTF would also benefit from receiving feedback from field offices on the utility of the information provided in FTTTF-developed leads. The FTTTF cannot enhance its support role to field offices by simply knowing that a lead has been addressed. For example, a field office may respond to the FTTTF that a preliminary investigation has been opened. However, the field office may not have used any of the FTTTF's analysis in its determination to open the case. By obtaining feedback on the usefulness of FTTTF-generated leads, the FTTTF will be better able to determine its effectiveness in supporting the National Security Branch and assisting field offices in locating and tracking individuals who pose threats to national security. As mentioned above, one method for obtaining this feedback is through requesting field offices to provide a narrative response in electronic communication format that can explain the usefulness and relevance of the information provided by the FTTTF. We understand that asking field offices to provide this type of written feedback on each lead may be a strain on existing personnel resources. As a result, the FBI may opt to obtain information regarding the usefulness of the FTTTF's analyses through other methods, such as an annual field office survey, that may be less burdensome to field office personnel. Nonetheless, we believe the FTTTF should develop a method by which to determine the utility of information provided to field offices.

Recommendations

We recommend that the FBI:

1. Implement a strategy and procedures to [REDACTED] in the Traveler Assessment project.
2. Strengthen its procedures for ensuring FTTTF analyses and information provided to headquarters operational sections and field offices is not [REDACTED].
3. Consider assigning FTTTF personnel to provide assistance to additional National Security Branch units similar to the support provided to the Strategic Operations Section's fusion cells.
4. Evaluate the effectiveness of the current outreach efforts and develop a plan to increase awareness of the FTTTF's capabilities

to the National Security Branch operational divisions and field offices.

5. Establish a system or procedure to ensure the National Security Branch components and the FTTTF coordinate timely threat criteria updates for all applicable FTTTF projects.
6. Ensure that FTTTF and National Security Branch executive management develop a strategy and methods to obtain more complete and timely feedback from field offices to allow the FTTTF to better assess the usefulness and effectiveness of the information provided to field offices.

II. Information and Privacy Management

We reviewed the FTTTF's controls on information management and found that employees receive annual privacy training and must verify compliance with privacy policies when conducting searches. Further, the FBI Office of General Counsel has assigned an attorney to the FTTTF to ensure compliance with DOJ and FBI information and privacy rules and regulations. However, between FY 2008 and FY 2012, the FTTTF had not completely satisfied DOJ's specific requirements relating to the Privacy Act and E-Government Act.

FTTTF Information Management

The FTTTF obtains and manages various sets of sensitive FBI data, intelligence community data, and public source data that contain personally identifiable information – some of which is information classified at the Secret level and above. As a result, the FTTTF must follow certain legal and regulatory rules that relate to the collection, use, and dissemination of this sensitive information. We found that the FTTTF has taken several steps to ensure it is following privacy regulations, as detailed below.

All new FTTTF employees and contractors are trained on DOJ and FBI privacy policies. The training covers policies relating to privacy, civil liberties, acceptable data searches, and restrictions on data used in investigations. Additionally, FTTTF data systems contain built-in security checks requiring FTTTF employees to verify completion of privacy training and compliance with laws and regulations before every search performed.

Pursuant to FBI policy, the FBI's Office of General Counsel advises the FTTTF regarding the initiation of new projects and development of threat assessment documents and approves receipt of new datasets to ensure there is no violation of U.S. Persons' privacy. To aid in this effort, the FBI has assigned to the FTTTF a dedicated attorney from its Office of General Counsel Privacy and Civil Liberties Unit (Office of General Counsel liaison) to ensure compliance with applicable privacy laws, regulations, and policies, including those contained in the Attorney General Guidelines and the FBI's Domestic Investigations and Operations Guide.¹⁰ According to the FTTTF,

¹⁰ In 2003 the Attorney General established guidelines for national security investigations and foreign intelligence collection that provide policies related to maintenance of records under the Privacy Act. The FBI's Domestic Investigations and Operations Guide provides policy related to investigative activities and intelligence collection conducted by the FBI within the United States to protect the privacy and civil liberties of individuals.

this practice ensures that any DOJ and FBI privacy-related issue is addressed before project implementation.

The Office of General Counsel liaison ensures that the data used in FTTTF analyses relate to the FTTTF's mission and that searches conducted on the data are conducted using the least intrusive method, are predicated, and do not violate First Amendment rights. For instance, an FBI official explained that the Office of General Counsel liaison does not always authorize the FTTTF to ingest entire datasets containing U.S. Persons' information into its Datamart because this method is not acceptable for privacy standards. Therefore, the FTTTF must receive Office of General Counsel approval to search these datasets on a case-by-case basis. This approval process for each dataset utilized by the FTTTF helps ensure compliance with FBI and DOJ privacy and civil liberty investigative and intelligence collection policies. Both the former FTTTF Director and the Office of General Counsel liaison stated that the FTTTF has not encountered any privacy-related issues or problems.

In addition to the Office of General Counsel liaison, the Office of General Counsel's Privacy and Civil Liberties Unit Chief reviews the FTTTF's retention and access policies for the data it maintains. This Unit Chief stated that the FTTTF has incorporated privacy-related rules for each dataset within its systems to ensure personnel accessing the information are aware of the search, access, and retention requirements. Further, the FTTTF tracks and maintains a historical record of all searches conducted.

We believe that the utilization of an on-site Office of General Counsel liaison at the FTTTF is a good practice because it strengthens the FTTTF's privacy oversight and management. Employees' annual training, validation of privacy policy adherence when conducting searches, and verification of DOJ and FBI privacy policy compliance in FTTTF programs and datasets provide evidence of the FTTTF's commitment to privacy and information management.

Privacy Requirements for the FBI's Information Systems

The Privacy Act of 1974 mandates for newly created and revised systems of records that agencies publish a System of Records Notice for the Office of Management and Budget, Congress, and the Federal Register for public comment.¹¹ The System of Records Notice provides information about the system of records, including the purpose for which the agency collects the particular data and how it uses the information in the system.

In addition, the E-Government Act of 2002 requires federal government agencies to complete a Privacy Impact Assessment for information systems, with the exception of National Security Information systems, that collect or store information on individuals.¹² A Privacy Impact Assessment is an analysis of how information is handled: (1) to ensure the handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy issues. Although the E-Government Act provides an exception for National Security Information systems, DOJ policy requires its components to complete Privacy Impact Assessments for all information systems, including National Security Information systems.

DOJ established the Office of Privacy and Civil Liberties (OPCL) in 2006 to handle all privacy matters and, in particular, to review and prepare all DOJ Privacy Impact Assessments for approval by the DOJ's Chief Privacy and Civil Liberties Officer. The OPCL reviews the Privacy Impact Assessments to ensure consistency with other privacy and security documentation relevant to the system, including a published System of Records Notice.

The FBI requires its Privacy Impact Assessments to be updated every 3 years or whenever an update to a system occurs prior to the end of the 3-year cycle. DOJ approved the Privacy Impact Assessment for the FTTTF's Datamart in FY 2005. In FY 2008, the FBI submitted to the Acting DOJ Chief Privacy and Civil Liberties Officer an updated Privacy Impact Assessment for the FTTTF's Datamart to incorporate the FTTTF's inclusion of the National Security Analysis Center and the new datasets associated with the National Security Analysis Center. FBI officials told us that the Acting DOJ Chief Privacy and Civil Liberties Officer provided conditional approval of the

¹¹ 5 U.S.C. § 552a

¹² 44 U.S.C. § 101

Privacy Impact Assessment to the FBI in FY 2008. The Acting DOJ Chief Privacy and Civil Liberties Officer informed the FBI that the FBI needed to submit a separate System of Records Notice for the FTTTF Datamart. The FBI initially asserted that the System of Records Notice for the FBI's Central Record System provided coverage for all records associated with FBI investigations and that this encompassed the FTTTF and the National Security Analysis Center systems. The Acting DOJ Chief Privacy and Civil Liberties Officer and the OPCL agreed that the FTTTF Datamart was covered under the System of Records Notice for the FBI's Central Records System. However, the Acting DOJ Chief Privacy and Civil Liberties Officer determined that for more transparency the FBI needed to complete a System of Records Notice specifically for the FTTTF Datamart. The FBI and OPCL continued to hold discussions regarding the System of Records Notice requirement through FY 2009.

During this time, the FBI continued to use the FTTTF Datamart despite not yet receiving OPCL unconditional approval of the Privacy Impact Assessment specifically covering this system. The FTTTF acknowledged that the outdated Privacy Impact Assessment and unapproved System of Records Notice as areas of concern. Despite having these concerns, the FBI did not submit the requested System of Records Notice until FY 2011. According to a senior OPCL official, the FBI's and OPCL's disagreement on the recommendation to submit a System of Records Notice specifically for the FTTTF Datamart was the primary cause of the significant delay in the approval. In August 2011, FTTTF officials stated that the FBI submitted to the OPCL a System of Records Notice that specifically addressed the FTTTF Datamart.¹³ In July 2012, DOJ published the FTTTF Data Warehouse System of Records Notice in the Federal Register.

As previously mentioned, the FTTTF had been granted conditional approval of its Privacy Impact Assessment in FY 2008 and would not receive final approval until the System of Records Notice for the FTTTF Datamart had been submitted. Due to the change in both DOJ and FBI privacy leadership and because of the differences in opinion regarding the need for a separate FTTTF Systems of Record Notice, the FY 2008 Privacy Impact Assessment was not finalized until September 2012.

In FY 2011, the FTTTF began updating its Privacy Impact Assessment to include all FTTTF systems and classification levels, including the FTTTF

¹³ The System of Records Notice also covers the FBI's Data Integration and Visualization System, which will eventually be merged with the Investigative Data Warehouse. The Data Integration and Visualization System currently has its own System of Records Notice, but the FBI wanted the Data Integration and Visualization System to be included within the System of Records Notice.

Datamart. This Privacy Impact Assessment is responsive to the FBI's policy requiring such updates every 3 years and is being coordinated internally within the FBI; the updated document has not yet been submitted to the OPCL for approval. We believe that the FBI should ensure that the FTTTF submits to the OPCL an update to the FY 2008 FTTTF Datamart Privacy Impact Assessment, as required by FBI policy.

Recommendation

We recommend that the FBI:

7. Ensure that the FTTTF submits to the OPCL an update to the FY 2008 FTTTF Datamart Privacy Impact Assessment.

STATEMENT ON INTERNAL CONTROLS

As required by the *Government Auditing Standards*, we tested, as appropriate, internal controls significant within the context of our audit objectives. A deficiency in an internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to timely prevent or detect: (1) impairments to the effectiveness and efficiency of operations, (2) misstatements in financial or performance information, or (3) violations of laws and regulations. Our evaluation of the FBI's internal controls was *not* made for the purpose of providing assurance on its internal control structure as a whole. FBI management is responsible for the establishment and maintenance of internal controls.

Through our audit testing, we did not identify any deficiencies in the FBI's internal controls that are significant within the context of the audit objectives and based upon the audit work performed that we believe would affect the FBI's ability to effectively and efficiently operate, to correctly state financial and performance information, and to ensure compliance with laws and regulations.

Because we are not expressing an opinion on the FBI's internal control structure as a whole, this statement is intended solely for the information and use of the FBI. This restriction is not intended to limit the distribution of this report, which is a matter of public record. However, we are limiting the distribution of this report because it contains sensitive information that must be appropriately controlled.

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS

As required by the *Government Auditing Standards* we tested, as appropriate given our audit scope and objectives, selected transactions, records, procedures, and practices, to obtain reasonable assurance that the FBI's management complied with federal laws and regulations, for which noncompliance, in our judgment, could have a material effect on the results of our audit. The FBI's management is responsible for ensuring compliance with applicable federal laws and regulations. In planning our audit, we identified the following laws and regulations that concerned the operations of the FBI and that were significant within the context of the audit objectives:

- Homeland Security Presidential Directive-2: Combating Terrorism Through Immigration Policies
- Privacy Act of 1974 (5 U.S.C. § 552a)
- E-Government Act of 2002 (44 U.S.C. § 101)

Our audit included examining, on a test basis, the FBI's compliance with the aforementioned laws and regulations that could have a material effect on the FBI's operations, through obtaining FTTTF documentation, interviewing FBI and OPCL personnel, and observing FTTTF analysis. Nothing came to our attention that caused us to believe that the FBI was not in compliance with the aforementioned laws and regulations.

OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

The objectives of our audit were to determine if: (1) the FBI has implemented a viable FTTTF strategy to locate and track suspected terrorists and their supporters, including coordination with FBI headquarters and field offices to enhance national security investigations; and (2) the FBI is following DOJ privacy policies in its management of information.

Scope and Methodology

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

To accomplish these objectives, we interviewed FTTTF officials, including the former FTTTF Director, assistant section chiefs, and nine unit chiefs, as well as analysts and agents within the operational units. We also interviewed officials within the Counterterrorism Division, including section chiefs of the International Terrorism Operations Section-1 and International Terrorism Operations Section-2, unit chiefs and analysts from the Strategic Operations Sections' fusion cells, and the FTTTF assignees to the fusion cells. In addition, we interviewed unit chiefs from the Counterintelligence Division and the Deputy Assistant Director of the Weapons of Mass Destruction Directorate.

Regarding privacy issues, we interviewed the FTTTF Office of General Counsel liaison, an official from the FBI's Office of General Counsel, and the Director and Assistant Director of the DOJ's Office of Privacy and Civil Liberties. We also reviewed the FTTTF's draft Privacy Impact Assessment and System of Records Notice for its systems.

We selected four FTTTF projects on which to focus our review.

[REDACTED]

We also chose these projects because two projects address counterterrorism, one addresses domestic terrorism, and the last focuses on counterintelligence threats. As a result, the projects we reviewed provided a broad view of the FTTTF's activities. We then met with FTTTF officials to observe analysis on each of

these projects. We obtained the total number of leads sent and subjects assessed by the FTTTF to every FBI field office for each of the selected projects. Using this data, we selected five field offices for which to obtain more specific information on leads sent by the FTTTF in FYs 2011 and 2012, specifically we requested the case identification number, serial number, date, disposition, and description of the case. Based on the volume of leads provided to field offices and the variety of the disposition of the leads, we selected three field offices for field site visits: (1) Chicago, Illinois; (2) New York, New York; and (3) Phoenix, Arizona. We then selected a sample of leads sent to these three field offices based on the disposition type. While on-site we interviewed the analysts and agents who addressed the selected leads, their supervisors, the Assistant Special Agents in Charge, and the Special Agents in Charge.

Prior Reviews

In FY 2010, the Office of the Inspector General contracted with KPMG LLP to conduct a review of the FTTTF's TECHTRACK Unclassified Network, pursuant to the Federal Information Security Management Act.¹⁴ The OIG found that the FTTTF did not consistently develop and enforce information technology security policies within the TECHTRACK network in accordance with DOJ policies and procedures. The identified deficiencies were considered low impact to the protection of the FTTTF's TECHTRACK network, including its data, from unauthorized use, disclosure, loss, or modification. The FBI has adequately addressed the deficiency.

¹⁴ OIG, *Foreign Terrorist Tracking Task Force (FTTTF) TECHTRACK*, Audit Report 10-42 (August 2010).

FTTTF UNITS

FTTTF OPERATIONS UNITS:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

FTTF OPERATIONAL SUPPORT UNITS:

[REDACTED]

FEDERAL BUREAU OF INVESTIGATION RESPONSE



U.S. Department of Justice
Federal Bureau of Investigation

Washington, D. C. 20535-0001

January 7, 2013

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, *Audit of the Federal Bureau of Investigation's Foreign Terrorist Tracking Task Force (FTTTF)*.

We are pleased you determined that the FBI has implemented a strategy that provides "significant value to the FBI by performing in-depth analyses that proactively identify national security threats and assist ongoing national security investigations." As noted, the FTTTF has worked to improve its coordination with the entire FBI National Security Branch, especially within the Counterterrorism Division.

The FBI continues to evaluate and strategize on ways to improve the mission of the FTTTF. In that regard, we concur with your seven recommendations and are pleased to report we have already implemented measures for many. Please find enclosed our responses.

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

Sincerely,

A handwritten signature in black ink, reading "Keith L. Bennett".

Keith L. Bennett
Assistant Director
Inspection Division

Enclosures (2)

**AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S
FOREIGN TERRORIST TRACKING TASK FORCE**

Report Recommendation #1 – “Implement a strategy and procedures to [REDACTED] in FTTTF's Traveler Assessment project.”

FBI Response to Recommendation #1:

Concur. FTTTF is conducting a review of the Traveler Assessment Project's threat criteria and is ensuring the criteria are commensurate with CTD's current threat picture to [REDACTED]

Report Recommendation #2 – “Strengthen its procedures for ensuring that FTTTF information provided to headquarters operational sections and field offices is not [REDACTED]
[REDACTED]

FBI Response to Recommendation #2:

Concur. FTTTF has procedures in place to mitigate the dissemination of [REDACTED]
[REDACTED] information. [REDACTED]
[REDACTED]

[REDACTED] as a result, FTTTF can provide information to headquarters operational sections and field offices in a timely manner. FTTTF routinely includes information compiled from field office investigative files and other government databases, which may appear [REDACTED], but provide a more comprehensive, contextual perspective.

Report Recommendation #3 – “Consider assigning FTTTF personnel to provide assistance to additional National Security Branch units similar to the support provided to the Strategic Operations Section's fusion cells.”

FBI Response to Recommendation #3:

Concur. FTTTF will continue to assign personnel to other FBI National Security Branch and Intelligence Community components, as resources allow. FTTTF has detailed three intelligence analysts to the FBI's Counterintelligence Division and an Intelligence Community partner.

Report Recommendation #4 – “Evaluate the effectiveness of the current outreach efforts and develop a plan to increase awareness of the FTTTF's capabilities to the National Security Branch operational divisions and field offices.”

FBI Response to Recommendation #4:

Concur. FTTTF continues to increase awareness of FTTTF capabilities to the National

Security Branch divisions and field offices through the following actions:

- FTTTF has assigned a Supervisory Special Agent (SSA) to serve as a full-time liaison to headquarters operational and analytical components with oversight of analysts embedded in the Operations Sections. The SSA reports directly to the FTTTF Assistant Section Chief for Operations. '
- FTTTF is preparing a request to the FBI Training Division to develop a Web-based Training (WBT) course that will be delivered through the FBI's Virtual Academy. This WBT course will provide an overview of FTTTF's capabilities and will be available to all FBI employees.
- FTTTF will participate in other FBI-sponsored regional and local training events and operational meetings.
- FTTTF has submitted an FTTTF-specific section for inclusion within the Counterterrorism Program Guide.
- FTTTF plans to request that FTTTF-specific instructional blocks be offered within various courses at the FBI Academy.

Report Recommendation #5 – “Establish a system or procedure to ensure the National Security Branch components and the FTTTF coordinates timely threat criteria updates for all applicable FTTTF projects.”

FBI Response to Recommendation #5:

Concur. The CTD instituted a Division-wide threat based management model which assessed prioritized, and published CT threats FBI-wide. This uniform threat model is now used as the basis for threat criteria. In addition, FTTTF opened a Type 3 Assessment for the Traveler Assessment Project and Type 3/4 Assessments for other applicable FTTTF projects supporting National Security Branch components. In accordance with the FBI's Domestic Investigations and Operations Guide, these FTTTF projects, including their applicable threat criteria, are reviewed, updated, and reauthorized every 90 days, in coordination with the National Security Branch.

Report Recommendation #6 – “Ensure that FTTTF and National Security Branch executive management develop a strategy and methods to obtain more complete and timely feedback from field offices to allow the FTTTF to better assess the usefulness and effectiveness of the information provided to field offices.”

FBI Response to Recommendation #6:

Concur. FTTTF currently solicits feedback from field offices by telephone and email. To obtain more complete and timely feedback, FTTTF has requested that the FBI's Resource Planning

APPENDIX III

Office expand the existing list of “predication source codes” within Sentinel. These codes will allow FTTTF to quantify the number of cases opened as a result of FTTTF's analytical products.

Report Recommendation #7 – “Ensure that the FTTTF submits to the OPCL an update to the FY 2008 FTTTF Data Mart Privacy Impact Assessment (PIA).”

FBI Response to Recommendation #7:

Concur. The PIA will be submitted to the OPCL. However, pursuant to Section 208(b)(I)(C) of the E-Government Act of 2002, to protect the classified and sensitive information it contains, the approved PIA containing information about the FTTTF Data Mart will not be made publicly available.

OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE REPORT

The OIG provided a draft of this audit report to the FBI. The FBI's response is incorporated in Appendix III of this final report. The following provides the OIG analysis of the response and summary of actions necessary to close the report.

Recommendation Number:

1. **Resolved.** The FBI concurred with our recommendation to implement a strategy and procedures to [REDACTED] in the FTTTF's Traveler Assessment project. The FBI stated in its response that to [REDACTED], the FTTTF is conducting a review of the Traveler Assessment project's threat criteria to ensure the criteria are commensurate with the Counterterrorism Division's current threat picture. While we believe this review will help ensure the Traveler Assessment project is focused on current threats, the FBI did not indicate whether it would be implementing a strategy and procedures to [REDACTED] following its review of the current threat picture. We believe that implementing a project-specific approach will help the FBI to assess the project's analysis on a regular basis and to help [REDACTED]

This recommendation can be closed when we receive a copy of a strategy and procedures for [REDACTED] on the Traveler Assessment project, as well as evidence that the FBI [REDACTED]

2. **Resolved.** The FBI concurred with our recommendation to strengthen its procedures for ensuring that FTTTF information provided to headquarters operational sections and field offices is not [REDACTED]. The FBI stated in its response that the FTTTF has procedures in place to mitigate the dissemination of [REDACTED] information. The FBI also stated that these procedures have been further bolstered through the FTTTF's implementation of [REDACTED]

The FBI explained that the FTTTF will be able to provide more timely information to headquarters operational sections and field offices by using this process of [REDACTED]. However, the FBI was

not clear on how its actions will ensure FTTTF information and analyses, on the whole, are timely.

In addition, the FBI stated that the FTTTF routinely includes information generated by field offices and other government databases to provide a more comprehensive, contextual perspective even though this information may appear [REDACTED] in nature. Despite the intentional inclusion of this additional content, as noted in our report some field office agents and analysts believed that the FTTTF provided such information and described it to be [REDACTED]. However, we believe this perception of [REDACTED] information will be less likely to occur as field office agents and analysts become more knowledgeable about the FTTTF and its processes. We believe that increasing FBI field office personnel's awareness on FTTTF's capabilities will provide field agents and analysts with additional insight to the FTTTF's analyses, including the data and information used, and help them to better understand the leads disseminated by the FTTTF. Recommendation 4 addresses enhancing the FTTTF's outreach efforts.

This recommendation can be closed when we receive a copy of the procedures the FTTTF has put in place to provide timely information to field offices, including an explanation on how the FBI's [REDACTED] We will evaluate the portion of the recommendation associated with [REDACTED] information in conjunction with the FBI's actions to address Recommendation 4.

- 3. Resolved.** The FBI concurred with our recommendation to consider assigning FTTTF personnel to provide assistance to additional National Security Branch units similar to the support provided to the Strategic Operations Section's fusion cells. The FBI stated that the FTTTF will continue to assign personnel to other FBI National Security Branch and Intelligence Community components based upon the availability of resources. The FBI further stated that the FTTTF detailed three intelligence analysts to the Counterintelligence Division and an Intelligence Community partner.

This recommendation can be closed when we receive evidence of the intelligence analysts assigned to the National Security Branch and the Intelligence Community, including the roles of these analysts. In addition, please provide an update on the FBI's intentions of assigning FTTTF personnel to other National Security Branch units.

- 4. Resolved.** The FBI concurred with our recommendation to evaluate the effectiveness of the current outreach efforts and develop a plan to increase awareness of the FTTTF's capabilities within the National Security Branch operational divisions and field offices. The FBI stated that the FTTTF continues to increase the awareness of the FTTTF's capabilities in a number of ways, including the assignment of a full-time liaison to FBI headquarters operational and analytical components, the submission of an FTTTF-specific section for inclusion within the Counterterrorism Program Guide, and participation in other FBI-sponsored regional and local training events and operational meetings. The FBI further stated that it plans to enhance its outreach by requesting that FTTTF-specific instructional blocks be offered within various courses at the FBI Academy and by requesting the development of a web-based training course on the FTTTF's capabilities available through the FBI Virtual Academy.

This recommendation can be closed when we receive evidence of the FTTTF's assignment of a full-time liaison to headquarters sections, including the responsibilities of the liaison. Additionally, please provide evidence of the FTTTF's efforts to enhance training through the development of an FTTTF-specific web-based training course available in the FBI Virtual Academy and in the offering of FTTTF-specific instructional blocks at the FBI Academy. Moreover, please provide evidence of the FTTTF's participation in other FBI-sponsored regional and local training events and operational meetings, as well as the inclusion of the FTTTF-specific section in the Counterterrorism Program Guide.

- 5. Resolved.** The FBI concurred with our recommendation to establish a system or procedure to ensure the National Security Branch components and the FTTTF coordinates timely threat criteria updates for all applicable FTTTF projects. The FBI stated that the Counterterrorism Division established a uniform threat model that assessed, prioritized, and published counterterrorism threats FBI-wide, and that this model is currently used as the basis for threat criteria. The FBI also stated that the FTTTF has threat assessments for its applicable projects, and that in accordance with the FBI's Domestic Investigations and Operations Guide, these projects, including the applicable threat criteria, are reviewed, updated, and reauthorized every 90 days in coordination with the National Security Branch.

This recommendation can be closed when we receive evidence that the FTTTF and the National Security Branch review, update, and

reauthorize the threat assessments, including the threat criteria, for all applicable FTTTF projects every 90 days during FY 2013.

- 6. Resolved.** The FBI concurred with our recommendation to ensure that FTTTF and National Security Branch executive management develop a strategy and methods to obtain more complete and timely feedback from field offices to allow the FTTTF to better assess the usefulness and effectiveness of the information provided to field offices. In its response, the FBI stated that the FTTTF currently solicits feedback from field offices via telephone and e-mail. However, as stated in our report, many field office agents and analysts do not respond to the FTTTF regarding the utility of information provided.

The FBI further stated that the FTTTF requested that Sentinel's functionality be expanded to include additional predication source codes that would allow the FTTTF to quantify the number of cases opened as a result of the FTTTF's analyses. This enhancement will help the FTTTF in its assessment of the information provided to field offices. However, whether a case was opened as a result of the FTTTF's analysis does not necessarily equate to whether the information was useful. Therefore, we believe that the FTTTF and National Security Branch executive management need to continue to develop a strategy and additional methods for obtaining feedback on the usefulness and effectiveness of FTTTF information provided to field offices. We believe the FBI could address this recommendation in conjunction with its actions to enhance the FTTTF's outreach efforts in Recommendation 4. We believe that increasing the FBI's awareness of the FTTTF's capabilities will enable FBI personnel to more fully understand the FTTTF's analyses and information and, in turn, become more willing and motivated to provide feedback to the FTTTF on the utility and effectiveness of the information.

This recommendation can be closed when the FBI provides evidence on the development of a strategy and additional methods to obtain feedback from field offices on the usefulness and effectiveness of FTTTF information. In addition, once implemented, please provide evidence of the additional predication source codes within Sentinel, as well as FTTTF's use of this information to assess its usefulness and effectiveness.

- 7. Resolved.** The FBI concurred with our recommendation to ensure that the FTTTF submits to the OPCL an update to the FY 2008 FTTTF Data Mart Privacy Impact Assessment. In its response, the FBI stated that the Privacy Impact Assessment will be submitted to the OPCL.

APPENDIX IV

This recommendation can be closed when we receive evidence that the FBI submitted to the OPCL an updated Privacy Impact Assessment for the FTTTF Data Mart.