THE FEDERAL BUREAU OF INVESTIGATION'S TERRORIST THREAT AND SUSPICIOUS INCIDENT TRACKING SYSTEM

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

Audit Report 09-02
November 2008

THE FEDERAL BUREAU OF INVESTIGATION'S TERRORIST THREAT AND SUSPICIOUS INCIDENT TRACKING SYSTEM

EXECUTIVE SUMMARY

In the aftermath of the September 11 terrorist attacks, the Federal Bureau of Investigation's (FBI) top priorities shifted from traditional law enforcement investigations to the prevention of terrorist attacks. In fulfillment of its new priorities, the FBI began to require that every terrorism-related lead from its sources, or from its federal, state, or local partners, be addressed, even if it required the diversion of resources from other priority areas. The FBI's principal automated system to track terrorist threats and suspicious incidents is its Guardian Threat Tracking System (Guardian).

Guardian is an automated system that records, stores, and assigns responsibility for follow up on counterterrorism threats and suspicious incidents. It also records the outcome of the FBI's handling of terrorist threats and suspicious incidents. Guardian can be used to distribute immediate threat information to users, and it also provides the capability to analyze threat information for trends and patterns.

Audit Approach

The Department of Justice Office of the Inspector General (OIG) initiated this audit to evaluate the policies and procedures the FBI uses to identify, assess, and track terrorist threats and suspicious incidents. In particular, we examined the FBI's: (1) Guardian Threat Tracking System; (2) Guardian threat assessment processes and operational guidance established by FBI headquarters; and (3) Guardian threat assessment policies and procedures in practice at six FBI field offices we visited.

To conduct this review we: (1) reviewed threat management documents developed by the FBI's Counterterrorism Division (CTD); (2) interviewed FBI officials and Guardian users assigned to various headquarters locations; (3) interviewed FBI officials and Guardian users at select field offices; (4) examined the process followed by the FBI in developing, implementing, maintaining, and updating Guardian; (5) tested samples of terrorism-related incidents tracked in Guardian; and (6) tested

samples of counterterrorism-related cases in the Automated Case Support (ACS) system.[1]

Results in Brief

From July 2004 through November 2007, the FBI documented approximately 108,000 potential terrorism-related threats, reports of suspicious incidents, and terrorist watchlist encounters in Guardian. The FBI determined that the overwhelming majority of the threat information documented in Guardian had no nexus to terrorism. However, as a result of information reported in Guardian the FBI initiated over 600 criminal and terrorism-related investigations from October 2006 to December 2007.

According to internal FBI assessments, the number of reported terrorist threats and suspicious incidents is expected to continue to grow. To adequately address this growth, the FBI recognizes that it must continually improve its ability to rapidly share this information and also improve communications among its federal, state, and local law enforcement partners.

In October 2006, the FBI implemented Guardian 2.0, an enhanced version of its primary threat tracking system. Guardian 2.0 allows threat information to be immediately available to users and provides the capability to search threat information for trends and patterns.

We found that Guardian represents a significant improvement over how the FBI tracked and handled threat information in the past because it provides users with the ability to enter suspicious activity and threat information and manage threat assessments through an automated electronic workflow process. However, we also found important aspects of Guardian that need improvement.

We determined that although FBI CTD guidance states that an FBI supervisor is responsible for reviewing and closing each threat or suspicious incident in Guardian, we found that supervisors did not perform the

[1] Typically, the FBI records and tracks terrorist threats and suspicious incidents in the Guardian system as pre-case incidents. After the FBI completes its investigative work on the pre-case incidents, the incidents are closed in Guardian. Some of the pre-case threats and suspicious incidents result in the opening of preliminary inquiries or full field investigations and are tracked as counterterrorism-related investigative cases in the FBI's ACS system. When the FBI completes investigations, the cases are resolved and closed in the ACS system.

supervisory review prior to closing the Guardian incident in 27 (12 percent) of the 218 incidents we tested.

Additionally, we found that the FBI considered some Guardian incidents to have a low priority. These routine incidents remained unaddressed in the threat tracking system for several months, even though CTD guidance states that all threats are to be resolved within 30 days. We found that priority and immediate level threats were generally addressed in a timely fashion.

In addition to the incident summary, information is entered in Guardian through supplementary tabs that separate an incident or threat into its basic components, such as sources, targets (places), subjects (people), weapons or methods, and vehicles. However, we found that the users did not consistently include basic component information in Guardian. Therefore, users who complete searches or trend analyses in Guardian could receive an inaccurate assessment of the threat due to this incomplete data.

FBI guidance regarding Guardian generally requires that all threat information developed during counterterrorism investigations and recorded in the FBI's Automated Case Support system also be entered in Guardian. However, we found that in almost half the cases in ACS we tested users did not enter the corresponding threat information in Guardian. As a result, threat information entered only in the ACS system may not be available to the FBI's government agency partners.

We also found that the deployment of Guardian's companion threat tracking system – E-Guardian – was delayed. After a planned October 2007 deployment, the FBI reported in September 2008 that E-Guardian was being tested on a pilot basis and that it planned to roll out E-Guardian in phases nationwide by the end of 2008. Implementation of Guardian maintenance patches designed to ensure optimal system operation were also delayed. FBI officials said that both delays were affected by a contractor change. Moreover, the FBI must develop or purchase new software to complete E-Guardian because the FBI's original contractor did not completely document the software used to develop Guardian. Because both Guardian and E-Guardian are critical to the FBI's terrorist threat tracking and management process, any additional delays in the deployment of E-Guardian could inhibit the system's ability to track terrorist threats and suspicious incidents.

The FBI's policy to investigate every credible terrorist threat that it receives requires the FBI to ensure that it uses its resources as effectively as possible. However, we found that the FBI did not have performance

measures to assess its overall effectiveness in resolving potential terrorist threats and suspicious incidents. Performance measures would help the FBI consistently manage its staffing workloads and enhance the FBI's efforts to deploy critical resources to the areas of need and priority.

Based on our audit, we believe the FBI should take additional steps to enhance Guardian's capability to track, manage, and resolve terrorist threats and suspicious incidents. In our report we make seven recommendations related to the FBI's tracking of terrorist threats and suspicious incidents. These recommendations are designed to help the FBI improve the data quality of Guardian information; ensure all required information is entered in Guardian; ensure all threat assessments are addressed, completed, and reviewed by supervisory personnel; resolve technical problems and delays identified in the development and implementation of its Guardian 2.0 and E-Guardian systems; and develop and utilize performance measures to ensure critical resources are deployed effectively.

The remaining sections of this Executive Summary summarize in more detail our audit findings.

Terrorist Threat and Suspicious Incident Assessment Process

The FBI receives terrorist threat and suspicious incident information from a variety of sources, including: (1) the public, (2) other government agency partners, (3) state and local law enforcement, (4) FBI field offices during ongoing investigations, and (5) FBI Legal Attachés. Regardless of the reporting source, the FBI requires that each threat or suspicious incident be reviewed, documented, and assessed to determine if a potential nexus to terrorism exits.

Guardian

In October 2006, the FBI deployed the latest version of its tracking system, Guardian 2.0. Guardian is an automated tracking system that records, stores, and assigns responsibility for follow up on counterterrorism threats and suspicious incidents. Moreover, it can provide immediate threat information to all users. Guardian can be searched by FBI employees and other government agency partners who the FBI has determined need counterterrorism-related intelligence information. Guardian also provides the capability to search threat information for trends and patterns.

The number of incidents in Guardian has grown dramatically since it was first implemented in 2004, and as of November 2007 the system

included approximately 108,000 individual threats, suspicious incidents, and terrorist watchlist encounters.

E-Guardian

The FBI is developing an additional threat tracking system to complement Guardian, called E-Guardian. E-Guardian is designed to facilitate the sharing of threat and suspicious incident information between the FBI and its state and local law enforcement partners that do not currently have access to Guardian due to security limitations. The FBI plans to routinely export unclassified threat information from Guardian to E-Guardian to enable access through Law Enforcement Online.[2] FBI law enforcement partners will also have the ability to enter local threat information directly in E-Guardian. E-Guardian users will be able to enter, view, search, and create reports based on threat data input by both state and local law enforcement and the FBI. However, the deployment of E-Guardian has been delayed. As previously stated, the FBI reported in September 2008 that E-Guardian was being tested on a pilot basis by certain agencies and that the FBI planned to complete rolling out E-Guardian in phases nationwide by the end of 2008.

OIG Evaluation of the FBI's Terrorist Threats and Suspicious Incidents Processing

The FBI's threat assessment process is centrally controlled and managed from FBI headquarters through three mechanisms: (1) the Counterterrorism Watch Unit (CT Watch), which operates a 24-hour global command center with complete visibility and oversight responsibility over Guardian; (2) the Threat Monitoring Unit (TMU), which disseminates counterterrorism policy guidance to FBI field components; and (3) the Foreign Terrorist Tracking Task Force (FTTTF), which develops Guardian terrorist threat tracking software.[3] FBI field offices and Legal Attachés are responsible for tracking and following up on leads that reside within their geographic areas of responsibility.

Field Office Terrorism-Related Incident Testing

To assess the FBI's terrorist threat management policies and procedures, we visited six FBI field offices and tested a sample of the

[2] The Law Enforcement Online (LEO) system provides a secure network that LEO members can use to store, process, and transmit Sensitive But Unclassified information.

[3] For this report, whenever we refer to FTTTF we are referring to the FTTTF Support Unit, Office of the Chief Technology Office.

terrorism-related incidents entered in Guardian. We selected the following field offices to provide perspectives from a cross-section in terms of field office size, operational activity, and geographic location.

- Philadelphia, Pennsylvania
- Washington, D.C.
- New York, New York
- Detroit, Michigan
- Kansas City, Missouri
- Los Angeles, California

Guardian's ability to accurately track threats depends on the accuracy, timeliness, and completeness of the incident information entered by system users. For example, inaccurate, incomplete, or untimely threat information entered in Guardian could cause a terrorist threat to go unaddressed or not be timely investigated.

At the six field offices, we therefore tested key attributes that we considered essential to successfully entering, updating, and managing incidents in Guardian: (1) the completeness of the incident summary, (2) supervisory oversight of the incident, (3) timeliness of investigative activity to address the incident, and (4) completion of supplementary search tabs.

In addition, we tested a judgmental sample of 218 terrorism-related incidents from a universe of 1,621 potential terrorism-related incidents in Guardian. As discussed below, we found 133 (61 percent) of the incidents we tested did not adhere to the FBI's policy or procedural guidelines in at least one of the four key areas in our testing.

Guardian Incident Summary

Guardian users are required to enter threat data in Guardian through a screen called the Incident Summary Screen. The Incident Summary Screen provides an overview of the terrorist threat or suspicious incident. To determine if the users entered the incident completely, we reviewed the Incident Summary Screen for the 218 sampled incidents. We found that all of the necessary summary information was included in the incidents we tested.

Supervisory Oversight of Guardian Incidents

According to the Guardian User's Guide, an FBI supervisor is responsible for reviewing and closing each threat or suspicious incident. The

supervisor must determine whether the threat is satisfactorily addressed or if additional investigation, analysis, or incident updating is required. This supervisory review provides critical oversight and the final quality assurance check for completed Guardian incidents.

We reviewed the supervisory actions taken in each of the 218 Guardian incidents tested. We found that supervisors did not perform the supervisory review prior to closing the Guardian incident in 27 (12 percent) of the incidents tested.

According to CTD guidance, supervisory review and closure of all Guardian incidents should only be performed by an FBI Supervisory Special Agent (SSA) or Supervisory Intelligence Analyst. We found that three of the six field offices we visited did not meet those requirements because supervisors had delegated the review and closure of Guardian incidents to a non-supervisor.

Timeliness of Threat Assessments

Guardian users are prompted by the system when entering an incident in Guardian to establish a priority rating for the reported incident. The system includes three ratings.

Immediate. Threat assessment begins upon receipt and the threat is normally addressed on the same day.

Priority. Threat assessment begins shortly after receipt and the threat is normally addressed on the same or the next day.

Routine. Threat assessment begins as time permits and the threat is normally addressed within 30 days.

We discussed the timeliness criteria with SSAs at FBI headquarters and Special Agents in field offices who were responsible for terrorist threat assessments.[4] In general, they said that they considered the 30-day period to address routine threats as guidance, not required criteria. They also said that some complex threats, such as threats that require contact with sources outside the United States, cannot be fully addressed within the 30-day guideline. Therefore, we evaluated timeliness by examining threat assessments that included periods of inactivity in excess of 30 days.

[4] The FBI conducts threat assessments during many stages of its investigative process. Unless otherwise noted in this report, threat assessment refers to the FBI's initial assessment of the threat during its pre-case determination of the credibility of the threat information.

We reviewed 218 Guardian incidents in our sample for the timeliness of the Guardian threat assessment process. For 5 of the 6 field offices we visited, we found 60 incidents (28 percent) that did not meet the 30-day criteria for routine assessments. For the remaining field office we found that all 25 incidents sampled were closed within the 30-day criteria. We found that both the CTD and field office supervisors exercised adequate oversight over threats and suspicious incidents identified in the system as priority or immediate.

Completeness of Guardian Supplementary Tabs

Information is entered in Guardian in two stages. Information is first entered into the incident summary in narrative form. Information in the narrative is searchable, but these searches are limited by the amount of information entered by the user. In addition to the incident summary, information is entered in Guardian through supplementary tabs that separate an incident or threat into its basic components, such as sources, targets (places), subjects (people), weapons or methods, and vehicles. These tabs must be completed separately by Guardian users from the incident summary, because the data is not automatically transferred from the incident summary. When the tabs are completed, Guardian users have enhanced ability to conduct search and trend analysis with the information contained specifically within the tabs.

However, we found that users did not complete the supplementary tabs in 66 of the 218 incidents (30 percent) we tested. From our analysis, we determined that guidance provided to the users was inadequate because FBI policy does not clearly establish whether the completion of the supplementary tabs is required. Some FBI officials stated that they believed the completion of the supplementary tabs was essential because it improved Guardian's search and trend analysis capabilities. However, other FBI officials stated that the increased workload generated by completing the supplementary tabs was not justified.

As a result of the inconsistent application of this guidance and data not being entered into the supplementary tabs, searches relying on the information contained within the tabs will return incomplete and inaccurate threat assessment information.

Attorney General Guidelines Testing

During our review of Guardian, we also found that in many instances the FBI had asked United States Attorneys' Offices to issue grand jury

subpoenas related to the assessment of suspicious incidents before opening a preliminary or full field investigation.[5] We found that two of the four field offices we visited, New York and Los Angeles, sought and obtained grand jury subpoenas without opening preliminary or full field investigations. However, at the other two sites, Detroit and Kansas City, the FBI would not obtain grand jury subpoenas without first opening a preliminary or full investigation. Officials from the Kansas City and Detroit field offices indicated that they understood that obtaining grand jury subpoenas required the opening of a preliminary or full field investigation.

First, we sought to determine the extent of the FBI's practice of requesting subpoenas without opening a preliminary or full field investigation. To do this, we reviewed a computer-generated report from FBI headquarters that identified FBI subpoena requests supported by administrative case control file numbers for the period October 2006 through July 2007. Control files are administrative case files used by the FBI to store information in the ACS system that do not relate to preliminary or full field investigations.

The FBI report that we reviewed identified 4,067 grand jury subpoenas issued from October 2006 to July 2007. Our analysis of the report data identified 1,785 potential instances where the FBI requested subpoenas based on information found exclusively in the administrative case files, where no investigation had been initiated. We reviewed 136 of the 1,785 potential instances and found that the FBI had requested and obtained grand jury subpoenas without opening a preliminary or full field investigation for 119 (87.5 percent) of the 136 files tested.

Second, we sought to determine whether the FBI's use of grand jury subpoenas in these instances was consistent with the applicable Attorney General's Guidelines. At the time of our audit, two sets of Attorney General's Guidelines governed the FBI's efforts to address potential terrorist threats and suspicious incidents: (1) the Attorney General's Guidelines on General Crimes, Racketeering Enterprise, and Terrorism Enterprise Investigations (General Crimes Guidelines); and (2) the Attorney General's partially classified Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSI Guidelines).

The General Crimes Guidelines govern the FBI's general crimes and criminal intelligence investigations, and also identify the circumstances under which domestic threat assessments and counterterrorism

[5] In most instances, these grand jury subpoenas were issued to identify the owners of specific telephone numbers or internet service provider addresses.

investigations may be started. In addition, the General Crimes Guidelines govern the permissible scope, duration, subject matters, and objectives of such investigations. There are three stages of investigative activity described in the General Crimes Guidelines – checking of leads, preliminary inquiries, and full investigations.

The General Crimes Guidelines do not specifically address whether grand jury subpoenas can be used in the checking of leads investigative stage – that is, before opening a preliminary inquiry or a full field investigation. Rather, the Guidelines authorize the use of "all lawful investigative techniques," with limited exceptions not relevant to this review. However, the Guidelines also state that the investigative activity that is permissible prior to the opening of a preliminary inquiry or full field investigation is restricted to "the prompt and extremely limited checking out of initial leads." The General Crimes Guidelines do not address whether specific investigative techniques, such as grand jury subpoenas, are or are not covered by this limitation.

By contrast, the NSI Guidelines, which relate to the investigation of international threats related to national security, specifically describe the investigative techniques permitted at each stage of investigation. The NSI Guidelines clearly state that the FBI may not use grand jury subpoenas during pre-investigation threat assessments. The NSI Guidelines further state that threat assessments are "comparable to the checking of initial leads in ordinary criminal investigations." However, the NSI Guidelines also provide that matters within their scope, such as crimes related to international terrorism, may also be investigated under the General Crimes Guidelines.

We discussed with the FBI Office of the General Counsel (FBI OGC) and the Department of Justice Office of Legal Policy (OLP) whether the FBI's use of grand jury subpoenas to assess leads without first opening a preliminary inquiry or full investigation was consistent with the Attorney General Guidelines. The FBI OGC asserted that the FBI was permitted to obtain grand jury subpoenas in these cases at the pre-investigation stage, noting that nothing in either the NSI or General Crimes Guidelines requires the FBI to make an immediate determination at this early investigative stage regarding which set of guidelines govern a case and that therefore any technique permitted by the General Crimes Guidelines was available to the FBI to assess Guardian leads. Moreover, the FBI asserted that, because the General Crimes Guidelines do not specifically prohibit the use of grand jury subpoenas during the "checking of leads," but rather permit "any lawful investigative technique," grand jury subpoenas were a legitimate investigatory tool for the FBI to utilize. The FBI OGC stated that the use of

grand jury subpoenas was an efficient and effective means of determining whether further investigation of a particular threat was warranted.

We also discussed this issue with the attorney in OLP who is an expert on the Attorney General Guidelines. The OLP attorney recognized that the General Crimes Guidelines were not explicit regarding the propriety of using grand jury subpoenas at the leads-checking stage, but agreed with the FBI OGC's view that the technique was permissible. He explained that the General Crimes and NSI guidelines are structured differently and use different means to limit the scope of permissible investigative activity in this context. The General Crimes Guidelines do not place specific restrictions on the techniques permitted at the lowest stage of investigative activity – the "prompt and extremely limited checking out of initial leads" – but rather limit activities at that stage through the requirement that they be "prompt and extremely limited" in character. In contrast, the NSI guidelines do not limit the duration of activities conducted at the corresponding ("threat assessment") stage, but limit such activities in a different way by listing the investigative techniques available at that stage, a list that does not include the use of grand jury subpoenas. Accordingly, in his view it is not sound to draw analogies between investigative techniques permitted under the General Crimes and NSI Guidelines in checking investigative leads. The OLP attorney also agreed that neither set of guidelines requires the FBI to decide immediately to proceed under the NSI Guidelines rather than the General Crimes Guidelines in a particular case.

In sum, it appears that the FBI is not required before initiating pre-investigative activity to determine which set of guidelines apply. Moreover, according to the OLP, the FBI's use of grand jury subpoenas to assess the threats in the matters we tested was permissible under the Attorney General Guidelines.

We note that the Department of Justice has revised and combined into one document the General Crimes Guidelines, the NSI Guidelines, and other Attorney General guidelines. The new guidelines were issued and made public by the Attorney General and FBI Director on October 3, 2008. The Attorney General Guidelines on Domestic FBI Operations are slated to go into effect on December 1, 2008. These new, consolidated guidelines carry forward the three stages of investigation used in the NSI Guidelines – assessments, preliminary investigations, and full investigations. The guidelines specifically authorize certain methods that can be used during an assessment, including the use of grand jury subpoenas for telephone or electronic mail subscriber information.

Automated Case Support System Testing

FBI field offices frequently uncover threat and suspicious incident activity during the course of ongoing counterterrorism investigations. The FBI currently tracks investigative cases in its ACS system.[6]

The CTD recognizes that some threat information can be so critical that an investigation should be opened immediately without entering the threat information in Guardian. Following the issuance of Guardian 2.0, the CTD provided the field offices with the following guidance for recording this type of threat information in Guardian:

> In all instances that involve the immediate opening of an official investigation, upon receipt of a terrorist related threat or suspicious activity report, a Guardian record must be created to summarize the nature of the incident. The record can be immediately marked complete after referencing the case file number.

To assess the number of incidents that were investigated with case files created in the ACS system but not included in the Guardian threat tracking system, we obtained a listing of all terrorism-related cases in the ACS system that did not have a corresponding reference to a Guardian incident number for the six field offices we visited. The report identified 546 ACS cases without an associated Guardian incident number. We selected a sample of 177 of the 546 ACS cases and found that 81 cases (46 percent) were opened in the ACS system but did not have an associated Guardian record.

FBI guidance identifies certain instances where threat information can be excluded from Guardian. Specifically, FBI guidance states that information derived from investigations utilizing sensitive sources or information obtained from more intrusive investigative techniques should not be included in Guardian.[7] We applied this criteria during our testing and found that the 81 cases we identified that required an entry in Guardian did not include information obtained through sensitive sources or intrusive investigative techniques.

---

[6] The FBI plans to replace the ACS system with the Sentinel Case Management System. The projected implementation date is 2009.

[7] The Attorney General's Guidelines identify more intrusive investigative techniques that may only be used during preliminary and full investigations. The information obtained during these investigations should not be included in a system that is designed for pre-case threat information.

We asked case agents why they did not include some of the threat information in Guardian. Some agents said that they thought it was redundant to include threat information in both the ACS system and Guardian because agents who had access to Guardian would also have access to the ACS system. However, according to FBI management officials, some of the FBI's other government partners have access to threat information in Guardian but do not have access to the ACS system. As a result, incident information entered only in the ACS system may not be available to all government agency partners. Other agents told us that they were not aware of the requirement to enter threat information in Guardian after an investigative case had been opened in the ACS system.

Other E-Guardian and Guardian Concerns

We also discovered additional concerns relating to delays in the deployment of E-Guardian and the implementation of Guardian maintenance patches designed to ensure optimal system operation.

The Foreign Terrorist Tracking Task Force provides technical assistance for projects such as the E-Guardian and Guardian applications. During the course of our audit, we found the Foreign Terrorist Tracking Task Force experienced considerable staff turnover. In addition, the FBI replaced the contractor that developed and provided technical support to Guardian. As a result, deployment of the E-Guardian application under development during our audit was delayed. Both the FTTTF and Office of the Chief Information Officer officials said that the E-Guardian project's delay was affected by the contractor change. Moreover, the FBI must develop or purchase new software to complete E-Guardian because the FBI's original contractor did not completely document the software used to develop Guardian.

The FTTTF also provided enhancements to Guardian through a series of maintenance patches designed to update Guardian's software and ensure optimal system operation. An FTTTF official said the goal for implementing the patches was to provide quarterly updates to Guardian. However, an SSA who was involved with threat assessments said the quarterly patches were 6 months behind schedule, and she believed Guardian needed to be updated more frequently.

FBI officials acknowledged that the change in contractor support reduced the number of technical professionals with the expertise to provide enhancements and maintenance patches. Consequently, the Guardian update program fell behind schedule. Because Guardian is critical to the FBI's terrorist threat tracking and management process, any additional delays in the implementation of maintenance patches could hamper the

system's ability to track terrorist threats and suspicious incidents. We believe that the FTTTF needs to prioritize updates to the system and develop a schedule to ensure enhancements and maintenance patches are completed in a timely manner.

Threat and Suspicious Incident Performance Reporting

With the FBI's policy to investigate every credible threat it receives, the allocation of resources to perform this function is critical. The number of terrorist threats and suspicious incidents entered into Guardian has increased on an annual basis, rising 51 percent between FYs 2005 and 2006. Over the same period of time, the number of registered Guardian users increased 11 percent. However, we found that the FBI has not taken adequate steps to plan for such increases.

During our fieldwork, we found that certain field offices collected terrorist threat and suspicious incident performance measurement data and that Guardian has the capability to create reports that could be used to measure performance. However, the FBI had not established performance measurements to address the number of hours expended during the threat resolution process or to report the effectiveness of its efforts to resolve terrorist threats and suspicious incidents.

As previously discussed, we identified a number of threats that received no investigative activity for over 30 days. We believe that developing performance measures could also help the FBI ensure that extended periods of inactivity would be recognized more quickly by supervisors and management. Additionally, performance measures would help the FBI consistently manage its staffing workloads and enhance the FBI's efforts to deploy critical resources to the areas of need and priority. Further, because the threat resolution process relies heavily on the investigative judgment of both Special Agents and supervisors, threat resolution-based performance measurements could also help the FBI identify instances where resource reallocations are warranted.

Conclusion and Recommendations

Guardian is an incident reporting and management system that collects, stores, and manages terrorist threats and reports of suspicious activities. Moreover, E-Guardian's future deployment should further enhance the FBI's efforts to share threat information among state and local law enforcement partners.

However, our review found that the FBI's use and maintenance of its Guardian system requires several improvements. The FBI needs to better ensure the accuracy, timeliness, and completeness of the information entered in Guardian. Additionally, we found that the Guardian system requires better oversight and updates to improve its functionality and value. We also concluded that the FBI should better utilize the reporting functions within Guardian to better determine the workload needs of addressing every terrorist threat and suspicious incident.

Our audit made seven recommendations to improve the FBI's tracking of terrorist threats and suspicious incidents, including ensuring the timely completion and supervisory review of all Guardian incidents, assuring appropriate information from ongoing counterterrorism cases is included in Guardian, developing and implementing a schedule to ensure technical patches to the Guardian system are completed in a timely manner, and develop and utilize performance measures to ensure critical resources for addressing threats and suspicious incidents are deployed effectively.

TABLE OF CONTENTS

INTRODUCTION

Shortly after the September 11 terrorist attacks, three FBI field offices began using an application called the Terrorist Activity Reporting System to track and monitor terrorist threats and suspicious incidents.[8] Soon after, this application was further developed and integrated throughout the FBI. It has become the cornerstone of the FBI's terrorist threat assessment process for supporting the identification, collection, management, evaluation, analysis, and dissemination of all terrorist threats and suspicious incidents up to the secret classification level.

Guardian Threat Tracking System

In 2002, the FBI upgraded the Terrorist Activity Reporting System to allow for multi-field office use and deployed a pilot terrorist threat tracking application, called Guardian, to select field offices. After successfully testing the pilot program in 2004, the FBI deployed an updated version of Guardian, Guardian 1.4, for use throughout the FBI on its internal computer network. In October 2006, the FBI deployed another upgraded version, Guardian 2.0, which remains in use today.

Counterterrorism threats and suspicious incidents are captured, stored, and assigned in Guardian, which can be searched by all FBI employees and other government agency partners who the FBI has determined need counterterrorism-related intelligence information. Guardian has grown into a sizeable threat tracking system over the years. As of November 2007, FBI officials stated that the system included approximately 108,000 potential threats, suspicious incidents, and terrorist watchlist encounters.[9]

The FBI is developing an additional threat tracking system to complement Guardian, called E-Guardian. E-Guardian is designed to facilitate the sharing of threat and suspicious incident information between the FBI and its state, local, and tribal law enforcement partners that do not have access to Guardian. Users will be able to access E-Guardian to enter incidents, view incidents, search data, or build reports. Additionally, users will be able to transfer data to other software applications using E-Guardian's data export capabilities. However, deployment of E-Guardian,

---

[8] The Terrorist Activity Reporting System was initially named the Baltimore Area Threat Tracking System because the Baltimore Field Office developed the initial application.

[9] The FBI defines an incident as a suspicious activity or threat that is tracked in Guardian to completion.

originally scheduled for October 2007, has been delayed. E-Guardian is now planned to be implemented in phases nationwide, and the FBI plans to fully complete its rollout by the end of 2008.

Guardian 1.4

The initial deployment of Guardian 1.4 in 2004 provided the FBI with a terrorist threat tracking system that included: (1) an electronic environment for the management of counterterrorism threats, (2) a centralized database for all counterterrorism threats received by both the FBI headquarters and the field offices, (3) a database to enter and search threats in real time, (4) an historical record of the investigative activities applied to address the threat, from entry of the threat to closure in the system, and (5) a tool to ensure threats are expeditiously assigned to an agent to investigate.

Guardian 2.0

The current version of the terrorist threat tracking system, Guardian 2.0, provides additional features to enhance the FBI's ability to assess and resolve terrorist threats and suspicious incidents. Guardian 2.0 enhancements include: (1) improved methods to route work, assign and accept tasks, and manage resources; (2) improved methods to share investigative data in support of intelligence analysis; (3) an increased capability to share investigative data with other government agency partners; and (4) a new capability that permits agents to auto-populate Guardian threat information directly in the FBI's Automated Case Support (ACS) system for additional investigation and threat resolution.

Guardian Concept of Operations

Guardian was developed to assure that all threats and suspicious activities are assigned and investigated, multiple users have real time access to investigative developments, and trend analysis up to the SECRET level can be conducted.

Guardian was intended to provide both the FBI and its government agency partners with the tools to track suspicious activity, add or update terrorist threat information, and perform analysis against the collected data. A definition for each class of Guardian user follows.

Guardian Classes of Users

User Roles	Definition
Administrator	Privileged user who creates and administers user accounts and the application to ensure compliance with policy. There are local and enterprise administrators. Local administrators can only affect their assigned office, while enterprise administrators can affect the entire organization.
Incident Assignee	An individual responsible for an incident.
Incident Author	An individual who initially enters the threat or suspicious activity report.
Supervisor	Supervisor of a group that owns and is responsible for the incident.[10]
Guardian User	An individual granted access to system functionality in accordance with FBI policies.

Source: Guardian 2.0 Concept of Operations

Guardian's Threat and Suspicious Activity Service is used to manage and track all suspicious activities and threats entered by Guardian users. This service is based on the following activities:

Incident Entry – As threats and suspicious activities are reported, the details associated with the threat are entered in Guardian. As additional investigative work is completed, information is added to the incident to update the status.

Incident Management – Assistance can be requested from offices to ensure incidents are investigated in a timely manner. These tasking requests are tracked and the system provides reporting capabilities on the status of the requests. For example, if investigative assistance is required by a field office from the FBI Counterterrorism Division (CTD) or another field office, the request can be tracked in Guardian.

Guardian Processing

The Guardian process to manage suspicious activities and threats can be summarized in three major areas.

Entering a Suspicious Activity/Threat – An incident entry is created when a suspicious activity or threat is entered in Guardian. The

[10] Guardian includes two supervisory levels called the owning and receiving groups. The supervisor of the Receiving Group has the authority to make assignments and reject incidents. For our audit, we limited our testing to the Owning Group, the group that is responsible for addressing the potential threat.

Guardian user records details about the suspicious activity or threat and enters this information in the Facts of Incident field. Once the incident is recorded and saved, it is available for review and assignment.

Modifying an Existing Suspicious Activity/Threat – Through their investigative lifecycle, incidents are updated with additional information. Authorized users have the ability to add information to an incident. For example, Intelligence Analysts, Special Agents, and Supervisory Special Agents (SSA) can add individual notes to an incident after the incident is assigned to them.

Closing a Suspicious Activity/Threat – Once a field office has completed its investigation of an incident, it can mark the incident as completed. The supervisor adds additional remarks as to the assessment of the incident to close the incident.

After completing the entry of an incident, a user submits the incident to the SSA for approval. After the SSA approves the incident entry, Guardian automatically generates a FD-71a complaint form, and the information from the FD-71a is automatically entered in the ACS system.[11] The FBI provided the following hypothetical example to describe a typical initial threat assessment utilizing Guardian's capabilities.

Guardian is intended to provide the capability to manage incidents through their entire lifecycle and account for all work performed against the incident. Guardian also provides a Workflow and Task Management Service that allows users to electronically task individuals and groups to investigate an incident. The workflow service allows supervisors to route incidents through various FBI field offices. Within the field office, the investigative squad supervisor can assign the incident to a squad member for investigative follow up.

Guardian Analytical Tools

Guardian also provides a Search Service that allows users to search all incidents in the system. The Search Service can locate records and search information contained in all Guardian incidents. Users can filter the information against which the search is conducted, such as:

[11] The FD-71a is the FBI's standard complaint form. If a preliminary investigation or full field investigation is not initiated, the Guardian incident information is retained in the ACS system for its intelligence value.

- the organizational structure (e.g., individual, group, office);
- the time period in which the information was obtained;
- incident location (e.g., all incidents within Los Angeles, CA);
- information categorizing incidents (e.g., type of incident, type of method, alleged organization); or
- information categorizing sources of information (e.g., state, local, or federal agency).

To provide the capability for trend analysis of threats, and to ensure that threats are properly investigated, Guardian also provides a Threat Reporting Service. Guardian can create both ad hoc and predefined reports to allow users to track investigative activity on an incident and provide trend analysis of threats. Ad hoc reports address unique or specialized needs, such as reports summarizing the number of terrorist incidents related to the oil and natural gas industry. The user specifies the report's criteria and parameters, identifies the information to include in the report, and formats the display of the information reported.

Predefined reports are designed to present statistical measures of information within Guardian. Guardian supports several broad categories of predefined reports including statistical, resource management, program management, incident management, and audit reports. The FBI provided the following two examples of typical reports that Guardian can generate:

(1) To support the yearly reallocation of personnel, an Assistant Special Agent in Charge in an FBI field office can generate a report showing all incidents assigned to the office's operational squads and detailing the statistics on each incident to evaluate the relative performance of the squads.

(2) FBI Headquarters can generate a report to answer a Congressional inquiry about the number of threats reported last year and how many of those threats resulted in the opening of a terrorism investigation.[12]

[12] The capability to report incidents reported in Guardian to specific cases opened in the ACS system is under development.

Department of Justice and FBI Terrorist Threat Policies and Guidelines

During our review, we tested the FBI's compliance with the Guardian 2.0 Policy and System Guidelines (Guardian System Guidelines), and the FBI's Guardian 2.0 User's Guide (User's Guide) regarding the accuracy, timeliness, and completeness of the incident information entered by users in Guardian. We also tested the FBI's compliance with the Attorney General's Guidelines on General Crimes, Racketeering, and Terrorism Investigations (General Crimes Guidelines) and the partially classified Attorney General's Guidelines for National Security Investigations (NSI Guidelines) regarding the FBI's process for requesting subpoenas.

Guardian-related Guidelines

To ensure all threats and suspicious incidents recorded in Guardian are assessed in a timely manner, the Threat Monitoring Unit (TMU) established Guardian-related Guidelines. These guidelines identify the requirements for the administration and management of Guardian and for the training of Guardian users. Additionally, the CTD developed a comprehensive Guardian User's Guide that identifies the specific actions required by Guardian users to enter, approve, assign, assess, and close potential or known terrorist threats and suspicious incidents.

Attorney General Guidelines

The Attorney General's General Crimes Guidelines provide guidance for FBI general crimes and criminal intelligence investigations. These guidelines identify the circumstances when threat assessments and counterterrorism investigations may be started, as well as the permissible scope, duration, subject matters, and objectives of the investigations.

The NSI Guidelines establish additional standards for the FBI to follow when investigating threats related to national security. The guidelines require that the FBI open a preliminary investigation or full field investigation before conducting certain investigative activity in national security cases, such as obtaining a subpoena.

OIG Audit Approach

The Department of Justice Office of the Inspector General (OIG) initiated this audit to evaluate the FBI's use of Guardian to identify, track, and address terrorist threats and suspicious incidents. To accomplish these objectives we examined: (1) the FBI's use of Guardian, (2) its threat assessment processes and operational guidance established by FBI

headquarters, and (3) its threat assessment policies and procedures in practice at the six field offices we visited.

To conduct this review we: (1) reviewed threat management documents developed by the FBI's Counterterrorism Division; (2) interviewed FBI officials and Guardian users assigned to various headquarters locations; (3) interviewed FBI officials and Guardian users at select field offices; (4) examined the process followed by the FBI in developing, implementing, maintaining, and updating Guardian; (5) tested samples of terrorism-related incidents tracked in Guardian; and (6) tested samples of counterterrorism-related cases in the FBI's Automated Case Support system.

Threat assessment investigative activities are normally conducted by Special Agents assigned to FBI field offices, supplemented by investigative support from the CTD. Our audit focused on the investigative activities reported in Guardian to address terrorist threats and suspicious incidents at the six field offices we visited, as well as the investigative support and oversight provided by the FBI's CTD.

We tested 218 Guardian incidents to determine if the FBI: (1) completed the required supervisory reviews of each threat and suspicious incident reported in Guardian, (2) addressed each incident in a timely manner, and (3) accurately and thoroughly reported the details of the incident in Guardian. We also tested 177 FBI terrorism cases reported in the ACS system to determine if the FBI included in Guardian all of the threat and suspicious incident activities identified during ongoing investigations. In addition, we tested the FBI's compliance with the Attorney General's investigative guidelines regarding subpoenas requested prior to opening a preliminary or full field investigation. Appendix I contains further discussion on our audit objectives, scope, and methodology.

FINDING AND RECOMMENDATIONS

Guardian is a significant improvement over how the FBI tracked and handled threat information in the past by providing users with the ability to enter suspicious activity and threat information and to manage threat assessments through an automated electronic workflow process. Guardian 2.0 provides immediate threat information to users and provides the capability to search threat information for trends and patterns. However, our audit identified areas where the FBI needs to improve its use of Guardian, including: (1) ensuring all field offices complete and document the required supervisory review of Guardian incidents; (2) ensuring Guardian incidents do not remain unaddressed in the system for extended periods and; (3) ensuring Guardian users consistently record detailed information about the threat. We also found FBI guidance regarding Guardian generally requires all threat information obtained during counterterrorism investigations and recorded in its Automated Case Support (ACS) system be entered in Guardian. However, in almost half the cases we tested users did not enter the required threat information from ACS in Guardian. In addition, we found instances where the FBI obtained grand jury subpoenas related to the assessment of threats and suspicious incidents before opening a preliminary or full field investigation. Through our review of the guidelines and through discussions with the Office of Legal Policy (OLP), it appears that this practice is permissible under the Attorney General's Guidelines. Finally, we concluded that the FBI could improve the use of Guardian's reporting capabilities to develop performance measures and better allocate its resources for addressing reported threats and suspicious incidents.

FBI Process to Address Potential Threats and Suspicious Incidents

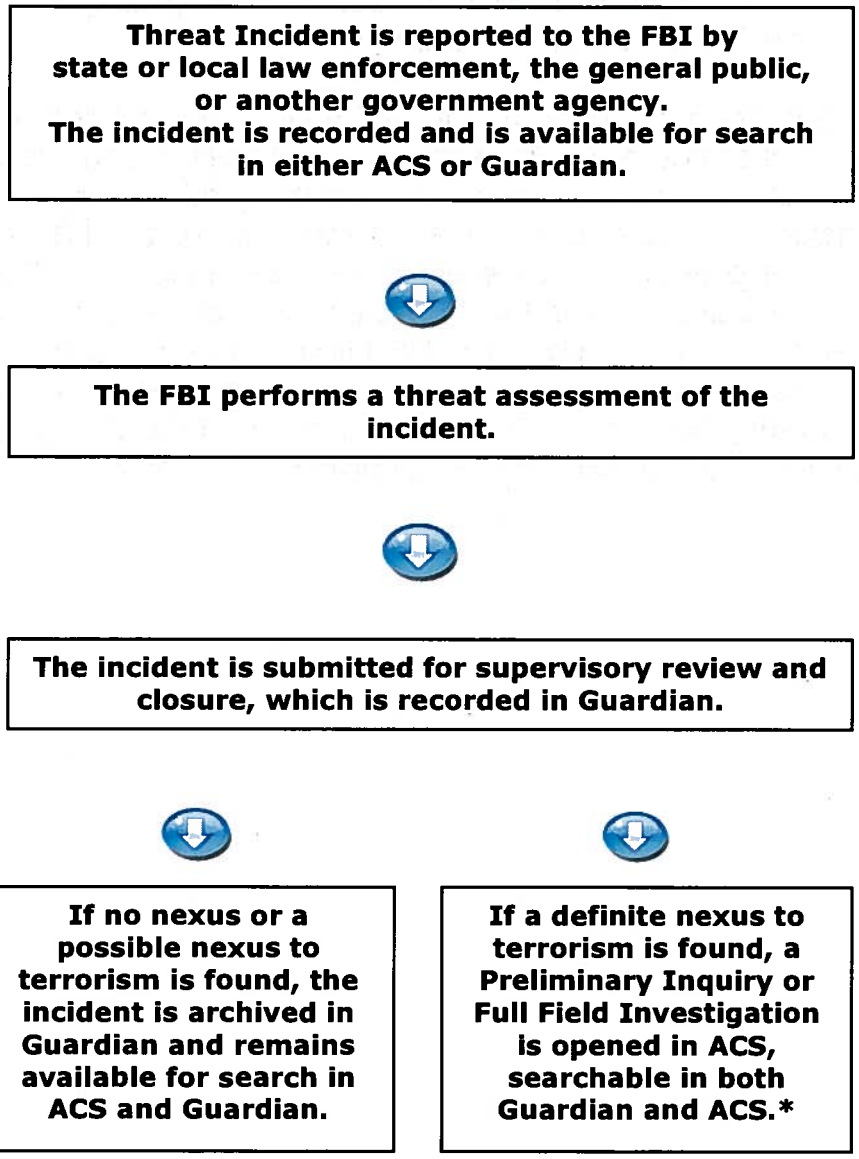
The FBI receives terrorist threat and suspicious incident information from a variety of sources, including: (1) the general public, (2) other government agency partners, (3) state and local law enforcement, (4) ongoing FBI investigations and intelligence assessments, and (5) FBI Legal Attachés.

Contacts from the general public generate a large number of threats and suspicious incidents that are reported to the FBI through telephone calls, e-mail, mail correspondence, or through the FBI's website. From our

review of FBI database information, we determined that during fiscal year (FY) 2006, the public provided the FBI with approximately 219,000 tips that resulted in over 2,800 counterterrorism threats and suspicious incidents entered in Guardian for investigative follow up.

Regardless of the reporting source, FBI policy requires that each threat or suspicious incident should receive some level of review and assessment to determine the potential nexus to terrorism and the creditability of the threat or suspicious incident. Guardian provides the vehicle for the FBI to track, assess, and manage pre-case threats and suspicious incidents. The results of those assessments are recorded in Guardian. Certain assessments are upgraded to preliminary inquiries or full field investigations, and other assessments are closed with the information retained in Guardian for possible future intelligence value. The graphic on the following page provides an overview of the FBI's threat disposition process.

OVERVIEW OF THE FBI'S THREAT INCIDENT DISPOSITION



*If the incident was initially reported in ACS and no corresponding entry was made in Guardian, the incident will only be searchable in ACS.

At FBI field offices, threats and suspicious incidents are normally entered in Guardian by either Special Agents specifically assigned to Guardian squads, or by the Special Agent or Intelligence Analyst who initially

received the threat information.[13] A Guardian pre-case incident entry field creates a task for the supervisor to determine if the threat is credible.[14]

If the supervisor determines the threat is credible, the supervisor assigns a Special Agent or Intelligence Analyst to investigate the threat or incident. The agent or analyst performs the necessary investigative work, returns the results to the supervisor, and requests closure of the incident in Guardian. The supervisor reviews the completed investigative work and, if the supervisor determines the incident is adequately investigated, the incident is considered addressed and the supervisor closes the pre-case incident in Guardian.

If the supervisor determines that additional investigative work is necessary, the supervisor returns the task to the agent or analyst. If the FBI's pre-case threat and suspicious incident assessment work finds a nexus to terrorism, a preliminary or full field investigation is initiated. If no definite nexus to terrorism is found, the incident information is retained in Guardian for its intelligence value, but no investigation is initiated.

OIG Evaluation of the FBI's Terrorist Threat Processing

We visited six FBI field offices and tested a sample of the terrorism-related incidents entered in Guardian to determine if the field offices: (1) completed the required supervisory reviews of each threat and suspicious incident reported in Guardian, (2) addressed each incident in a timely manner, and (3) reported the details of the incident in Guardian. We selected the following field offices to provide perspective from a cross-section of the FBI field organization in terms of field office size, operational activity, and geographic location.

- Philadelphia, Pennsylvania
- Washington, D.C.
- New York, New York
- Detroit, Michigan
- Kansas City, Missouri
- Los Angeles, California

---

[13] Guardian squads are specialized units at FBI field offices that conduct terrorism-related threat assessments utilizing the Guardian system.

[14] A non-credible threat submitted solely due to a person's nationality could be immediately removed from Guardian based on the supervisor's judgment. Alternatively, a non-credible threat with no obvious nexus to terrorism could be immediately closed by the supervisor, but retained in Guardian for its intelligence value, based on the supervisor's judgment.

Sampling

We obtained from the FBI a universe of Guardian threat incidents for each of the field offices we selected. The universe included incidents with inactivity of 30 days or more and recorded after October 23, 2006 – the date the latest version of Guardian was implemented. We did not test incidents recorded in the previous version of Guardian because that version had substantially less functionality than the current version of Guardian and did not archive the same data in the current version of Guardian.

In selecting our judgmental test samples for each field office, we sought to include a minimum of 10 percent of the total threat incidents recorded in Guardian for the 6 sampled field offices in our universe, with a minimum of 25 and a maximum of 50 incidents tested at each field office. Our testing sample included all incidents open for over 30 days at each field office. Our total testing sample for the 6 field offices included 218 threat incidents. The following table illustrates the threat universes we found for each of the six field offices during the period October 23, 2006, through June 22, 2007, and the testing sample we drew from each.

Guardian Incident Universe and Number of Incidents Selected for Testing by Field Office

FBI Field Office	Total Guardian Incident Universe	Guardian Incidents Selected For Testing
Philadelphia	81	25
Washington	285	33
New York	537	50
Detroit	115	30
Kansas City	32	30
Los Angeles	571	50
Total	**1,621**	**218**

Source: FBI Counterterrorism Division

We reviewed additional data from the New York Field Office because we found, in addition to the 537 incidents in our sample universe, over 700 open incidents in the prior version of Guardian that were entered before October 2006. We added a sample of 30 more incidents at the New York Field Office only to determine the causes for these incidents remaining open for an extended period.

Testing

Guardian's ability to accurately track threats depends on the accuracy, timeliness, and completeness of the incident information entered by users of the system. At each field office we visited, we tested the key attributes we considered essential to successfully entering, updating, and managing incidents in Guardian: (1) the completeness of the incident summary, (2) supervisory oversight of the incident, (3) timeliness of investigative activity, and (4) completion of Guardian's supplementary search tabs.

Guardian Incident Summary

Users are required to enter threat data in Guardian through a screen called the Incident Summary Screen, which provides a summary of the terrorist threat or suspicious incident and describes the details of a terrorist threat or suspicious incident. We reviewed the Incident Summary Screen for the 218 sampled incidents to determine if the users entered the incident completely. We found that all of the necessary summary information was included in the incidents we tested.

We believe the FBI's completeness in the initial incident recording is a result of the training provided to Guardian users through its Virtual Academy. The FBI's Virtual Academy is a computer-based training initiative that provides FBI personnel with access to a wide range of training from their desktop computers. In addition, the Foreign Terrorist Tracking Task Force (FTTTF) and the Threat Monitoring Unit (TMU) formed a deployable Guardian training team that visited most of the FBI's field offices. We believe that the initial training provided to the field agents contributed to the rapid assimilation and complete entry of initial incident information in the latest version of Guardian at the FBI's field offices.

Supervisory Oversight of the Guardian Incident

To provide supervisory oversight and improve the workflow process, users who enter information in Guardian are assigned one of three user roles: (1) investigator or analyst, (2) supervisor, or (3) administrator.

Investigator or Analyst. This user role is for individuals who enter Guardian incidents and are responsible for investigating and conducting analysis of terrorist related threats and suspicious activity reports. All work conducted by the investigator or analyst within Guardian must be submitted to the supervisor for review and approval.

Supervisor. Supervisory Special Agents (SSA) or Supervisory Intelligence Analysts review incidents submitted by investigators or analysts and certify that the assessment was sufficiently performed and that the incident information in Guardian is complete and accurate. Threats cannot be closed in the Guardian system until the supervisor approves the investigator or analyst's investigative work.

Administrator. The administrator performs a variety of administrative functions in Guardian, including activating accounts, reassigning incidents within an office, re-naming accounts, and changing user roles.

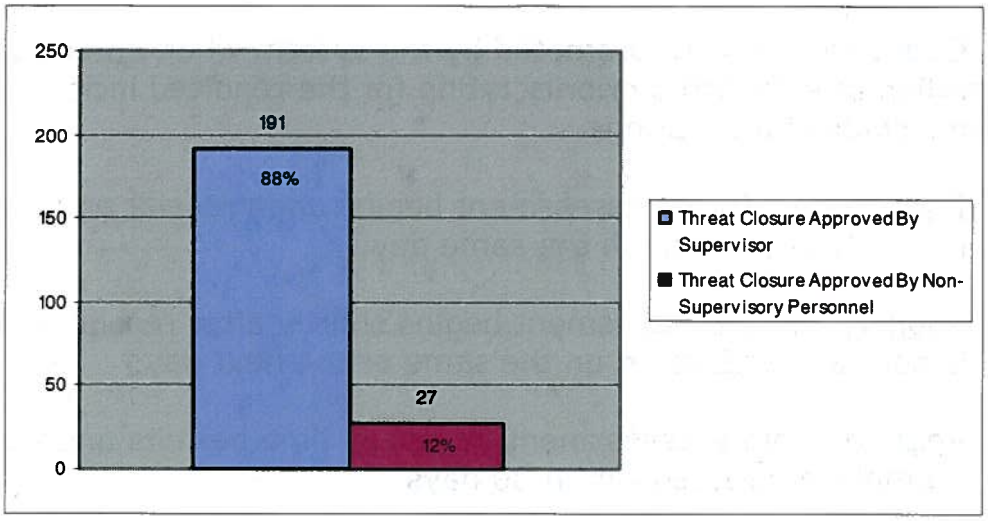
According to the Guardian User's Guide, an SSA or a Supervisory Intelligence Analyst is responsible for reviewing and closing each threat or suspicious incident in Guardian. The User's Guide requires the supervisor to then make a determination as to whether the threat is satisfactorily addressed or if additional investigation, analysis, or updating of the incident is required. The supervisor performs critical oversight during the Guardian threat assessment process because the supervisor provides the FBI's final quality assurance check to ensure that each Guardian threat assessment is resolved completely and accurately.

The FBI provided an example of an SSA initially receiving, assigning, and evaluating the Guardian incident:

> A special agent answers a phone call from an individual identifying himself as a microbiologist. The caller informs the FBI that his colleague was bragging about planning to send anthrax bacteria to the Governor at his office for cutting his department funding and that his colleague has extensive knowledge of biological agents and their use in warfare. The agent enters the threat information in Guardian, recording the details of the threat. After saving the threat, the incident is available for the supervising agent to review and route to the appropriate agency.

We reviewed the supervisory actions taken in each of the 218 Guardian incidents tested. For 191 (88 percent) of the incidents tested, we found the required supervisory review was entered in Guardian. However, in 27 (12 percent) of the incidents, the supervisor did not record the required supervisory review prior to closing the Guardian incidents.

Supervisory Oversight in Guardian



Source: OIG analysis of FBI data

At three FBI field offices that we visited (Washington, New York, and Los Angeles), we found that a supervisor reviewed each of the Guardian incidents we tested. We also found that the SSAs and the investigative squads responsible for the Guardian program in these offices understood the requirements of the Guardian threat tracking system. At these three field offices, the Guardian SSAs reviewed Guardian threats and suspicious incidents and rarely delegated the supervisory review of the incidents to another supervisor.

At the other three FBI field offices we visited (Detroit, Kansas City, and Philadelphia), we determined that supervisors did not review all Guardian incidents. At one of the field offices, the SSA assigned oversight responsibilities for the Guardian program was not aware of the Guardian supervisory requirements. At another field office, we found that the responsible SSA had technical problems accessing Guardian, and he delegated the closure of some incidents to a non-supervisor. At the third field office, the SSA delegated the supervisory closure to the Guardian administrator who was not a supervisory agent or analyst.

Thus, although CTD guidance clearly states the Guardian supervisory review requirements, three of the six field offices we visited did not meet those requirements. Threats and suspicious incidents are at risk of closure without complete and thorough assessment if a supervisor does not review Guardian incidents. We therefore recommend that the CTD should increase its oversight of the Guardian review program to ensure all Guardian incidents receive the required supervisory review.

Timeliness of Investigative Activity to Address Guardian Incidents

Guardian users are prompted by the system when entering an incident in Guardian to establish a priority rating for the reported incident. The system includes three ratings.

Immediate. Threat assessment begins upon receipt and the threat is normally addressed on the same day.

Priority. Threat assessment begins shortly after receipt and the threat is normally addressed on the same or the next day.

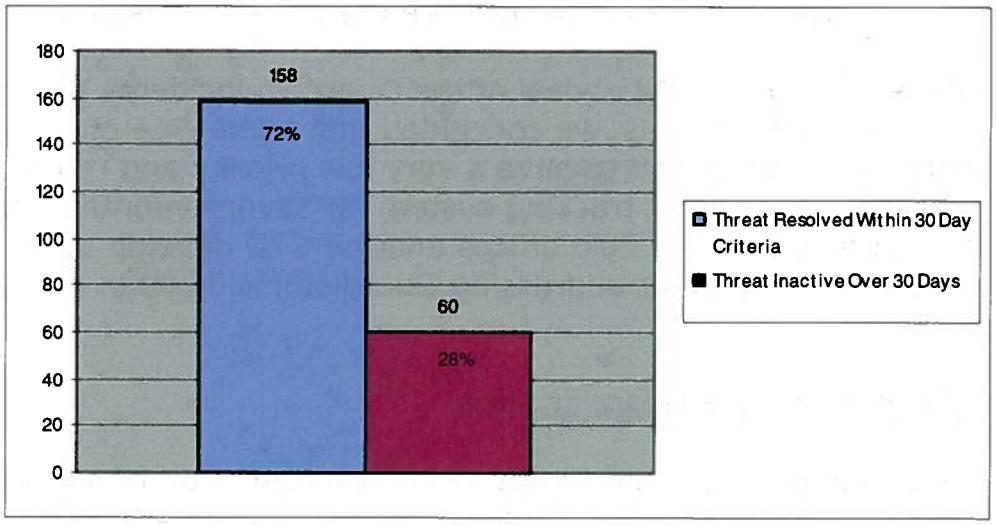
Routine. Threat assessment begins as time permits and the threat is normally addressed within 30 days.

The prompt assessment of terrorist threats and suspicious incidents is essential to ensure Guardian's database is complete and promptly updated. Delays in assessing Guardian incidents could also result in incorrect assessments of the threat or duplication of the Special Agent's work because the most current threat information will not be included in Guardian's database. During our review of 218 Guardian incidents, we examined the timeliness of the Guardian threat assessment process. At 5 of the 6 field offices we visited, we found 60 incidents (28 percent) that did not meet the 30-day criteria for routine assessments. At the remaining field office we found that all 25 incidents sampled were closed within the 30-day criteria. Because Guardian 2.0 provides real time threat information to all users we found that both the CTD and field office supervisors exercised adequate oversight over each threat and suspicious incident assessed at the priority or immediate level.

We discussed the timeliness criteria with SSAs at the FBI's headquarters and Special Agents at the field offices and found that they considered the 30-day period to address routine threats as guidance, not required criteria. We were told that some complex threats, such as threats that require contact with sources outside the United States, cannot be fully addressed within the 30-day guideline. FBI officials agreed that the current policy needs to be clarified.

Therefore, we also evaluated timeliness by examining threat assessments that included periods of inactivity in excess of 30 days. We analyzed FBI documentation and identified Guardian incidents that had not been addressed for a period in excess of 30 days. From the Guardian universe of over 2,450 open Guardian incidents, we identified 1,621 (66 percent) that remained open for a period in excess of 30 days.

Timeliness Testing



Source: OIG analysis of FBI data

We found 60 of the 218 incidents we tested (28 percent) with periods of inactivity that exceeded 30 days. We could not readily determine the reason for the extended period of inactivity based on the information available in Guardian because the incident information in Guardian did not include reasons for the periods of inactivity.

We found differing records of adherence to timelines for threat assessments in the field offices we visited. At the Philadelphia Field Office, we found that all 25 routine incidents sampled were closed within the 30-day requirement. The SSA responsible for the field office's threat management used a spreadsheet that accurately tracked the status of each of the open Guardian incidents at the field office. He also provided evidence that he routinely briefed the field office's senior managers on the status of all ongoing threat assessments in progress. Although other field offices produced evidence of briefings to field office senior management, in our view the Philadelphia Field Office's controls on the timely management of threat assessments was the most effective of the six field offices we visited.

By contrast, at the New York Field Office we identified 700 Guardian incidents that remained open for a period in excess of 90 days. We expanded our testing at this location to include an additional 30 Guardian incidents. We found 27 of the 30 additional tested incidents (90 percent) remained open beyond 90 days and several remained open for over 1 year. An SSA there said he believed the incidents had been closed at some point, but the conversion process that occurred during an update of Guardian caused the incidents to re-open. We did not find a problem with the

Guardian 1.4 conversion process at any of the other field offices we visited. From our review of the 27 incidents that remained open for over 90 days, we could not determine if the incidents were ever closed in Guardian.[15]

Based on our overall review of the Guardian incidents and our interviews with FBI officials, we concluded that some Guardian incidents in the system were perceived to have a very low priority and remained unaddressed in the threat tracking system for several months. We recommend that both the field offices and the CTD develop additional guidelines and controls for addressing Guardian incidents in a timely manner.

Completeness of Guardian Data

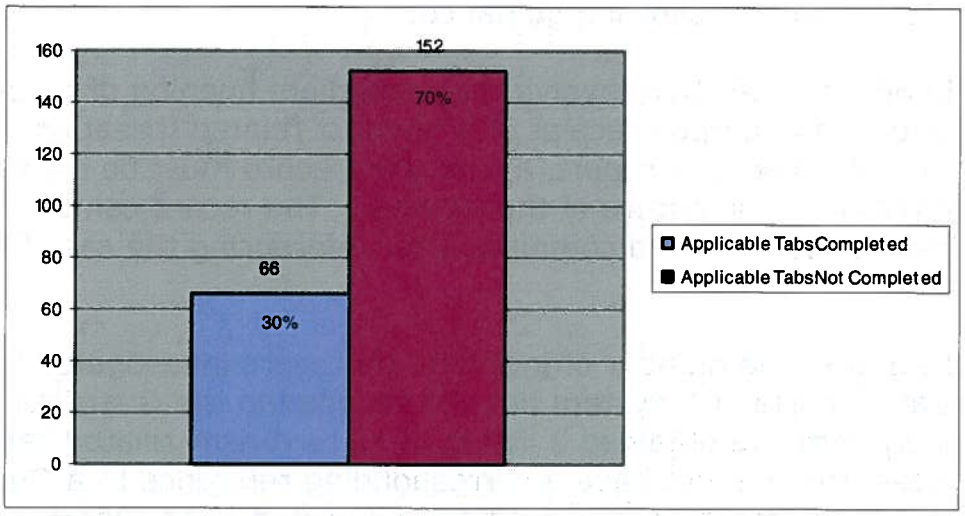
Guardian can separate threat incident information into its basic components, such as sources, targets (places), subjects (people), weapons or methods, and vehicles. The additional breakdown of threat information can provide Guardian users with enhanced search and trend analysis capability. After a user enters the threat information in Guardian, information can be searched by a particular threat component. The user completes a series of tabs within Guardian that provide specific details on the aforementioned threat components, such as sources, targets (places), subjects (people), weapons or methods, and vehicles. As a result, searches can be done for various types of information in Guardian, and trend information can be readily established.

For example, Guardian's Incident Vehicles Screen allows users to search for vehicles associated with an incident to determine if they were also associated in another incident. Guardian also has the ability to add a picture of a vehicle to the database. However, if a user does not enter full and complete data on a vehicle associated with an incident, the effectiveness of Guardian as a search tool to aid in the threat assessment process is reduced. Additionally, Guardian's ability to provide users with useful trend analysis of threats and suspicious incidents is similarly diminished.

As noted in the following chart, our testing found that users did not complete the supplementary tabs in 66 of the 218 incidents (30 percent) we tested.

[15] Most of the incident information we reviewed was entered through Guardian 1.4, and because of the limitations inherent in Guardian 1.4 we could not determine why the incidents remained open for long periods.

Supplementary Tabs Testing



Source: OIG analysis of FBI data

We also determined that the guidance the FBI provided to its Guardian users about completion of the supplementary tabs was inadequate. FBI policy does not clearly establish whether the completion of the supplementary tabs is required. Some FBI officials stated that they believed the completion of the supplementary tabs was essential because it improved Guardian's search and trend analysis capabilities. Other FBI officials stated that the increased workload generated by completing the supplementary tabs was not justified. As a result of the inconsistent application of this guidance, searches of Guardian can result in incomplete and inaccurate threat assessment information. We believe the CTD should issue definitive guidance to Guardian users regarding the completion of the supplementary tabs based on its assessment of the value added by the completion of the tabs.

Results of Automated Case Support System Testing

FBI field offices frequently uncover threat and suspicious incident information during the course of ongoing investigations. Sometimes the imminent nature of the threat requires that the FBI bypass the threat assessment process and immediately open an investigative case. The FBI currently tracks investigative cases electronically in its ACS system.[16]

The CTD recognized that threat information could be developed from an existing case and that an investigation should be opened immediately.

[16] The FBI plans to replace the ACS system with the Sentinel Case Management System. The projected implementation date is 2009.

Therefore, following the deployment of Guardian 2.0, the CTD provided the field offices with the following guidance:

> In all instances that involve the immediate opening of an official investigation, upon receipt of a terrorist related threat or suspicious activity report, a Guardian record must be created to summarize the nature of the incident. The record can be immediately marked complete after referencing the case file number.

To assess the number of incidents that were investigated with case files created in the ACS system but not included in the Guardian threat tracking system, we obtained a listing of all terrorism-related cases in the ACS system that did not have a corresponding reference to a Guardian incident number for the six field offices we visited. The report identified 546 ACS cases without an associated Guardian incident number. We selected a sample of 177 of the 546 ACS cases and found that 81 cases (46 percent) were opened in the ACS system but did not have an associated Guardian record. Appendix III shows the universe of FBI terrorism cases without a corresponding Guardian incident number for each of the six field offices we visited.

The FBI guidance regarding Guardian generally requires that all threat information obtained during counterterrorism investigations be included in Guardian. However, the FBI has issued additional guidance for specific instances when threat information should be excluded from Guardian. Specifically, information derived from investigations utilizing sensitive sources or information obtained from more intrusive investigative techniques should not be included in Guardian. Whether to exclude information from Guardian is left to the judgment of the agent performing the investigation.

In reviewing those cases where information was contained within ACS but not entered in Guardian, we asked agents why they did not include some of the required threat information in Guardian. Some agents said they were not aware of the requirement to enter threat information in Guardian after an investigative case had been opened in the ACS system. Other agents said that they thought it was redundant to include threat information in both the ACS system and Guardian because an agent who had access to Guardian would also have access to the ACS system. However, according to FBI management officials, some government agency partners have access to threat information in Guardian but do not have access to the ACS system. As a result, incident information entered only in the ACS system may not be available to all other government agency partners.

Moreover, the E-Guardian application currently under development, discussed later in this report, is designed to share threat information with state and local law enforcement partners, and E-Guardian uses threat information that is only available in Guardian. State and local law enforcement partners generally do not have access to the FBI's ACS system. Consequently, threat information entered only in the ACS system will not be shared with the state and local law enforcement community.

During the development of Guardian, FBI agents requested that the development team include the ability to enter threat information once in Guardian and automatically transfer the threat information to the ACS system. The development team included this capability in Guardian, and as a result threats entered in Guardian are now auto-populated in the ACS system. However, the reverse of the threat data entry process does not exist. That is, when threat information is entered in the ACS system, the information is not automatically entered in Guardian. Thus, useful threat information obtained during preliminary or full investigations and entered in the ACS system must be entered twice – once in the ACS system and a second time in Guardian. We believe this double-entry process contributed to the exclusion of some of the ACS-related threat data from Guardian.

We also found that the organizational structure of the field offices contributed to the exclusion of some threat information from Guardian. The investigative structure of each field office we visited varied slightly. The basic structure included a Guardian squad that was responsible for entering, tracking, and addressing threats in Guardian, and a counterterrorism investigative squad that was normally part of the field office's Joint Terrorism Task Force (JTTF).[17] The JTTF squad members conducted most counterterrorism investigations after the threat had been entered in Guardian and assigned to the JTTF for further investigation. Because the JTTF members typically enter counterterrorism investigations in the ACS system, they were not as familiar with the requirement to include most threat information in both Guardian and the ACS system.

We believe the CTD should ensure that all agents are aware of and follow the requirement to include appropriate threat information obtained from ongoing counterterrorism investigations in Guardian. This also would ensure that potentially valuable counterterrorism information gathered during the course of investigative case work is retained for future intelligence value and information sharing.

---

[17] The JTTFs include teams consisting of FBI Special Agents, state and local law enforcement officers, and other federal agencies who share information and work together to prevent acts of terrorism.

Attorney General Guidelines Testing

During our review of Guardian, we also found that in many instances the FBI had asked United States Attorneys' Offices to issue grand jury subpoenas related to the assessment of suspicious incidents before opening a preliminary or full field investigation.[18] We found that two of the four field offices we visited, New York and Los Angeles, sought and obtained grand jury subpoenas without opening preliminary or full field investigations. However, at the other two sites, Detroit and Kansas City, the FBI would not obtain grand jury subpoenas without first opening a preliminary or full investigation. Officials from the Kansas City and Detroit field offices indicated that they understood that obtaining grand jury subpoenas required the opening of a preliminary or full field investigation.

First, we sought to determine the extent of the FBI's practice of requesting subpoenas without opening a preliminary or full field investigation. To do this, we reviewed a computer-generated report from FBI headquarters that identified FBI subpoena requests supported by administrative case control file numbers for the period October 2006 through July 2007. Control files are administrative case files used by the FBI to store information in the ACS system that do not relate to preliminary or full field investigations.

The FBI report that we reviewed identified 4,067 grand jury subpoenas issued from October 2006 to July 2007. Our analysis of the report data identified 1,785 potential instances where the FBI requested subpoenas based on information found exclusively in the administrative case files, where no investigation had been initiated. Because of the large number of subpoenas that would be required for testing, we did not attempt to project our results over the FBI's entire universe of subpoenas. However, we concluded from our testing that the practice of issuing subpoenas supported by administrative control files was not confined to the two FBI field offices where we first discovered the issue.

Of the 200 subpoenas we tested, we removed 64 because we could not readily locate electronic files. We then reviewed the remaining 136 of the 1,785 potential instances and found that the FBI had requested and obtained grand jury subpoenas without opening a preliminary or full field investigation for 119 (87.5 percent) of the files tested. In 17 (12.5 percent) of the cases tested, we found documentation that indicated the subpoena

[18] In most instances, these grand jury subpoenas were issued to identify the owners of specific telephone numbers or internet service provider addresses.

request could be supported by investigative information from a preliminary or full field investigation.[19]

Second, we sought to determine whether the FBI's use of grand jury subpoenas in these instances was consistent with the applicable Attorney General's Guidelines. At the time of our audit, two sets of Attorney General's Guidelines governed the FBI's efforts to address potential terrorist threats and suspicious incidents: (1) the Attorney General's Guidelines on General Crimes, Racketeering Enterprise, and Terrorism Enterprise Investigations (General Crimes Guidelines); and (2) the Attorney General's partially classified Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSI Guidelines).

The General Crimes Guidelines govern the FBI's general crimes and criminal intelligence investigations, and also identify the circumstances under which domestic threat assessments and counterterrorism investigations may be started. In addition, the General Crimes Guidelines govern the permissible scope, duration, subject matters, and objectives of such investigations. There are three stages of investigative activity described in the General Crimes Guidelines – checking of leads, preliminary inquiries, and full investigations.

The General Crimes Guidelines do not specifically address whether grand jury subpoenas can be used in the checking of leads investigative stage – that is, before opening a preliminary inquiry or a full field investigation. Rather, the Guidelines authorize the use of "all lawful investigative techniques," with limited exceptions not relevant to this review. However, the Guidelines also state that the investigative activity that is permissible prior to the opening of a preliminary inquiry or full field investigation is restricted to "the prompt and extremely limited checking out of initial leads." The General Crimes Guidelines do not address whether specific investigative techniques, such as grand jury subpoenas, are or are not covered by this limitation.

By contrast, the NSI Guidelines, which relate to the investigation of international threats related to national security, specifically describe the investigative techniques permitted at each stage of investigation. The NSI Guidelines clearly state that the FBI may not use grand jury subpoenas during pre-investigation threat assessments. The NSI Guidelines further

---

[19] We completed a subject search within the ACS system, and for the 17 subpoenas we found the subject matter of the subpoena also pertained to an additional active case. However, based on the information available to us in the ACS system, we could not conclusively determine if the case supported the subpoena in our sample.

state that threat assessments are "comparable to the checking of initial leads in ordinary criminal investigations." However, the NSI Guidelines also provide that matters within their scope, such as crimes related to international terrorism, may also be investigated under the General Crimes Guidelines.

We discussed with the FBI Office of the General Counsel (FBI OGC) and the Department of Justice Office of Legal Policy (OLP) whether the FBI's use of grand jury subpoenas to assess leads without first opening a preliminary inquiry or full investigation was consistent with the Attorney General Guidelines. The FBI OGC asserted that the FBI was permitted to obtain grand jury subpoenas in these cases at the pre-investigation stage, noting that nothing in either the NSI or General Crimes Guidelines requires the FBI to make an immediate determination at this early investigative stage regarding which set of guidelines govern a case and that therefore any technique permitted by the General Crimes Guidelines was available to the FBI to assess Guardian leads. Moreover, the FBI asserted that because the General Crimes Guidelines do not specifically prohibit the use of grand jury subpoenas during the "checking of leads," but rather permit "any lawful investigative technique," grand jury subpoenas were a legitimate investigatory tool for the FBI to utilize. The FBI OGC stated that the use of grand jury subpoenas was an efficient and effective means of determining whether further investigation of a particular threat was warranted.

We also discussed this issue with the attorney in OLP who is an expert on the Attorney General Guidelines. The OLP attorney recognized that the General Crimes Guidelines were somewhat ambiguous regarding the propriety of using grand jury subpoenas at the checking of leads stage, but agreed with the FBI OGC's view that the technique was permissible under these Guidelines. He explained that the General Crimes and NSI guidelines are structured differently and use different means to limit the scope of permissible investigative activity. The General Crimes Guidelines do not place specific restrictions on the techniques permitted at any given stage of investigation and instead create time limits on investigative activity. He also said that the language in the General Crimes Guidelines restricting the earliest stage of investigative activity to the "prompt and extremely limited checking out of initial leads" means that, with two exceptions not relevant here, the FBI can use any lawful investigative technique to check out a lead, so long as that pre-investigative stage is concluded quickly. In contrast, the NSI guidelines explicitly list the investigative techniques available at each stage, without regard to how long each stage of investigative activity takes, and explicitly prohibit the use of grand jury subpoenas. Accordingly, in his view it is not sound to draw analogies between investigative techniques permitted under the General Crimes and NSI Guidelines. The OLP attorney

also agreed that neither set of guidelines requires the FBI to determine immediately which set of guidelines govern in a particular case.

In sum, it appears that the FBI is not required before initiating pre-investigative activity to determine which set of guidelines apply. Moreover, according to the OLP the FBI's use of grand jury subpoenas to assess the threats in the matters we tested was permissible under the Attorney General Guidelines.

We note that the Department of Justice recently revised and combined into one document the General Crimes Guidelines, the NSI Guidelines, and other Attorney General guidelines. The new guidelines – the Attorney General Guidelines on Domestic FBI Operations – were issued and made public by the Attorney General and FBI Director on October 3, 2008, and are slated to go into effect on December 1, 2008. These new, consolidated guidelines carry forward the three stages of investigation used in the NSI Guidelines – assessments, preliminary investigations, and full investigations. The guidelines specifically authorize certain methods that can be used during an assessment, including the use of grand jury subpoenas for telephone or electronic mail subscriber information.

FBI Headquarters Threat Assessment Management

The threat assessment process is centrally controlled and managed from FBI headquarters through three mechanisms: (1) the CT Watch, which operates a 24-hour global command center that has complete visibility and oversight responsibility over Guardian; (2) the Threat Monitoring Unit (TMU), which disseminates counterterrorism policy guidance to the field locations; and (3) the FTTTF, which develops Guardian terrorist threat tracking software. FBI field offices and Legal Attaché offices assist in administering the threat assessment process by tracking and following up on leads that reside within their geographic areas of responsibility.

To measure the effectiveness of the policy and procedural guidance as well as the oversight of the threat assessment process, we: (1) reviewed threat management documents developed by the CTD; (2) interviewed FBI officials at the FBI headquarters and Guardian users at field offices we visited; (3) reviewed the process followed by the FBI in developing, implementing, maintaining, and updating Guardian; (4) tested a sample of terrorism-related incidents tracked in Guardian; and (5) tested a sample of counterterrorism-related cases in the ACS system.

Counterterrorism Watch Unit

The primary mission of the CT Watch is to direct the immediate response to terrorism threats, incidents, and suspicious activities, and to provide oversight to FBI response operations. The CT Watch is the focal point for the receipt, preliminary analysis, and immediate assignment for action on all domestic and international terrorism threats. It also ensures the timely alert within the FBI and to its other government agency partners.

The CT Watch functions as the clearinghouse for counterterrorism threat information, and its personnel provide input to the FBI Director's morning and afternoon threat briefings. The CT Watch receives periodic updates regarding completed and pending investigative actions for dissemination to FBI leadership and the Intelligence Community. The CT Watch also shares terrorist threat information with the National Joint Terrorism Task Force (NJTTF), Homeland Security Operations Center, and Transportation Security Operations Center.

To facilitate the sharing of terrorist threat information: (1) the CT Watch is co-located with the NJTTF. The Department of Homeland Security (DHS) provides an analyst for each CT Watch shift, and the CT Watch Commander communicates directly with the Transportation Security Operations Center. Both the FBI's agents and analysts, as well as analysts at the FBI's other government agency partners who are approved Guardian users, have access to all of the terrorism threat tracking information in Guardian.

As threats are identified, the CT Watch acts as the conduit between the field and the FBI leadership. The CT Watch sometimes initiates certain investigative steps, although the vast majority of the investigative effort is performed by Special Agents in the field. The CT Watch oversees the investigative effort to ensure the FBI responds to these threats in a coordinated and logical manner. Guardian provides the CT Watch and FBI field agents with a counterterrorism incident management application to aid the management and tracking of terrorist threats and suspicious incidents.

The CTD developed an operating manual that includes threat assessment investigative oversight procedures. We also reviewed terrorist threat incidents in Guardian at each of the field offices we visited and found evidence of CT Watch oversight in the investigative process.[20] In addition,

[20] CT Watch oversight is limited to the initial review and assignment of the threat. Long term oversight concerning the management and timeliness of the Guardian records is the responsibility of the TMU and the field offices.

we interviewed field office supervisors, investigators, and analysts, who said they were satisfied with the support they received from the CT Watch.

Threat Monitoring Unit

The Threat Monitoring Unit (TMU) administers Guardian by:

- providing training to personnel granted access to the system,
- managing the Guardian Help Desk Team,
- coordinating with the FTTTF to address Guardian deployment and enhancement issues, and
- providing management controls over the timeliness and quality of the incidents reported in Guardian.

During our field office visits, Guardian users said they were satisfied with the training they received on the system. The TMU, working with the FTTTF, has developed a computer-based Guardian training program. Guardian users have access to the program through the FBI's Virtual Academy. Additionally, most of the Guardian users we interviewed were satisfied with the latest version of Guardian and the support provided by the Help Desk Team.

Foreign Terrorist Tracking Task Force

According to the FBI, the mission of the FTTTF is to provide information that helps keep foreign terrorists and their supporters out of the United States or leads to other legal action, such as deportation, detention, or prosecution. One of the FTTTF's roles is to provide technical assistance for projects such as the E-Guardian and Guardian applications.

FTTTF officials stated that the Guardian 2.0 development process did not initially follow the Life Cycle Management Directive (LCMD) guidelines because at the time of Guardian's development the LCMD process was under revision.[21] However, FTTTF officials provided us with documentation

[21] To ensure the FBI's IT processes and resources align with the OCIO's information system requirements, the OCIO developed the LCMD. The LCMD provides guidance and direction for the technical management and engineering practices used in the planning, acquisition, operation, maintenance, and replacement of IT systems and services. The LCMD provides direction to each Program and Project Manager charged with the responsibility to manage IT programs and projects through their entire life cycles, from inception through deactivation.

demonstrating they attempted to adhere to the revised LCMD development requirements after they developed the system. Additionally, FTTTF officials stated that they considered the LCMD process to be cumbersome at times and that the Office of the Chief Information Officer's (OCIO) officials were not always responsive to their needs. One FTTTF official commented that the Guardian 2.0 system would have taken more time to develop and the cost of the system would have been much higher had the full LCMD process been followed.

The FTTTF also provided enhancements to Guardian through a series of maintenance patches designed to update Guardian's software and ensure optimal system operation. An FTTTF official said the goal for implementing the patches was to provide quarterly updates to Guardian. However, an SSA who was involved with threat assessments said the quarterly patches were 6 months behind schedule. This SSA believed Guardian needed to be updated more frequently.

During our audit, the FBI replaced the contractor that developed and provided technical support to Guardian. FBI officials stated that the change in the contractor supporting Guardian reduced the number of technical professional staff with the expertise to provide enhancements and maintenance patches. Consequently, the Guardian update program fell behind schedule and further delays could inhibit the system's ability to track terrorist threats and suspicious incidents. Because Guardian is critical to the FBI's terrorist threat tracking and management process, we recommend that the FTTTF prioritize updates to the system and develop a schedule to ensure enhancements and maintenance patches are completed in a timely manner.[22]

Updates to the FBI's Threat Tracking System

The FBI is designing the E-Guardian application to provide state and local law enforcement with the capability to share its local terrorism incident information with the FBI and to receive nationwide unclassified terrorism incident information from the FBI's Guardian application. State and local law enforcement users will be able to enter, view, search, and create reports from threat data entered by both state and local law enforcement and the FBI. The initial assessment of the threat or suspicious incident begins when the threat or suspicious incident is entered into Guardian. E-Guardian users

---

[22] At our audit exit conference FBI officials told us the Guardian maintenance patch program is now on schedule and the system has not experienced significant down time resulting from maintenance patch issues.

will enter those activities, incidents, or citizen complaints that may have a nexus to terrorism.

As previously mentioned, during our audit the FBI replaced the contractor that designed and provided technical support to Guardian. Both FTTTF and OCIO officials said that because the E-Guardian creation relies on technology used to develop Guardian the project's delay was affected by the contractor change. As a result, deployment of the E-Guardian application under development during our audit has been significantly delayed. In addition, the FBI is developing and purchasing new software to complete E-Guardian because the FBI's original contractor did not completely document the software used to develop Guardian.

FTTTF and OCIO officials also stated that the lessons learned during the Guardian development process are being applied to the E-Guardian development process and that the FBI is following the OCIO's LCMD guidelines in creating E-Guardian. We verified that the OCIO and FTTTF are currently working together, developing or purchasing new software, applying the lessons learned during Guardian's development, and following the LCMD process. The FBI reported in September 2008 that E-Guardian was being tested on a pilot basis by certain agencies and that the FBI planned to complete rolling out E-Guardian in phases nationwide by the end of 2008.

E-Guardian Concept of Operations

The E-Guardian application is intended to allow terrorist threat reporting, threat data sharing, and threat information tracking for Fusion Centers and Joint Terrorism Task Forces as well as state, local, and tribal law enforcement agencies.[23] The unclassified E-Guardian application will include agencies that do not already have access to the classified Guardian application through the FBI's Fusion Centers and JTTFs. The application will allow the FBI and state and local law enforcement to collect, share, and analyze threat and suspicious activity data electronically. The E-Guardian application is expected to be an unclassified version of the current Guardian application and should include many of the features developed for the Guardian classified application.

The E-Guardian application is intended to enable users to enter, view, and search threat information as well as create useful reports from state and local law enforcement data and from FBI unclassified threat information exported from the classified Guardian application. Unclassified information from Guardian is expected to be routinely added to E-Guardian to enhance

[23] Fusion Centers are facilities created by state and local entities where homeland security, criminal-related information, and intelligence are shared.

information sharing. All E-Guardian users will be able to read the data, but only a limited number will be able to add data. The FBI expects its local law enforcement partners will submit incidents through both the Fusion Centers and JTTFs.

Talon – The Department of Defense Threat Reporting System

The U.S. Department of Defense (DOD) implemented the Talon threat reporting system to collect and evaluate information about possible threats to U.S. service members and defense civilians at both domestic and overseas military installations. According to the DOD, the system was closed on September 17, 2007, because the number of threats entered into the system had declined so significantly that it determined Talon possessed little analytical value.

The DOD is working to develop a new threat reporting system to replace Talon. According to the DOD, in the interim all information concerning the DOD's force protection threats will be entered into the FBI's Guardian application. In the future, the DOD will evaluate reporting systems to replace Talon, but the DOD has not established a timeline to acquire a replacement system. The DOD is considering Guardian as a permanent replacement for Talon, and the FBI is granting Talon users read-only access to Guardian.

The increased use of Guardian by the DOD also suggests that the potential exists for a dramatic increase in the number of terrorism-related incidents reported to the FBI.

Threat and Suspicious Incident Performance Reporting

Since the beginning of Guardian's implementation, the number of terrorist threats and suspicious incidents entered into the system has increased on an annual basis. Based on documentation provided by the FBI, between FYs 2005 and 2006, the number of incidents recorded in Guardian increased by 51 percent. Over the same period of time, the number of registered Guardian users increased 11 percent. In addition to the increases that have taken place with Guardian, it is anticipated that the implementation of E-Guardian will further increase the number of threats and incidents entered into Guardian. However, we found that the FBI has not taken adequate steps to plan for such increases.

As discussed earlier in this report, the FBI's policy is to investigate every credible threat it receives. During our fieldwork, we found that field offices collected terrorist threat and suspicious incident performance

measurement data and reported the data to field office senior management on a regular basis. However, we found that the CTD did not track or periodically report such information to FBI senior management on a regular basis. We also found no evidence to indicate that the FBI established performance measurements to address the number of hours expended during the threat resolution process or to report the effectiveness of its efforts to resolve terrorist threats and suspicious incidents. Performance measurements would help the FBI to consistently manage the Special Agent's and supervisor's counterterrorism workload and enhance the FBI's efforts to deploy these critical resources.

FBI officials told us that they were reluctant to establish targets for the number of threats resolved. The number of threats the FBI is expected to resolve varies from year to year, and FBI officials said it is difficult to assign a value for the number of threats to be resolved. In our view, though it may be difficult to project the number of incoming threats and incidents, by identifying the number of threats resolved based on the reporting capabilities available in Guardian, valuable trend information could be gathered to assist FBI management with assigning investigative and analytical resources to historically high threat areas. Moreover, performance goals and measurements, based on the time to resolve immediate, priority, and routine threats, could be developed without the requirement to project the number of threats in future years.

As previously discussed, we identified 60 routine threats and suspicious incidents (28 percent of those tested) at FBI field offices we visited that received no investigative activity for over 30 days. We believe that developing performance measures could also help the FBI ensure that extended periods of inactivity would be recognized more quickly by supervisors and management.

In addition, because the threat resolution process relies heavily on the investigative judgment of both the Special Agents and the supervisor, threat resolution-based performance measurements could also help the FBI identify instances where resource reallocations are warranted. Prior Office of the Inspector General audit reports have also identified the need for the FBI to allocate resources based on its assessment of both current and future threats.[24]

---

[24] U.S. Department of Justice Office of the Inspector General, *The Federal Bureau of Investigation's Efforts to Hire, Train, and Retain Intelligence Analysts*, Audit Report 05-20 (April 2005), 40-44; OIG, *The Federal Bureau of Investigation's Effort to Protect the Nation's Seaports*, Audit Report 06-26 (March 2006), 72; and OIG, *Follow-up Audit of the Federal Bureau of Investigation's Efforts to Hire, Train, and Retain Intelligence Analysts*, Audit Report 07-30 (April 2007), 16-17.

The latest version of Guardian, Guardian 2.0, includes significant improvements in terrorist threat and suspicious incident performance-related reporting. For example, Guardian can now produce the following reports:

(1) Incidents by Office – a summary of the status and number of incidents broken down by field office;

(2) Overdue Investigations – a summary of the overdue incident closures by field office;

(3) Current Activity – a summary of FBI system-wide incident activity by field office for the last 24 hours, 7-days, and 30-days by field office; and

(4) Incidents and Sessions by Month – a summary of the total number of incidents and Guardian sessions by month and the average incidents and sessions by day or month by field office.

We believe that the FBI can improve its threat and suspicious incident reporting and resource allocation by effectively utilizing Guardian's improved reporting capabilities and in developing performance measures to support the efforts of resolving every terrorist threat and suspicious incident.

Conclusions

We believe that the development and deployment of Guardian has enhanced the FBI's ability to address and track terrorist threats and suspicious incidents. Guardian provides the FBI with ability to: (1) route work, assign and accept tasks, and manage resources; (2) share investigative data to support intelligence analyses; (3) share investigative data with other government agency partners; and (4) allow agents to auto-populate Guardian threat information directly into ACS for additional investigation and threat resolution. We also found the FBI successfully deployed an improved version of Guardian and developed a comprehensive Guardian User's Manual. Moreover, although the deployment of E-Guardian has been delayed, E-Guardian should further enhance the FBI's efforts to share threat information.

However, during our audit we identified several areas of concern regarding the FBI's use of Guardian. Although the summaries of the incidents we reviewed in Guardian were complete and accurate, we found several incidents that were not properly reviewed by a supervisor. We

concluded the quality control provided by the supervisory review needs to be improved.

Many of the incidents we tested in Guardian were resolved in a timely manner. However, we found 60 of the 218 incidents (27 percent) we tested exceeded the FBI's guideline for timeliness. Based on our review of the Guardian incidents and our interviews with FBI officials we concluded that some Guardian incidents in the system were perceived to have a very low priority and were permitted to remain inactive in the threat management system for several months at a time. The prompt assessment of terrorist threats and suspicious incidents is essential. We believe both the field offices and the CTD should develop additional controls to ensure all Guardian incidents are acted upon in a timely manner.

The supplementary tabs introduced with Guardian 2.0 improve the user's ability to search for specific threats. Yet we found the guidance provided to the field offices concerning the completion of the supplementary tabs was not clear, and as a result supplementary tabs were not always completed. Incomplete or inconsistent completion of this supplementary information could cause agents to obtain an inaccurate threat assessment. The FBI should review its requirement to complete the supplementary tabs, issue clear guidance for completing the tabs, and ensure the field offices consistently follow the guidance.

Frequently, the FBI obtains additional threat information during an existing investigation or the imminent nature of the threat results in a case opening in the ACS system without an assessment in Guardian. We tested cases in the ACS system and found that agents did not always create a Guardian incident record based on information derived from active investigations. In our test cases we found threat information obtained during active investigations that should have been included in Guardian.

E-Guardian should improve the FBI's ability to share counterterrorism information with its state and local law enforcement partners. However, we found that the change in the contractor developing E-Guardian and early problems with the system's development have contributed to delays in implementing the system.

While Guardian has enhanced the FBI's ability to address and track terrorist threats and suspicious incidents, because of its policy to investigate every credible threat it receives the FBI must ensure that it uses its resources as effectively as possible. We found that performance measures were not in place to measure the FBI's effectiveness to resolve threats and incidents. Performance measures would help ensure that the FBI

consistently manages staffing workloads and that it deploys critical resources according to priority and need.

OIG Recommendations

We recommend that the FBI:

1. Ensure SSAs and Supervisory Intelligence Analysts review threat incidents entered into Guardian.

2. Ensure that terrorist threats and suspicious incidents entered in Guardian are closed or forwarded for investigation in a timely manner.

3. Determine the value added by the completion of Guardian's supplementary tabs, issue comprehensive guidance, and ensure the field offices follow the guidance for completing the supplementary tabs.

4. Ensure that all threat information obtained from ongoing counterterrorism investigations that meets Guardian entry requirements is entered in Guardian.

5. Develop and implement a schedule to ensure technical patches to the Guardian system are completed in a timely manner.

6. Develop performance measurements to support the FBI's efforts to resolve terrorist threats and suspicious incidents.

7. Incorporate threat and incident performance measurements into existing resource allocation plans.

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS

The audit was conducted in accordance with the generally accepted government auditing standards. As required by the standards, we reviewed management processes and records to obtain reasonable assurance that the FBI's compliance with laws and regulations that could have a material effect on FBI operations. Compliance with laws and regulations applicable to the FBI's efforts to address terrorist threats is the responsibility of the FBI's management.

Our audit included examining, on a test basis, the FBI's compliance with certain laws and regulations. The specific laws and regulations against which we conducted our tests are contained in:

- 18 U.S.C. § 2331;
- 28 U.S.C. § 0.85;
- The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations; and
- The Attorney General's Guidelines for FBI National Security Investigations.

Our audit did not identify any areas where the FBI was not in compliance with the laws and regulations referred to above. With respect to those transactions not tested, nothing came to our attention that caused us to believe that FBI management was not in compliance with the laws and regulations cited above.

STATEMENT ON INTERNAL CONTROLS

In planning and performing our audit, we considered the FBI's internal controls for determining our audit procedures. This evaluation was not made for the purpose of providing assurance on the internal control structure as a whole. However, we noted certain matters that we consider to be reportable conditions under generally accepted government auditing standards.

Reportable conditions involve matters coming to our attention relating to significant deficiencies in the design or operation of the internal control structure that, in our judgment, could adversely affect the FBI's ability to resolve terrorist threats. As discussed in the Findings and Recommendations sections of this report, we found that:

- controls need to be developed to ensure all required threats and suspicious incidents are: (1) included in Guardian, (2) addressed in a timely manner, and (3) properly entered into Guardian; and

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 in managing its terrorist threat resolution efforts. This restriction is not intended to limit the distribution of this report, which is a matter of public record.

APPENDIX I

OBJECTIVES, SCOPE, AND METHODOLOGY

Objective

The objectives of this audit were to evaluate the policies and procedures the FBI uses to identify, assess, and track terrorist threats and suspicious incidents, and to determine the extent the FBI field offices follow guidance from FBI headquarters.

Scope and Methodology

The audit was performed in accordance with generally accepted government auditing standards, and included tests and procedures necessary to accomplish the audit objective. We conducted work at FBI headquarters components in Washington, D.C., and the surrounding metropolitan area. We also conducted work at six FBI field offices: New York, New York; Philadelphia, Pennsylvania; Washington, D.C.; Detroit, Michigan; Kansas City, Missouri; and Los Angeles, California.

To perform our audit, we interviewed officials from the FBI's Counterterrorism Division components, including the Federal Terrorist Tracking Task Force, Counterterrorism Watch, Threat Monitoring Unit, Public Access Control Unit, Threat Review Unit, and the International and Domestic Terrorism Operations Sections. We also interviewed officials from the Weapons of Mass Destruction Directorate and Office of the Chief Information Officer. We reviewed documents detailing terrorist threat resolution, organizational structures, directives, policies, and procedures.

To verify and test the implementation of the directives, policies and procedures established by FBI headquarters, we performed site visits at the aforementioned six FBI field offices chosen to represent a cross-section in terms of size, geography and activity. At each office, we interviewed senior managers, line supervisors, Special Agents, and Intelligence Analysts responsible for terrorist threat resolution. We reviewed representative samples of threat incidents from the FBI's Guardian threat tracking system and terrorism-related cases from the FBI's Automated Case Support system to test the field organization's usage of these systems and compliance with FBI headquarters directives.

APPENDIX II

PRIOR REPORTS INVOLVING THE FBI'S TERRORIST THREAT RESOLUTION

Below is a listing of relevant reports discussing the FBI's efforts to resolve terrorist threats. These include reports issued by the Department of Justice Office of the Inspector General (OIG) and the Government Accountability Office (GAO).

Prior OIG Reports Involving FBI Terrorist Threat Resolution

In September 2002, the OIG issued a report entitled *A Review of the Federal Bureau of Investigation's Counterterrorism Program: Threat Assessment, Strategic Planning, and Resource Management,* which reviewed aspects of the FBI's management of its counterterrorism resources. This report found that the FBI had not performed a comprehensive assessment of the terrorist threat facing the United States and that the FBI had not adequately established strategic priorities or effectively allocated resources to its counterterrorism program. The report provided 14 recommendations, including the development of criteria for evaluating and prioritizing incoming threat information for analysis and the establishment of a protocol to guide the distribution of threat information. At the time of our audit, the FBI completed actions necessary to close 12 of the report's 14 recommendations.

In June 2005, the OIG issued a report entitled *A Review of the Terrorist Screening Center* (TSC). The TSC was created to consolidate government watch lists of suspected terrorists, and the FBI was designated as the lead agency responsible for administering the TSC. The report provided 40 recommendations to the TSC to strengthen its operations. The OIG identified weaknesses in the completeness and accuracy of data in the consolidated watch list, and recommended that the TSC develop procedures to regularly review and test the information contained in the terrorist screening database.

In addition, the OIG concluded that the management of the TSC call center and its staff needed improvement. The OIG recommended that the TSC establish protocols for the proper entry and review of data in the Encounter Management database and develop an automated method for flagging records in the database that require follow-up action. Likewise, the TSC needed to establish an automated method for entering call data and sharing this data with the FBI's Counterterrorism Watch (CT Watch) to eliminate redundancy and reduce the time it takes for CT Watch to receive

the data. Based on actions taken by the FBI, all of the reports 40 recommendations have been closed.

In March 2006, the OIG issued a report entitled *The Federal Bureau of Investigation's Efforts to Protect the Nation's Seaports*. The report found that the FBI had taken steps to enhance its capability to identify, prevent, and respond to terrorist attacks in the maritime domain, including establishing the Guardian Threat Tracking System to collect information on terrorist threats and suspicious incidents at seaports and elsewhere and to manage follow-up action on these threats and incidents.

However the OIG found that Guardian could not be easily searched to identify trends in maritime-related suspicious activities or threats, and the FBI had not ensured that FBI offices complied with directives concerning the use of Guardian and the need to document the resolution of all incidents entered in Guardian. As a result, the FBI could not identify for the OIG the number of maritime-related threats for the audit period. The report expressed the concern that not all FBI field offices were fully utilizing Guardian. In the judgment of the OIG, the underutilization of Guardian prevented the FBI's Threat Monitoring Unit from developing a complete understanding of threat trends, including threats associated with the maritime domain. At the time of our audit, the FBI had closed 16 of this report's 18 recommendations.

In February 2007, the OIG issued a report entitled *The Department of Justice's Internal Controls Over Terrorism Reporting*. The report found that the FBI, along with the Criminal Division, the Executive Office for United States Attorneys, and United States Attorney's Offices, had not accurately reported terrorism statistics. The FBI did not accurately report eight of the ten statistics reviewed for FY 2003 and 2004, including:

- the number of terrorism-related threats tracked,
- the number of terrorism threats to transportation and facilities, and
- the number of terrorism threats to people and cities.

The report found that the number of terrorism threats tracked in FYs 2003 and 2004 were inaccurate primarily because the reported statistics included threats that were counted multiple times. In addition, the number of threats tracked during this period did not include approximately 60 percent of threats tracked by FBI field offices, the FBI's Counterterrorism Watch Unit, and the FBI's International Terrorist Operations Sections. The report observed that use of the Guardian Threat Tracking System should

significantly improve the accuracy of the number of threats reported, and recommended that the FBI establish and document internal control procedures for gathering, verifying, and reporting terrorism related statistics and maintain documentation to support the threat reporting process.

In March 2007, the OIG issued a report entitled *A Review of the Federal Bureau of Investigation's Use of National Security Letters.* Among other findings, the OIG determined that the FBI had generated over 300 national security letters from an administrative control file rather than from an investigative case file in violation of FBI policy. In these instances, FBI agents did not generate and supervisors did not approve documentation demonstrating that the factual predicate had been established as required by the Electronic Communications Privacy Act, the Attorney General's Guidelines for FBI National Security Investigations, and internal FBI policy. When national security letters are issued from control files rather than investigative files, internal and external reviewers cannot determine whether the requests are tied to investigations that established the required evidentiary predicate for issuing the national security letters.

The OIG reported that the FBI's Counterterrorism Division, in consultation with the FBI Office of General Counsel, had taken steps in response to the OIG's identification of this issue to ensure that future national security letter requests are issued from investigative files rather than from control files so that these requests conform to national security letter statutes, the Attorney General's Guidelines for FBI National Security Investigations, and internal FBI policy.

Prior GAO Reports Involving FBI Terrorist Threat Resolution

In June 2002, GAO issued a report entitled *FBI Reorganization: Initial Steps Encouraging, but Broad Transformation Needed.* Among the issues identified for more in-depth review and scrutiny was the implementation of the newly revised Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations (Guidelines).

In June 2003, the GAO issued a follow-up report entitled *FBI Reorganization: Progress Made in Efforts to Transform, but Major Challenges Continue.* Among other topics, the report discussed implementation of the Guidelines. The report found that FBI internal controls were in place to ensure compliance with the Guidelines, including:

- policies and procedures,
- training,

- supervision,
- inspections, and
- allegations of abuse.

The report found no reported allegations or investigations of noncompliance with the new Guidelines, but cautioned that the revised Guidelines were in their infancy in terms of implementation, and concluded that while it was a good sign that the GAO had not identified any reported allegations, investigations, or indications of abuse of the new investigative authorities, this was not a situation that should result in reduced vigilance on the part of the Department of Justice or Congress.

APPENDIX III

FBI COUNTERTERRORISM CASES WITHOUT CORRESPONDING GUARDIAN INCIDENT NUMBERS

Active FBI Counterterrorism Cases Without Corresponding Guardian Incident Numbers by Sampled Field Offices October 23, 2006, to February 22, 2007

FBI Field Office	ACS CT Cases Without a Guardian Incident Number	ACS CT Cases Selected For Testing	ACS CT Cases With No Corresponding Guardian Entry
Philadelphia	76	30	21
New York	138	33	10
Washington, D.C.	129	30	25
Detroit	36	30	5
Kansas City	24	24	9
Los Angeles	143	30	11
Total	546	177	81

APPENDIX IV

ACRONYMS

ACS	Automated Case Support System
CT	Counterterrorism
CT Watch	Counterterrorism Watch Unit
CTD	Counterterrorism Division
DOD	Department of Defense
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
FTE	Full Time Employee
FTTTF	Foreign Terrorist Tracking Task Force
FY	Fiscal Year
GAO	Government Accountability Office
ITOS	International Terrorism Operations Section
JTTF	Joint Terrorism Task Force
LCMD	Life Cycle Management Directive
NSB	National Security Branch
NSI	National Security Investigation
NTCS	National Threat Center Section
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
PACU	Public Access Center Unit
PART	Program Assessment Rating Tool
SSA	Supervisory Special Agent
TMU	Threat Monitoring Unit
TRU	Threat Resolution Unit
TSC	Terrorist Screening Center
WMD	Weapons of Mass Destruction

APPENDIX V

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

October 14, 2008

The Honorable Glenn A. Fine
Inspector General
United States Department of Justice
Suite 4706
950 Pennsylvania Avenue, NW
Washington, DC 20530

RE: THE FEDERAL BUREAU OF INVESTIGATION'S TERRORIST THREAT AND SUSPICIOUS INCIDENT TRACKING SYSTEM

Dear Mr. Fine:

The Federal Bureau of Investigation (FBI) appreciates the opportunity to review and respond to your report entitled, "The Federal Bureau of Investigation's Terrorist Threat and Suspicious Incident Tracking System" (hereinafter, "Report").

The Report documents your examination of the polices and procedures used by the FBI to identify, assess, and track terrorist threats and suspicious incidents. In particular, the FBI's (1) Guardian Threat Tracking System; (2) Guardian threat assessment process and operational guidance established by FBI headquarters; and (3) Guardian threat assessment policies and procedures in practice at six FBI field offices were evaluated. Guardian is the automated system employed by the FBI which records, stores and assigns responsibility for follow up on counterterrorism threats and suspicious incidents. Guardian can also distribute immediate threat information to users, and analyze threat information for trends and patterns.

As noted in the Report, the FBI's Guardian application and related process represents a significant improvement from the past over how the FBI tracks and handles threat information as it provides users an automated workflow process to manage suspicious activity and threat information. Between July 2004 to November 2007, the FBI utilized Guardian to resolve over 100,000 potential terrorism-related threats, reports of suspicious incidents, and terrorist watchlist encounters. The overwhelming majority of these had no terrorism nexus yet the process provided sufficient predication to initiate over 600 terrorism and criminal investigations.

Based on a review of the Report, the FBI concurs with the seven recommendations for improvement made therein. To date, the FBI has implemented measures to resolve all of the identified issues. In the post-9/11 world in which we live, the FBI remains fully committed to future enhancements of Guardian to ensure continued success in our counterterrorism efforts.

In conclusion, the FBI appreciates the professionalism exhibited by your staff in working with our representatives throughout this audit process. Enclosed herein is the FBI's response to the report. With the instituted remedial changes already implemented throughout the FBI, I respectfully request the report be appended. In addition, in light of the new Attorney General Guidelines, we will maintain coordination with your office and report future progress on each of your recommendations. Please feel free to contact me should you have any questions.

Sincerely yours,

Michael J. Heimbach
Assistant Director
Counterterrorism Division
National Security Branch

Enclosure

1 - Mr. Thomas Puerzer
Regional Audit Manager
Philadelphia Regional Audit Office
Office of the Inspector General
U.S. Department of Justice
701 Market Street, Suite 201
Philadelphia, Pennsylvania 19106

Recommendation 1: Ensure SSAs and Supervisory Intelligence Analysts review threat incidents entered into Guardian.

FBI Response: FBI Concurs. The FBI's existing Guardian Policy (GP) Electronic Communication (EC) defined "Supervisor," within the Guardian context as follows:

1. Supervisory Special Agents (SSAs)
2. Acting Supervisory Special Agents (A/SSAs)
3. Supervisory Task Force Officers
4. Supervisory Intelligence Analysts (SIA)

The GP did not specifically refer to "Relief Supervisors," however, in many instances where there was a question of supervisory review of a Guardian incident; a "Relief Supervisor" did conduct an appropriate review of the incident report. Guardian Policy will be amended to specifically include "Relief Supervisors," and/or other individuals designated by FBI management to function in the Guardian "Supervisor" role. This will be designated by the ADIC/SAC or his or her designee, and will be documented via EC to the Guardian file. Additionally, the Threat Monitoring Unit (TMU) will draft updated Guardian Policy to clarify this issue, and to enumerate pending Guardian enhancements, as a result of the consolidated AGG for Domestic FBI Operations.

Recommendation 2: Ensure that terrorist threats and suspicious incidents entered in Guardian are closed or forwarded for investigation in a timely manner.

FBI Response: FBI Concurs. Existing GP regarding this matter continues to be reinforced by the National Threat Center Section (NTCS). The NTCS compiles weekly statistics for Guardian compliance and communicates directly with FBI Field Office and Legat management via e-mail and/or EC to address any compliance issues. This includes incidents which are not addressed in a timely manner, as well as, to direct specific investigative action to mitigate a threat. Additionally, the Guardian Training Program (GTP) has begun to stress and will continue to stress the importance of entry of threats and suspicious activity incidents into Guardian, as well as the mitigation window dictated by policy. Current policy dictates all Guardian incidents should be closed within thirty (30) days of incident creation. Recent contact with the field reinforced the Counterterrorism Division's (CTD) dedication to ensuring timely mitigation, incident closure and/or forwarding for investigation. The TMU sends an e-mail communication to all field offices on a monthly basis detailing field office performance in addressing Guardian leads and instructing them to address any incidents not closed within 30 days. The TMU offers additional on-site Guardian training for field offices which are rated below minimally successful in complying with GP during any fiscal year.

Any reports of terrorism related threats, terrorists' events, or suspicious activity first received by the NTCS are immediately entered into Guardian by Counterterrorism (CT) Watch. CT Watch tracks the incident through Guardian and makes sure it is updated in a timely fashion.

If the threat requires more sophisticated techniques beyond those allowed by the Attorney General Guidelines (AGG) for Threat Assessments (TA), the Guardian incident is closed and the threat is forwarded to the International Terrorism Operations Section (ITOS) within approximately 72 hours.

Additionally, the NTCS has two protocols for review of all Guardian threat incidents, one analytical and one operational. The Threat Review Unit (TRU) consists primarily of Intelligence Analysts (IA's), including two SIA's, and one Unit Chief SIA. This unit is responsible for the review of all Guardian incidents to determine trends or patterns with regard to threats in Guardian, and publishes a weekly Emerging Trend Report on the FBI Intranet. The CT Watch Unit has initiated a Threat Review Group (TRG) within CT Watch consisting of IA's, Staff Operations Specialists (SOS), and Personnel Service Contractors as well as SSAs. The TRG reviews all new Guardian threat incidents and ensures all possible investigative avenues are being actively pursued by the field or Legat. If the TRG determines additional investigative steps are necessary to completely mitigate any threat, the field or Legat will be contacted and directed to conduct the follow up measures.

Recommendation 3: Determine the value added by the completion of Guardian's supplementary tabs, issue comprehensive guidance, and ensure the field offices follow the guidance for completing the supplementary tabs.

FBI Response: FBI Concurs. The completion of Guardian's supplementary tabs strengthens individual searches and improves analysis capabilities. The TMU will conduct periodic random sampling of new incidents to determine field office usage of the supplementary tabs. It has been determined by FBI analysts, that the completion of the supplementary tabs yields better search results. The TMU will draft updated Guardian policy to reinforce this issue. The GTP stresses the importance of populating the supplementary tabs upon incident entry and update as well as the resultant search benefit derived from doing so. New users are informed that the: location, name, vehicle, target and weapon searches are fed directly from the incident supplementary tabs. New users are encouraged to creatively utilize several search tools available in Guardian to ensure they find complete results. Demonstrations of various search features during instruction reinforce this important point. The TMU has reinforced the need to populate the individual tabs for: confidential human sources, targets, subjects, alleged groups, weapons/methods and vehicles not only when the incident is first entered, but also as information is received throughout mitigation of the threat.

Recommendation 4: Ensure that all threat information obtained from ongoing counterterrorism investigations that meets Guardian entry requirements is entered in Guardian.

FBI Response: FBI Concurs. The GTP will continue to stress the importance that all new threat information meeting Guardian entry requirements, even those arising from an ongoing investigation or a terrorism event which has already occurred, is entered into Guardian in a timely manner. This is outlined in Guardian Policy, and reinforced with a scenario discussion exercise in the GTP. Additionally, the Automated Case Support (ACS) Unit is creating a new mandatory field in ACS to be utilized during the creation of all new 315 cases. This new field documents the origin of the 315 case, and will capture any case which originated as a Guardian

incident. The new field is searchable and will provide an accurate count of 315 investigations which originated as a Guardian incident.

Current Guardian Policy dictates that all field offices, Legal Attaches and other FBI entities are required to enter all terrorism related threats and suspicious activity incidents into Guardian. This is mandatory even when a preliminary investigation or full field investigation is immediately opened. In all such instances that involve the immediate opening of an official investigation upon receipt of a terrorist related threat and/or suspicious activity report, a Guardian record must be created to summarize the nature of the incident. The record can be immediately marked "complete," after referencing the case file number and checking the appropriate boxes from the disposition tab, "drop down" menus.

Recommendation 5: Develop and implement a schedule to ensure technical patches to the Guardian system are completed in a timely manner.

FBI Response: FBI Concurs. This recommendation has been implemented in coordination with scheduled technical patches to the Guardian system and performing emergency maintenance as needed.

The Guardian Technical Team (GTT) obtained clearance from the Technical Configuration Control Board (TCCB) to use an eight hour window during the first Saturday of each month to conduct any necessary maintenance to the Guardian program. Authority must be granted by the TCCB because the GP must be taken off line in order to perform this regularly scheduled maintenance. Any emergency maintenance is done on an as-needed basis with proper authority and special attention paid to minimal inconvenience to users. In January, 2008, TMU advised that a quarterly release schedule would take effect for calendar year 2008. As intended, three successful releases have been implemented this year to date.

Recommendation 6: Develop performance measurements to support the FBI's efforts to resolve terrorist threats and suspicious incidents.

FBI Response: FBI Concurs. This recommendation has been implemented beginning Fiscal Year 2007 by rating each Assistant Director in Charge(ADIC)/Special Agent-in-Charge (SAC) on their Performance Appraisal Reviews (PAR) and through the Inspection Division's (INSD) new Semi-Annual Program Reviews (SAPR) which contain sections which specifically addresses the field offices performance in the utilization of Guardian for documenting, tracking, and resolving potential terrorist threats.

Each field office is rated by CTD on an annual basis on their adherence to the threat mitigation period policy. The results of this rating are reflected in the ADIC/SAC's PAR. The following criteria are utilized to determine field office compliance with Guardian Policy:

- The percent pending is calculated by dividing the number of Guardian incidents open after thirty days by the total incidents entered in the fiscal year (multiplied by 100).
- Outstanding = 0-4%
- Excellent = 5-9%

- Achieved Results = 10%
- Minimally Successful = 11-15%
- Unsatisfactory = 16% or Greater

As part of the FBI INSD's re-engineered inspection process, the INSD developed new SAPRs for all FBI investigative programs. The SAPRs for both the International Terrorism (IT) and Domestic Terrorism (DT) Programs contain sections which specifically address the field offices performance in the utilization of Guardian for documenting, tracking, and resolving potential terrorist threats. The following criteria are utilized to determine IT/DT program compliance with Guardian:

- Were all threats and suspicious activities with a possible nexus to terrorism entered into the Guardian system?
  _____Yes _____No (Explain)

- Were 90% of Guardian leads addressed and resolved in less than 30 days?

System enhancements are currently being implemented that will allow for enhanced tracking of various Guardian measures and statistics such as, the timeliness and results of TAs. Additionally, the system enhancements will permit the tracking of specific investigative techniques utilized in the vetting and/or mitigation of a threat or suspicious incident report (referred to as "Assessments" in the new AGG). Guardian will also track the number of incidents which result in initiation of a Preliminary or Full Investigation. It is anticipated that the aforementioned enhancements will be implemented on or before December 1, 2008.

In response to the September 29, 2008 signing of the new AGG for Domestic FBI Operations and the instant report regarding the FBI's Terrorist Threat and Suspicious Incident Tracking System, the NTCS will issue updated policy and guidance to all field offices and personnel working CT matters. This guidance will incorporate recommendations made by the DOJ/OIG and changes to the FBI's Threat Mitigation Policy and Procedures which are directly affected by the new AGG. This policy and guidance will be issued prior to the effective date of the new AGGs on December 1, 2008.

As mentioned previously, the consolidated AGG were signed by the Attorney General on September 29, 2008 and will be fully implemented by December 1, 2008. Several changes to the Guardian Program, as well as enhancements to Guardian Policy will be necessary to comply with the new Guidelines. As a result of the below listed changes, the NTCS will have the ability to generate reports which track the timeliness and results of Assessments conducted in Guardian. These technology enhancements to the Guardian application are needed to effectively measure performance.

Change 1: Guardian must have the ability to identify which approved investigative methods have been used in each assessment, therefore Guardian users will be required to document which methods were used in each incident. This will likely be accomplished by choosing one of the ten methods from a drop-down menu box whenever a new note is written to

the incident. This will allow the user to clearly identify which method they are documenting with the note. Guidance and training will be made available when this change is completed.

Change 2: Guardian must have the ability for the "Supervisor" to identify the correct 0-ASSESS file for upload. Guardian incident reports (FD-71a's) will no longer upload to the 324 classification files, as the 324 classification will be eliminated. Users will likely choose from a drop-down menu list of Assessment sub-files (A through U) for upload. Guidance and training will be made available when this change is completed.

Change 3: Guardian must have the ability to designate an Assessment as a Sensitive Investigative Matter (SIM). The SIMs will require Chief Division Counsel (CDC) review and SAC approval in an Assessment, as soon as practical after the identification of the Assessment as a SIM. Guidance and training will be made available when this change is completed.

Change 4: Guardian must develop language to include in all Assessments that are closed without leading to a predicated investigation indicating that, at the time of closing of the Assessment, there was no basis for further investigation by the FBI. Guidance and training will be made available when this change is completed.

Recommendation 7: Incorporate threat and incident performance measurements into existing resource allocation plans.

FBI Response: FBI Concurs. As previously mentioned, the NTCS currently utilizes Guardian performance measures as an element of the ADIC/SAC PAR. FBI Field Offices are measured on their Guardian usage, to include ensuring Guardian incidents are entered, and are closed or forwarded for investigation in a timely manner. This metric is also included in the INSD SAPRs for both the IT and DT Programs. TMU provides direct input to INSD in the evaluation of field office participation in the Guardian Program. Along with other performance measures, these evaluations are utilized by CT Executive Management (EM) to evaluate the effectiveness of each field offices' IT and DT Programs to determine if their Funded Staffing Levels for CT are appropriate based on the threat faced by each office.

The Resource Planning Office (RPO) established the Corporate Resource Planning Board (CRPB) to apply executive oversight to the resource allocation process and ensure resource decisions are made in accordance with the FBI's strategic objectives. The CRPB is responsible for reviewing all corporate-level resource decisions, including the management and review of positions, hiring decisions, and corporate plans. More specifically, the CRPB seeks to align existing resources, financial and human capital, and assets with the FBI's five-year strategic plan. The CRPB is comprised of executives representing a cross-section of FBI operational and support divisions. The Guardian staff will work with the CRPB to incorporate Guardian threat and incident performance measurements into existing resource allocation plans.

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 for its review and comment. The FBI's response to our audit report is included as Appendix V of this report. The FBI concurred with all seven recommendations in this report. Our analysis of the FBI's response to the seven recommendations is provided below. Based on the FBI's response, the OIG considers the report resolved. The following is a summary of the actions necessary to close the recommendations.

Summary of Actions Necessary to Close the Recommendations

1. **Resolved.** The FBI agreed with this recommendation. In its response, the FBI said that it will amend the Guardian policy to specifically include relief supervisors and other individuals designated by FBI management to function in the Guardian Supervisor role. The FBI also stated that the Threat Monitoring Unit (TMU) will draft updated Guardian policy to clarify this issue and to enumerate pending Guardian enhancements resulting from the recently issued Attorney General Guidelines for Domestic FBI Operations. This recommendation can be closed when we receive documentation showing that the Guardian policy has been appropriately updated and implemented to ensure that the review of threat incidents entered into Guardian is performed by those individuals designated as supervisors.

2. **Resolved.** In response to this recommendation, the FBI agreed to ensure that terrorist threats and suspicious incidents entered in Guardian are closed or forwarded for investigation in a timely manner. The FBI stated that current policy dictates all Guardian incidents should be closed within 30 days of incident creation and that existing Guardian policy regarding this matter continues to be reinforced by the National Threat Center Section (NTCS). Additionally, the TMU sends an e-mail communication to all field offices on a monthly basis detailing field office performance in addressing Guardian leads and instructing them to address any incidents not closed within 30 days. During our audit testing, however, we found instances where threats were not closed within 30 days of their creation in Guardian. This recommendation can be closed when we receive documentation evidencing that the FBI is closing Guardian incidents or forwarding them for investigation within 30 days of their creation.

3. **Resolved.** In response to this recommendation, the FBI agreed that completion of Guardian's supplementary tabs strengthens individual searches, improves analysis capabilities, and yields better results for searches of Guardian information. The FBI said its TMU will conduct periodic random sampling of new incidents to determine field office usage of the supplemental tabs. Additionally, the TMU will draft updated Guardian policy to reinforce completion of the supplementary tabs. This recommendation can be closed when we receive documentation showing that the Guardian policy has been appropriately updated and that the guidance for completing the supplementary tabs is being followed.

4. **Resolved.** The FBI agreed with our recommendation. In its response, the FBI stated that all threat information obtained from ongoing counterterrorism investigations that meet Guardian entry requirements should be entered in Guardian in a timely manner. The FBI stated that current Guardian policy dictates that all field offices, Legal Attachés, and other FBI entities are required to enter all terrorism related threats and suspicious incidents into Guardian. During our audit testing, we found instances where the FBI did not always ensure that threat information obtained from ongoing counterterrorism investigations was included in Guardian. This recommendation can be closed when we receive evidence of specific actions implemented to ensure that all threat information obtained from ongoing counterterrorism investigations that meets Guardian entry requirements is entered in Guardian.

5. **Resolved.** In response to this recommendation, the FBI agreed to develop and implement a schedule to ensure technical maintenance patches to the Guardian system are completed in a timely manner. The FBI said this recommendation has been implemented in coordination with scheduled technical patches to the Guardian system and in performing emergency maintenance as needed. The FBI noted that the Guardian Technical Team received authorization from the Technical Configuration Control Board for a specific fixed monthly timeframe to conduct any necessary maintenance to the Guardian system. Additionally, for calendar year 2008 the TMU advised that a quarterly Guardian release schedule would be implemented and that three successful releases updating Guardian were implemented during 2008. This recommendation can be closed when we receive documentation showing that the FBI has developed and implemented a schedule to ensure technical patches to the Guardian system are completed in a timely manner.

6. **Resolved.** In response to this recommendation, the FBI agreed to develop performance measures to support its efforts to resolve terrorist threats and suspicious incidents. The FBI said that in FY 2007 it began using threat and suspicious incident performance measures in management performance appraisal reviews, as well as through the FBI Inspection's Division's new Semi-Annual Program Reviews, which contain sections specifically addressing field office performance in utilizing Guardian. The FBI noted that each field office is annually rated by the Counterterrorism Division (CTD) on its adherence to the FBI 30-day policy for closing a Guardian incident or referring the incident for investigation. Additionally, Guardian system enhancements are currently being implemented that will allow for better tracking of various Guardian measures and statistics, such as the FBI's timeliness and results of its threat assessments. Finally, the newly issued Attorney General Guidelines have necessitated changes to the Guardian program and Guardian policy. The Guardian program changes are intended to provide NTCS the ability to generate reports that will track the timeliness and results of assessments tracked in Guardian. This recommendation can be closed when we receive documentation showing that the FBI has developed performance measures to evaluate its efforts in addressing terrorist threats and suspicious incidents.

7. **Resolved.** The FBI agreed with this recommendation. In its response, the FBI stated that it would incorporate threat and incident performance measures into existing resource allocation plans. The FBI said its Resource Planning Office established the Corporate Resource Planning Board to apply executive oversight to the resource allocation process and to ensure resource decisions are made in accordance with the FBI's strategic objectives. Additionally, the FBI said Guardian staff will work with the Corporate Resource Planning Board to incorporate Guardian threat and suspicious incident performance measures into existing resource allocation plans. This recommendation can be closed when we receive documentation demonstrating that the FBI has incorporated threat and suspicious incident performance measurements into existing resource allocation plans.