The Federal Bureau of Investigation's Efforts to Improve the Sharing of Intelligence and Other Information

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

Audit Report 04-10
December 2003

THE FEDERAL BUREAU OF INVESTIGATION'S EFFORTS TO IMPROVE THE SHARING OF INTELLIGENCE AND OTHER INFORMATION*

EXECUTIVE SUMMARY

The Federal Bureau of Investigation (FBI) has established as its highest priority the prevention of terrorist attacks on the United States. The accomplishment of this critical national security mission requires the FBI to collect, analyze, and appropriately disseminate intelligence and other information needed to disrupt or defeat terrorist activities. However, in the past, Congressional inquiries concerning the September 11, 2001, terrorist attacks on the United States, reports of commissions examining terrorism before and since September 11, and Office of the Inspector General (OIG) reports have suggested various weaknesses in the FBI's ability to effectively carry out the vital intelligence component of its counterterrorism program.[1]

As a result, the OIG initiated this audit to review the FBI's progress in addressing deficiencies in the FBI's intelligence-sharing capabilities that the FBI, Congress, the OIG, and others identified subsequent to the September 11 terrorist attacks. Our audit focused specifically on the FBI's: 1) identification of impediments to the sharing of counterterrorism-related intelligence and other information; 2) improvement of its ability to share intelligence and other information both within the FBI and to the intelligence community and state and local law enforcement agencies; and 3) dissemination of useful threat and intelligence information to other intelligence and law enforcement agencies. The focus of this audit was to identify and evaluate corrective actions taken by the FBI to improve the

[1] The commissions and their reports include: 1) the Bremer Commission's (National Commission on Terrorism) June 2000 report entitled "Countering the Changing Threat of Terrorism"; 2) the Gilmore Commission's (Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction) second and fourth reports in December 2000 and December 2002, respectively; and 3) the Thornburgh Panel's (National Academy of Public Administration) June 2003 Congressional testimony on the FBI's reorganization. The OIG reports include: "Review of the Federal Bureau of Investigation's Counterterrorism Program: Threat Assessment, Strategic Planning, and Resource Management" (September 2002), and "An Investigation of the Federal Bureau of Investigation's Belated Production of Documents in the Oklahoma City Bombing Case" (March 2002).

***BECAUSE THIS REPORT CONTAINED INFORMATION CLASSIFIED AS "SECRET" OR "LAW ENFORCEMENT SENSITIVE" BY THE FEDERAL BUREAU OF INVESTIGATION, WE REDACTED (WHITED OUT) THAT INFORMATION FROM THE VERSION OF THE REPORT THAT IS BEING PUBLICLY RELEASED. WHERE SUCH INFORMATION WAS REDACTED IS NOTED IN THE REPORT.**

sharing of intelligence information. The audit does not directly assess the viewpoints of the broader intelligence community or state and local law enforcement agencies to avoid overlap with related work on governmentwide information sharing recently conducted by the U.S. General Accounting Office (GAO).

Introduction

The terrorist attacks of September 11, 2001, revealed severe deficiencies in the FBI's intelligence analysis and information-sharing capabilities and processes. During the OIG's September 2002 audit of the FBI's counterterrorism program, some FBI managers described the FBI's intelligence analysis capability as "broken." Others on terrorism-related commissions and in Congress have suggested that the FBI's intelligence capability was more than broken; it had been virtually nonexistent.

The FBI's historic expertise has been in crime-fighting and in building cases for prosecution of criminals. Refocusing the FBI to preventing terrorist acts and developing the sets of skills required to collect, analyze, and disseminate intelligence strategically as well as tactically has required a change in the FBI's culture that has not been easy or quick.

FBI Director Robert Mueller took office one week before the September 2001 terrorist attacks and was immediately confronted with the need to change the focus of the FBI, and address various management problems at the FBI. He established as the FBI's highest priority the prevention of terrorist attacks and set about restructuring the Counterterrorism Division (CTD) to improve analysis and to foster the internal sharing of information. The Director also addressed the FBI's lack of a full, professional intelligence capability by bringing on board through temporary assignments seasoned Central Intelligence Agency (CIA) managers and analysts to help address the FBI's deficiencies in intelligence analysis and dissemination. Recognizing that the FBI's information technology (IT) systems were severely antiquated, the Director also hired professional IT managers from outside the FBI to develop more modern computer systems.

Impediments

The FBI has faced a number of impediments in its efforts to transform itself into a law enforcement agency with a robust intelligence capability to help prevent future terrorist attacks. An inherent part of this reinvention is

the ability to securely share intelligence and other information. During the course of our audit work, we asked FBI CTD managers about the problems they have encountered in sharing intelligence and other information both within the FBI and also to and from the intelligence community and state and local law enforcement agencies. FBI counterterrorism managers universally cited the FBI's IT limitations – particularly the existing Automated Case File (ACS) system – as the predominant impediment to the effective dissemination of intelligence and other information. Not only is the ACS system outmoded and a poor tool for disseminating information, but because of security vulnerabilities ACS cannot be used to transmit Top Secret (TS) or Sensitive Compartmented Information (SCI). Since much intelligence is TS or SCI, ACS was restricted to Secret level information or below and could not communicate with other agencies' systems. The other major impediment cited was the FBI's problems with being able to pull information together from a variety of sources, analyze the information, and disseminate it. In other words, the FBI lacked the ability to "connect the dots" or create a mosaic of information. Along with the FBI's analytical weakness was the lack of a capability to prepare a strategic threat assessment or "big picture" intelligence estimate.

In addition to IT and analytical impediments, FBI counterterrorism managers outlined a number of day-to-day information-sharing problems. For example, incoming cables or other information from the intelligence community were not always disseminated, or not disseminated timely, to the individuals or units that needed to act on the information. Such misdirected information could occur if the addressee had transferred jobs or the specific and correct unit was not designated. Internal communications through Electronic Communications (EC) were a problem because ECs required layers of review and approval as they made their way through the organization. In addition, although state and local law enforcement have publicly complained that the FBI was not sharing information, some state and local officials would not apply for the security clearances required for access to the information. Further, if the FBI was not the originator of the information, the intelligence agency providing the information needed to approve dissemination beyond the FBI. Passing information beyond the originating office also required the "scrubbing" of more sensitive aspects, such as the sources and methods used to acquire the information, to avoid potential compromise.

FBI managers stated that to accompany the organizational changes and the focus on improving information-sharing processes, the FBI has not

yet established policies and procedures that delineate the appropriate processes to be used to share information and intelligence, either internally or externally. For example, when we requested a flow chart for the processing of intelligence or other information received by FBI headquarters, none was available, and the FBI instead prepared a narrative description to meet our request. Further, the FBI has no formal policy or directive on what information should be disseminated to state and local law enforcement and under what circumstances. Without formal policies on information sharing, FBI managers and staff lack criteria and guidance by which to ensure that appropriate information is disseminated to the appropriate parties either within or outside the FBI. However, the FBI recently created Concepts of Operations that serve as a framework for improving key aspects of its intelligence program, including information sharing, and intends to develop the policies and procedures required to implement the plan.

Improvements

We found that based on their own reviews – and undoubtedly as a result of Congressional investigations and hearings on the FBI's counterterrorism program – FBI managers were aware of the obstacles the FBI faces in improving its ability to process and disseminate intelligence and other information from multiple sources. Although most of the FBI's efforts to improve information and intelligence sharing are ongoing, we found that fundamental reform has begun. Specifically, the FBI has taken the following actions to improve its ability to communicate information within the FBI, analyze intelligence, and disseminate information outside the FBI.

- Established the wide area network portion of Trilogy in preparation for IT improvements such as the Virtual Case File to replace ACS later this calendar year.

- Worked on a pilot of a TS/SCI network that has wired the CTD for access to higher-level classified intelligence information.

- Continued its longstanding exchange of managers with the CIA, including FBI personnel assigned to the CIA's Counterterrorist Center and CIA personnel assigned to FBI CTD sections.

- Temporarily borrowed 25 analysts from the CIA to establish an interim corps of intelligence analysts and, under the direction of an experienced CIA manager, began hiring and training FBI

Intelligence Reports Officers and analysts within a defined career track.

- Revamped the FBI analyst corps to establish a professional career track and a training program for Intelligence Analysts, Reports Officers, and Operations Specialists.

- Named an Executive Assistant Director and a Deputy Assistant Director for a newly formed Office of Intelligence to oversee both terrorist-related and criminal intelligence matters, including management of the informant program.

- Developed nine Concepts of Operations to establish goals and key principles for improving the core elements of the FBI's intelligence program, including information sharing.

- Restructured the CTD from two main sections to nine sections under three Deputy Assistant Directors, including new emphasis on analysis, terrorist threats, terrorist financing, and dissemination of intelligence and other information.

- Provided intelligence reports and assessments to the intelligence community and certain other agencies.

- Widely circulated information and declassified intelligence to the state and local law enforcement community through a weekly Intelligence Bulletin.

- Provided threat information to state and local law enforcement through messages over the National Law Enforcement Telecommunications System.

- Entered data on terrorist suspects to the National Crime Information Center system for access by state and local law enforcement officers.

- Worked cooperatively with the CIA on the daily Threat Matrix and report to the President and produced a Presidential Report to provide information on current issues of concern to the White House, CIA, and Department of Homeland Security.

- Established less formal "Urgent Reports" for immediate notification of FBI managers concerning terrorist threats or other events deemed important for senior management attention.

- Established an interagency National Joint Terrorism Task Force at FBI headquarters to work more closely with other federal agencies.

- Worked on pilot projects to develop a shared investigative database with participating federal, state, and local law enforcement agencies at selected locations.

- Increased the number of Joint Terrorism Task Forces from 36 in 2001 to 84 in 2003, in order to work with and share intelligence and other information with state and local law enforcement and other federal agencies.

- Managed the Foreign Terrorist Tracking Task Force to improve the FBI's ability to identify terrorist suspects in the United States and to block the entry of terrorist suspects.

- Established an Office of Law Enforcement Coordination to act as a liaison to state and local law enforcement agencies.

In June 2003, the new Executive Assistant Director for Intelligence launched a 10-week initiative to develop Concepts of Operations for each of 9 core intelligence functions, including information sharing. The Concepts of Operations provide a framework for developing formal policy and procedures and give FBI managers guidance through broad principles for information sharing. Also, the FBI is in the process of developing an FBI-wide enterprise architecture. In conjunction with the enterprise architecture, the FBI should develop a process map to define the current state and end state for its information-sharing processes and an implementation plan to put its Concepts of Operations into action.

Dissemination

Other than by conversation or passing of documents by hand, the FBI has nine primary ways of disseminating intelligence and other information outside the FBI: 1) The Director's Briefing, including input to the daily Threat Matrix and the Presidential Report, 2) Intelligence Information Reports as information dictates, 3) Intelligence Assessments,

4) Secure Video Teleconferencing System, 5) Urgent Reports, 6) weekly Intelligence Bulletins, 7) Quarterly Terrorist Threat Assessments, 8) e-mail messages, and 9) Terrorist Watch List in the National Crime Information Center. Also, when the TS/SCI LAN is fully operational, the FBI will be able to electronically transmit information, not only internally but to the broader intelligence community. We analyzed the content of the nine methods of information sharing to determine the nature of the information and to evaluate its potential usefulness.

The information disseminated by the FBI was generally useful, although some items were classified and therefore available only to the intelligence community or to those with the requisite security clearances. Other items were either unclassified information or were modified to allow broader distribution on a "law enforcement sensitive" basis. In the latter category, in particular, the information in Intelligence Bulletins and Quarterly Terrorist Threat Assessments varied as to content and usefulness for the purposes of helping state and local law enforcement agencies deal with the high-risk threat of radical Islamic fundamentalist terrorism. For example, some of the information provided dealt with upcoming social protests or with environmental extremists. While local law enforcement agencies nationwide might be interested in the potential for criminal activities by such groups – which fall under the FBI's broad definition of terrorism – the focus of the information the FBI provides to state and local law enforcement is not always on international terrorism. Instead, much of the material disseminated falls within the FBI's definition of domestic terrorism. Our specific observations about the nine types of information-sharing products follows.

1. The Director's Briefing and Threat Matrix. The FBI Director's morning briefing included a number of items, most notably the daily Threat Matrix for which the FBI provides information to the CIA and which in turn is used to prepare the President's daily threat briefing.[2] The Director's Briefing also included a counterterrorism update, operational highlights, a summary of significant intelligence, and information on Foreign Intelligence Surveillance Act activities. The briefing and the matrix focused on international terrorism. Since the OIG's September 2002 audit on the FBI's

[2] The interagency Terrorist Threat Integration Center (TTIC), established on May 1, 2003, with CIA and FBI representation, has assumed responsibility for the Threat Matrix and the Presidential Terrorism Threat Report, to which the FBI contributes.

Counterterrorism Program, the information in the matrix showed more analysis of the credibility of threats, relationships to other threats, and capacity to carry out a threat. After completion of our audit work, the FBI replaced the Director's Briefing with a more broadly-focused Director's Daily Report covering various FBI activities. Although we did not review the new reports, FBI officials indicated that counterterrorism aspects continued to be included in the report.

2. Intelligence Information Reports provide the FBI, intelligence community agencies, the White House, the State Department, the military, and other selected federal agencies with the specific results of classified intelligence collected on internationally-based terrorist suspects and activities, chiefly abroad. By design, the reports are not analyses or necessarily validated intelligence, and are not broad assessments or estimates. Rather, the reports are relatively short (several pages) narrative results of potentially actionable intelligence disseminated to parties with a need to know. In some cases, the FBI asks recipients to provide additional information on the topic.

3. Intelligence Assessment products are also being developed and issued by the FBI. For example, we reviewed the classified national threat assessment "The Terrorist Threat to the U.S. Homeland: An FBI Assessment" and found that this intelligence estimate is a comprehensive view of terrorist capabilities and intent. The report, produced at the Secret/SCI level, was distributed within the intelligence community.

4. The Secure Video Teleconferencing System provides an opportunity for frequent contact among members of the intelligence and counterterrorism community to communicate face-to-face and discuss terrorist and related intelligence. While video teleconferencing is limited to cleared federal personnel, the ability to directly share information on a real-time basis is valuable.

5. Urgent Reports are intended to provide breaking information quickly to senior FBI managers from field offices without the inherent delay of the formal EC, although the Urgent Reports are expected to be formalized through a subsequent EC. We reviewed 42 urgent reports issued during about a two-week period. The reports are in

e-mail format and are one or two pages in length. Urgent Reports can be on any topic and are not limited to terrorism. Of the reports we reviewed, 26 percent pertained to actual or suspected terrorism matters; others reported on criminal issues or on incidents at airline checkpoints.

6. Intelligence Bulletins, issued weekly, are intended to share information with state and local law enforcement agencies on an unclassified, law-enforcement-sensitive basis. The Bulletins are not alerts that give specific guidance to law enforcement agencies on preventing a terrorist act, but rather appear to be an effort to educate and raise general awareness about terrorism issues. The Bulletins are usually a page or two of general information on a variety of topics. Some Bulletins have provided information that would be useful to law enforcement agencies' efforts to help detect and disrupt terrorist activities by radical Islamic fundamentalists. For example one Bulletin described terrorist surveillance techniques. Other Bulletins have covered upcoming social protests or protestors' tactics. Of the 15 Bulletins we reviewed, 6 dealt with international terrorism topics, 6 were unrelated to the threat of international terrorism, and 3 gave general information on terrorism or called for vigilance.

7. Quarterly Terrorist Threat Assessments are approximately two dozen pages that provide state and local law enforcement agencies a general overview of the terrorist threat, the civil disturbance threat, and events in various regions of the world. These unclassified, law-enforcement-sensitive assessments discuss in general the potential for terrorist activities and provide background on terrorist methods. The assessments do not delineate specific steps that should be taken to thwart terrorist acts or investigate terrorist suspects. We reviewed five reports, which provide similar information with minor updates to each subsequent report.

8. E-mail messages over the National Law Enforcement Telecommunications System allow the FBI to instantly provide threat warnings or other information to state and local law enforcement personnel. In practice, the messages have varied in their relevance to the threat of international terrorism and in their guidance to state and local law enforcement agencies.

9. The FBI posts names from its Terrorist Watch List on the National Criminal Information Center database, along with guidance on what state or local law enforcement should do, for example, if they encounter a named individual during a traffic stop. The sharing of the watch list information is critical to integrating state and local law enforcement into the war on terrorism and greatly enhances the nation's ability to identify and arrest or detain terrorist suspects.

Recommendations

To improve its ability to provide useful information within the FBI and to other federal, state, and local agencies, we make the following six recommendations to the FBI based on the results of this audit:

- Using the Concepts of Operations as a framework, establish a written policy on – and procedures for – information sharing, including what types of information should be shared with what parties under what circumstances.

- Ensure that the FBI-wide enterprise architecture currently under development is accompanied by a process map for information sharing that clearly defines the current state and an end for the information-sharing process so that the numerous information sharing initiatives can be coordinated and properly monitored and managed.

- Consider transferring responsibility for investigating crimes committed by environmental, animal rights, and other domestic radical groups or individuals from the Counterterrorism Division to the Criminal Investigative Division, except where a domestic group or individual uses or seeks to use explosives or weapons of mass destruction to cause mass casualties.

- For each Concept of Operations, develop an implementation plan that includes a budget along with a time schedule detailing each step and identifying the responsible FBI official.

- Issue guidance on Urgent Reports so that top FBI managers' attention focuses on the most important matters of national security and public safety.

- Focus the content of Intelligence Bulletins and Quarterly Terrorist Threat Assessments to provide – to the extent possible – actionable information on the high risk of international terrorism and any domestic terrorist activities aimed at creating mass casualties or destroying critical infrastructure, rather than information on social protests and domestic radicals' criminal activities.

TABLE OF CONTENTS

BACKGROUND

Authorities

The Federal Bureau of Investigation's (FBI) authorities in counterterrorism derive from legislation and from several National Security Directives and Presidential Decision Directives (PDD).[3] Title 28, United States Code, Section 533 authorizes the Attorney General to appoint officials "to detect and prosecute crimes against the United States." Under this authority, the Attorney General has assigned the FBI "lead agency responsibilities in investigating all crimes for which it has primary or concurrent jurisdiction and which involve terrorist activities or acts in preparation of terrorist activities within the statutory jurisdiction of the United States." National Security Directive 207, issued in 1986, assigned responsibility to the FBI for responding to terrorist attacks, stating: "The Lead Agency will normally be designated as follows: the Department of Justice for terrorist incidents that take place within the U.S. territory. Unless otherwise specified by the Attorney General, the FBI will be the Lead Agency within the Department of Justice for operational response to such incidents."

Following the bombing of the Murrah Federal Building in Oklahoma City in April 1995, the President issued Presidential Decision Directive (PDD) 39, which directs responsible federal agencies to take various measures aimed at: 1) reducing vulnerabilities to terrorism, 2) deterring and responding to terrorism, and 3) preventing and managing the consequences of terrorist uses of weapons of mass destruction (WMD). The FBI specifically is tasked with reducing the United States' vulnerability to terrorism through an expanded program of counterterrorism. PDD 39 also requires the FBI Director to ensure that the FBI's counterterrorism capabilities are well managed, funded, and exercised.

In May 1998, the President issued PDD 62, which clarified the roles and activities of many of the agencies involved in the war against terrorism. The directive addresses the prevention of terrorist acts, apprehension of terrorists, prosecution of terrorists, and consequence management after terrorist acts. The directive also includes

[3] A complete list of abbreviations appears in Appendix 2.

transportation security and the protection of critical computer-based systems.

Following the September 2001 terrorist attacks, Congress passed and the President signed into law the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Patriot Act). The Patriot Act lifted legal barriers to the sharing of foreign intelligence information between the federal intelligence community and the federal law enforcement community. Section 203 of the Patriot Act authorizes the sharing with the FBI of foreign intelligence, counterintelligence, and foreign intelligence information whether obtained through grand jury proceedings or through authorized surveillance methods. Section 905(a) of the Patriot Act authorizes the Attorney General to disclose to the Director of Central Intelligence, foreign intelligence acquired in the course of a criminal investigation. As mandated in the Patriot Act, the Attorney General established classified "Guidelines for Disclosure of Grand Jury and Electronic, Wire, and Oral Interception Information Identifying United States Persons" and "Guidelines Regarding Disclosure to the Director of Central Intelligence and Homeland Security Officials of Foreign Intelligence Acquired in the Course of a Criminal Investigation."

Further, the Attorney General's "Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations," issued May 30, 2002, govern the dissemination of intelligence in domestic terrorism situations. Specifically, the guidelines authorize the FBI to disseminate information acquired during the checking of leads, preliminary inquiries, and investigations conducted within the guidelines to another federal agency or to a state or local criminal justice agency when such information:

- falls within the investigative or protective jurisdiction or litigative responsibility of the agency;

- may assist in preventing a crime or the use of violence or any other conduct dangerous to human life;

- is required to be furnished to another Federal agency by Executive Order 10450;[4] or

- is required to be disseminated by statute, interagency agreement approved by the Attorney General, or Presidential Directive.

Intelligence Authorities

In addition to the FBI's law enforcement authorities for counterterrorism, the FBI also has authorities for intelligence activities. The three main authorities for intelligence are Executive Order 12333, the National Security Act of 1947, and a series of Director of Central Intelligence Directives (DCID).[5]

Executive Order 12333, issued in December 1981, authorizes the FBI within the United States to collect, produce, and disseminate foreign intelligence. However, the order states that intelligence community agencies such as the FBI are authorized to collect information on U.S. persons only in accordance with procedures established by the head of the agency concerned and approved by the Attorney General. The National Security Act of 1947 includes the FBI in its authorization of foreign intelligence activities by the intelligence community. Such activities include those designed to protect against international terrorist activities. This foreign intelligence authority supplements the FBI's investigative authority.

Under the DCIDs that implement national foreign intelligence requirements, the FBI disseminates foreign intelligence acquired in the course of investigations conducted in accordance with FBI priorities and guidelines. Thus, when the FBI recruits sources in its

[4] Executive Order 10450 establishes security requirements for government employees. Section 5 states: "Whenever there is developed or received information indicating that the retention in employment of any officer or employee of the Government may not be consistent with the interest of national security, such information shall be forwarded to the head of the employing department or agency…"

[5] DCIDs are the principal means by which the Director of Central Intelligence (DCI) provides guidance, policy, and direction to the intelligence community pursuant to authorities of the DCI as the head of the intelligence community. DCIDs are normally coordinated through the Intelligence Community Deputies Committee and intelligence community working groups.

investigations to protect the United States from terrorist attack, those sources may be queried on other foreign intelligence topics to meet national requirements. The DCIDs applicable to the FBI's management of foreign intelligence collection and production include:

- DCID 2/3 implements the National Intelligence Priorities Framework, which translates national foreign intelligence objectives and priorities approved by the President into specific prioritization guidance for the intelligence community;

- DCID 2/1 establishes the authorities and responsibilities of the Assistant DCI for Analysis and Production and the National Intelligence Analysis and Production to oversee, monitor, and evaluate national intelligence production;

- DCID 3/1 establishes the authorities and responsibilities of the Assistant DCI for Collection and the National Intelligence Collection Board to oversee, monitor, and evaluate intelligence collection;

- DCID 3/7 concerns the National Human Intelligence Requirements Tasking Center, which coordinates the National Human Intelligence Directives that guide FBI foreign intelligence collection;

- DCID 6/1 covers security policy for SCI;

- DCID 6/3 covers the protection of SCI within information systems,

- DCID 6/6 addresses security controls for the dissemination of intelligence information; and

- DCID 6/7 establishes policy for the disclosure or release of classified U.S. intelligence to foreign governments and international organizations.

Organization and Resources

During our audit, the FBI's Counterterrorism Division (CTD) was completing a major reorganization begun by the FBI Director in the

spring of 2002. In written testimony for the Senate Judiciary Committee in June 2002, the Director stated:

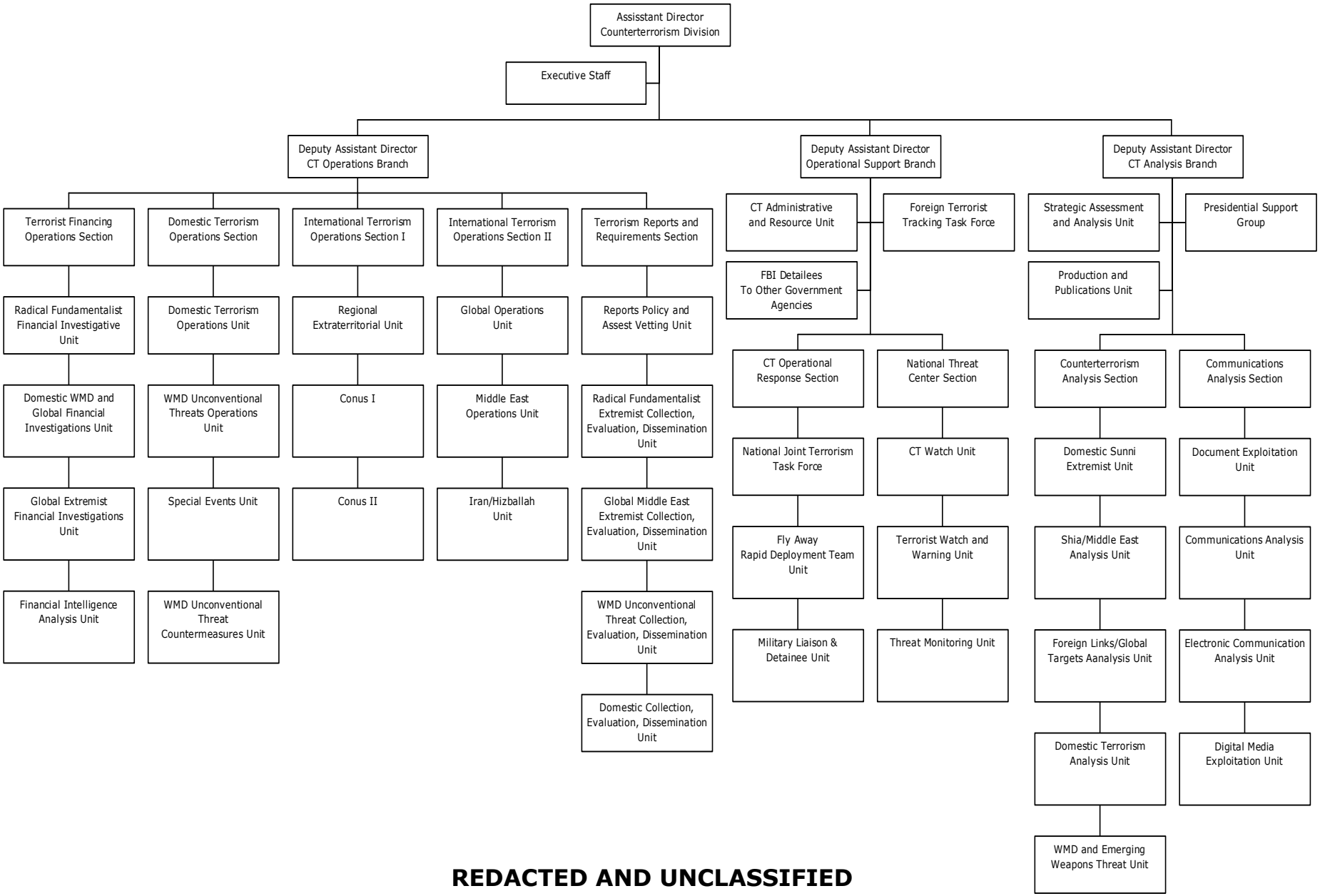
> A significant restructuring and expansion of the Counterterrorism Division at FBI headquarters is being proposed for three basic reasons. First, the more direct role envisioned for the Counterterrorism Division in managing investigations, providing operational support to field offices, and collaborating with law enforcement and the Intelligence Community partners requires additional staff at Headquarters. Second, implementing a more proactive approach to preventing terrorist acts and denying terrorist groups the ability to operate and raise funds requires a centralized and robust analytical capacity that does not exist in the present Counterterrorism Division. Third, processing and exploiting the information gathered domestically and from abroad during the course of the PENTTBOM [Pentagon-Trade Towers Bombing Investigation] and related investigation requires an enhanced analytical and data mining capacity that is not presently available.

The two main operating sections under the FBI's former structure were the International Terrorism Operations Section and the Domestic Terrorism Operations Section. An Assistant Director led the CTD, and a Deputy Assistant Director was directly responsible for the two sections. The National Domestic Preparedness Office, responsible for interagency coordination with state and local emergency responders, also reported to the Deputy Assistant Director. The two counterterrorism sections contained functional units. For example, within the International Terrorism Operations Section were the Usama bin Ladin Unit and the Radical Fundamentalist Unit.[6]

The reorganization expanded the CTD from two sections to nine. As shown in the following chart, the new CTD organization created three branches under Deputy Assistant Directors: Counterterrorism Operations, Operational Support, and Counterterrorism Analysis. The CTD organizational structure is discussed in greater detail in Finding 2 of this report.

[6] Although this name is often spelled "Osama bin Ladin," within the FBI the name is spelled as "Usama bin Ladin," so we will use that spelling in this report.

Counterterrorism Division Organizational Chart



The CTD expansion led the FBI to increase both the number of agents assigned to the division and the number assigned to the Joint Terrorism Task Forces (JTTF). During an April 10, 2003, appropriations hearing the Director testified that the FBI has shifted about 500 field agents from criminal investigations to counterterrorism investigations and activities.[7] According to the U.S. General Accounting Office (GAO), in fiscal year (FY) 2003 about 36 percent of the FBI's field agents worked on counterterrorism, counterintelligence, and cyber matters compared to 26 percent in FY 2002.[8] The CTD Assistant Director stated in February 2003 that the FBI had [CLASSIFIED INFORMATION REDACTED] agents assigned to counterterrorism matters, of which [CLASSIFIED INFORMATION REDACTED] are covering international terrorism and 500 are covering domestic terrorism. The Assistant Director also stated that of the total agents assigned to counterterrorism, [CLASSIFIED INFORMATION REDACTED] are assigned to JTTFs. As of March 14, 2003, the CTD had [CLASSIFIED INFORMATION REDACTED] support personnel onboard and another [CLASSIFIED INFORMATION REDACTED] pending background checks. The CTD has undertaken a major hiring effort to fill new positions required to support the war on terrorism. The expansion of the division and the increased staffing levels are directly related to a steady increase in the Division's budget. The CTD budget allocation increased from [CLASSIFIED INFORMATION REDACTED] in 2002 to [CLASSIFIED INFORMATION REDACTED] in 2003. In its 2004 budget submission, the FBI has requested [CLASSIFIED INFORMATION REDACTED] for the CTD.

Prior Reviews

In September 2002, the Office of the Inspector General (OIG) issued an audit report entitled, "A Review of the Federal Bureau of Investigation's Counterterrorism Program: Threat Assessment, Strategic Planning, and Resource Management" (Report 02-38). This audit focused on: 1) the FBI's progress toward developing a national-level risk assessment of the terrorist threat to the United States; 2) whether the FBI's strategic planning process provides a sound basis to identify counterterrorism requirements; and 3) the amount of resources dedicated to the FBI's counterterrorism program from

[7] Hearing of the Commerce, Justice, State, and Judiciary Subcommittee of the Senate Appropriations Committee on the Fiscal Year 2004 Appropriations for the FBI (April 10, 2003).

[8] The report is entitled: "FBI Reorganization: Progress Made in Efforts to Transform, but Major Challenges Continue" (GAO-03-759T, June 18, 2003).

1995 to April 2002. In addition, the audit assessed the FBI's management of its training and after-action reporting as they relate to counterterrorism operations.

The OIG's audit found that the FBI had not developed a comprehensive written assessment of the risk of terrorist threat facing the United States and that its strategic plan had not been updated. The OIG also found that the level of resources that the FBI dedicated to counterterrorism and counterintelligence increased dramatically between 1995 and 2002. The OIG made 14 recommendations to the FBI.

The GAO has performed audits and has testified frequently about the federal government's efforts to combat terrorism, including the FBI's role. In June 2003, the Comptroller General testified before the Subcommittee on Commerce, Justice, State, and the Judiciary, Committee on Appropriations, House of Representatives on the FBI's reorganization efforts.[9] In April 2003, the GAO reported that to protect the nation's borders, federal agencies maintain 12 different watch lists.[10] One of the watch lists cited was the FBI's Violent Gang and Terrorist Organization File. The GAO recommended that the Department of Homeland Security (DHS) lead an effort to consolidate and standardize the disparate watch lists. The GAO also has reported and testified on the need for better interagency coordination. For example, in September 2001 the GAO reported on overlapping functions among several agencies with counterterrorism responsibilities,[11] and in October 2002 the Comptroller General stated the following in testimony before the Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence.[12]

[9] The testimony is entitled "FBI Reorganization: Progress Made in Efforts to Transform, but Major Challenges Continue" (GAO-03-759T) and updates June 2002 testimony entitled "FBI Reorganization: Initial Steps Encouraging but Broad Transformation Needed" (GAO-02-865T).

[10] The report is entitled "Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing" (GAO-03-322, April 15, 2003).

[11] The report is entitled "Combating Terrorism: Selected Challenges and Related Recommendations" (GAO-01-822, September 20, 2001).

[12] The testimony is entitled "Homeland Security: Information-Sharing Activities Face Continued Management Challenges" (GAO-02-1122T, October 1, 2002).

> The success of a homeland security strategy relies on the ability of all levels of government and the private sector to communicate and cooperate effectively with one another. Activities that are hampered by organizational fragmentation, technological impediments, or ineffective collaboration blunt the nation's collective efforts to prevent or minimize terrorist acts.

As we note in the following sections of this report, the FBI has been taking steps to improve its counterterrorism and intelligence capabilities, including the sharing of information both within and outside the FBI.[13]

[13] Our objectives, scope, and methodology appear in Appendix 1. The details of our work are contained in the Findings and Recommendations sections of the report.

FINDINGS AND RECOMMENDATIONS

FINDING 1: Impediments to Sharing Intelligence and Information

The FBI has realized that to effectively carry out its post-September 11 mission to prevent future terrorist acts, it must improve its ability to share intelligence and related information both internally and with the intelligence community, other federal agencies, and state and local law enforcement agencies. The FBI has acknowledged that it faces a number of impediments to improving its intelligence and information sharing. We have grouped these impediments into four categories: 1) information technology (IT), 2) security clearances, 3) intelligence capability, and 4) policies and procedures.

With respect to IT, the FBI has lacked secure and modern systems to electronically transfer information both within the FBI and to outside organizations. Second, security considerations have prevented the full dissemination of intelligence, especially outside the federal community, because recipients must have security clearances and a need to know the information. Also, in keeping with standard intelligence community policy, before disseminating intelligence outside the intelligence community the FBI must obtain the permission of the "owner" if the FBI is not the originator of the information.

The third obstacle affecting the FBI's ability to disseminate intelligence and other sensitive information has been the FBI's organization and culture as a reactive law enforcement agency. The Director is attempting to transform the FBI into an agency that can gather, analyze, and disseminate intelligence to prevent terrorist acts rather than only investigating such acts after the fact. Lastly, the FBI lacks written policies and procedures for guiding and ensuring that information is shared appropriately and an overall strategy and blueprint for managing and controlling the numerous initiatives for improving information sharing at various organizational

levels. However, the FBI recently created Concepts of Operations that serve as a framework for improving key aspects of its intelligence program, including information sharing, and intends to develop the policies and procedures required to implement the plan.

Information Technology Systems

In December 2002, we reported that the FBI has not effectively managed its IT because it has not fully implemented the management processes associated with successful IT investments.[14] The foundation for sound IT investment management (ITIM) includes the following fundamental elements:

- defining and developing IT investment boards;
- following a disciplined process of tracking and overseeing each project's cost and schedule milestones over time;
- identifying existing IT systems and projects;
- identifying the business needs for each IT project; and
- using defined processes to select new IT project proposals.

We reported that the FBI failed to implement these critical processes. We found that the FBI did not have fully functioning IT investment boards that were engaged in all phases of IT investment management. The FBI was not following a disciplined process of tracking and overseeing each project's cost and schedule milestones. The FBI also failed to document a complete inventory of existing IT systems and projects, and did not consistently identify the business needs for each IT project. The FBI did not have a fully established process for selecting new IT project proposals that considered both existing IT projects and new projects.

We found that because the FBI has not fully implemented the critical processes associated with effective IT investment management, the FBI

[14] The OIG audit report is entitled "Federal Bureau of Investigation's Management of Information Technology Investments" (Report 03-09).

continued to spend hundreds of millions of dollars on IT projects without adequate assurance that these projects will meet their intended goals. We concluded that these shortcomings primarily resulted from the FBI not devoting sufficient management attention in the past to IT investment management.

Nearly every Section Chief and other FBI managers we interviewed for this audit stressed that the foundation for information sharing, both internally and externally, is reliable, modern, and user friendly IT systems. These same FBI managers said that the FBI's obsolete IT systems were the greatest impediment to the FBI's ability to efficiently and effectively disseminate information within the FBI and to other agencies. One manager detailed from the Central Intelligence Agency (CIA) to the FBI summarized the place of technology in information dissemination by saying: "Technology is the key to everything." The FBI managers pointed out that the FBI's ability to fully and effectively share information depends on its success in implementing the IT initiatives currently underway. Specifically, they said the success of the Virtual Case File (VCF) and the Secure Counterterrorism Operational Prototype Environment (SCOPE) components of the FBI's Trilogy system, currently under development, are crucial to improving the FBI's ability to share intelligence and other key information. The managers also emphasized the critical need for a secure Top Secret and Sensitive Compartmented Information Local Area Network (TS/SCI LAN) to allow for the electronic dissemination of the most sensitive and vital intelligence. These systems are discussed in further detail in Finding 2 of this report.

The September 11 Joint Inquiry[15] found that the FBI's IT weaknesses contributed to the FBI's inability to properly respond to the Phoenix memorandum.[16]

Inadequate information sharing within the FBI, particularly between the operational and analytical units, is also highlighted by our review

[15] The Joint Inquiry into the September 11 attacks, conducted by the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence, examined the intelligence community's activities before and after the September 11, 2001, terrorist attacks on the United States.

[16] The Phoenix memorandum, or Electronic Communication, was written by an agent in the FBI's Phoenix field office to the FBI's Counterterrorism Division on July 10, 2001. The memorandum outlined the agent's concerns about a coordinated effort underway by Usama bin Ladin to send students to the U.S. for civil aviation training.

> of the Phoenix Electronic Communication (EC). Several of the addressees on the EC, especially at the supervisory level, did not receive it prior to September 11 due to limitations in the electronic dissemination system.

FBI officials we interviewed echoed this observation.

One Section Chief we interviewed described the vital role of IT in disseminating intelligence, saying that until the FBI's IT weaknesses are corrected, the FBI will have an information-sharing problem. According to this official, for the past 20 years the FBI's IT systems have been patched instead of replaced; information the FBI does share is disseminated despite the FBI's IT systems, not because of them. According to this official, the major IT problems the FBI faces include: 1) the FBI's antiquated investigative case management system known as Automated Case Support, or ACS, is approved for the storage and transmission of information only up to the secret level; 2) the FBI is connected to the Department of Defense (DOD) systems on a fiber optic cable, but the connection to the CIA is not fiber optic; and 3) the FBI's ACS system is so obsolete that no other agency wants to use it. As a case management system, ACS was not designed for communicating with other agencies. Under ACS, all documents, including ECs, require handwritten signatures; therefore, all documents are physically passed from person to person as they move through the review chain. The FBI's fundamental information-sharing problem is the inability to move classified information, especially TS and/or SCI, securely outside of the FBI. Due to the FBI's IT limitations, even e-mails cannot be forwarded securely to the CIA. Instead, FBI personnel must print a paper version of the e-mail and provide this to their CIA counterparts.

Because the FBI does not have a system that can communicate securely with other agencies, it is forced to rely on teletypes to receive and disseminate intelligence. However, teletypes are a difficult method of communicating classified information because the information cannot easily be transferred to teletype from another type of electronic media and because teletypes are not user friendly. Further, according to several FBI managers we interviewed, incoming cables or other information from the intelligence community were often not disseminated or disseminated timely to those who needed the information for analytical or operational purposes. Information often was misdirected if the addressee had changed positions or the specific unit was not designated.

In contrast, the CIA has developed much more efficient IT systems to share intelligence information. For example, detailees from the FBI to the CIA share paper copies of FBI Form 302 investigation records with their CIA counterparts. If the CIA officials think the information is valuable, a Form 302 can be uploaded into the CIA system, making it searchable.

The efforts of the FBI to correct its IT deficiencies are discussed in Finding 2 of this report.

Security Clearances

When the FBI disseminates intelligence and other classified information, it must ensure that only the appropriate people receive the information. Specifically, the recipients of classified information must have a need to know the information and have been granted the proper level of security clearance. Further, if the FBI is not the originator of the information, the FBI must have received permission to disseminate the information. Permission from the originator may require revision of the information to render the information unclassified or modified to protect intelligence sources and methods.

Obtaining security clearances for state and local law enforcement personnel is in itself an obstacle to disseminating information. The FBI has been working to provide clearances to state and local law enforcement officers who need the clearances. To that end, since the September 11 terrorist attacks, the FBI has issued over 800 security clearances to state and local law enforcement personnel.

The process for obtaining a security clearance is cumbersome and time consuming and a process over which the FBI has little control. The application forms are the same ones that federal employees use, including FBI agents, when applying for a security clearance. The forms are lengthy and detailed. For example, applicants are required to list their residences for the last seven years along with details on education, employment, foreign travel, and other data. After the forms are completed, background investigations are conducted on each applicant. These background investigations are mandated by Presidential Executive Order. Compounding the expense and time required to grant a security clearance to a state or local law enforcement official is the perception, according to the Police Executive Research Forum, by some state and local officials that they should not have to undergo the same background investigation process as other

people who receive security clearances.[17] FBI officials told us that some state and local law enforcement executives think that their position alone demonstrates their trustworthiness.

Because not all state and local law enforcement officials who need security clearances have the clearances, the FBI is often constrained from providing detailed classified information to state and local law enforcement officials. As described subsequently in this report, the FBI is disseminating information to state and local officials on an unclassified but "law enforcement sensitive" basis except for members of JTTFs, all of whom hold security clearances. FBI officials told us, however, in the event of a high priority case where there is a threat to life, the FBI would provide the pertinent information to those with a need to know by granting interim clearances to those individuals.

Security classifications may also inhibit the FBI from disseminating information. According to one FBI Section Chief, the FBI does not originate 90 percent of the intelligence it uses. The agency that originally collected the intelligence may mark it ORCON, or originator controlled. All agencies that receive this information must receive permission from the originating agency before further dissemination. Agencies usually mark a document ORCON for two reasons. First, it allows the originating agency to protect the sources and methods disclosed in the classified document. Second, it is a vehicle to allow the originating agency to control how the information or conclusions in a document are used. FBI officials with whom we spoke said they thought that some of the criticism of the FBI for not sharing raw intelligence is misplaced because the information is often controlled by another agency. The FBI works with the CIA and other intelligence agencies to have information approved for dissemination by deleting sources and methods so the FBI can disseminate intelligence more quickly. The use of "tear lines" aids in achieving this goal. Documents containing tear lines are broken into sections. Some sections contain summary information and others contain detailed information such as sources and methods. The sections containing summary information can be disseminated to those with

[17] The Police Executive Research Forum is a national organization of police executives from the largest city, county, and state law enforcement agencies. The Forum is dedicated to improving policing and advancing professionalism through research and involvement in public policy debate. FBI Director Mueller addressed the Forum's annual meeting in May 2002.

proper clearances. The sections containing sources and methods cannot be disseminated.

Although the FBI faces a number of security-related constraints as to what information it can lawfully share with state and local law enforcement agencies, it is under increasing pressure to release as much information as possible. For example, the House Permanent Select Committee on Intelligence in its recent report on the 2004 intelligence authorization states that:

> Committee members remain concerned that information sharing between the FBI and state and local law enforcement colleagues still needs improvements. The Committee strongly urges the FBI to place high priority on making additional progress on this issue.

FBI officials told us that state and local law enforcement agencies often perceive that the FBI has more information than it is willing to share. This condition leads state and local law enforcement officials to sometimes have unrealistic expectations about what information the FBI can provide. For example, when the DHS increases the threat level, FBI officials are often asked for information about the specific threat. As is reasonable, officials from state and local law enforcement agencies often want to know whether anything in their jurisdiction is being specifically targeted. FBI officials usually do not have any information about specific targets. However, FBI officials with whom we spoke said that state and local law enforcement officials often believe the FBI is withholding information when told that the FBI does not have any specific threat information. FBI officials speculated that some state and local law enforcement officials may have this misconception about the detail available concerning threat information because the officials have not been involved in the collection and dissemination of intelligence. A Police Executive Research Forum white paper quotes a law enforcement executive as saying that local law enforcement "…often presumes that federal agencies are withholding detailed, relevant, and important information. We need to work on issues of mutual trust so that we can share what information there is, while retaining necessary security and integrity."[18]

[18] The white paper, issued in March 2003, is entitled "Protecting Your Community From Terrorism: Strategies for Local Law Enforcement."

FBI managers told us they are pushing their subordinates to share as much information as possible. Some managers expressed concern that the pendulum has swung too far in the FBI's efforts at openness and the key concepts for sharing classified information are sometimes ignored by the recipients. One FBI Section Chief told us that he believes the FBI sometimes shares more information than it should and that originator control of classified information and "need to know" are important requirements that other agencies need to honor. He argued that originator control of intelligence is a valuable tool that allows limited dissemination and control at the same time. Further, he said, every intelligence organization has to be able to control its information because the free flow of information can expose investigations and put agents' lives in jeopardy. He believes that some recipients currently may be disseminating ORCON information without permission and that some parties who receive intelligence or other sensitive information unilaterally decide to disseminate information that should go no farther than the immediate recipient.

FBI officials told us, however, that some leaks of sensitive information are the price to be paid for greater information sharing outside of the intelligence community. One official used a law enforcement sensitive FBI bulletin (discussed in Finding 3) as an example of leaks occurring when the FBI shares information. He noted that the information the FBI disseminates to the state and local law enforcement community frequently is seen or heard in the news media nearly immediately upon distribution.

Intelligence Capability

The FBI Director recognized as a result of the September 11 attacks that the FBI needed to develop a greater domestic intelligence capability to meet its new priority of preventing future terrorism. The FBI has a longstanding reputation as an investigative and law enforcement agency, and the Director's attempt to transform the FBI into a law enforcement agency with an intelligence capability to thwart terrorism represents a significant cultural change. As discussed in Finding 2, many steps toward this transformation have begun, including the establishment of an Executive Assistant Director for Intelligence, an Analysis Branch, a Terrorism Reports and Requirements Section, and a College of Analytical Studies. We heard repeatedly from FBI managers that the FBI needs to produce more intelligence products.

In our September 2002 report on the management of the FBI's counterterrorism program, we described the need for the FBI to add professional intelligence staff to help the FBI meet a clear need for improving its ability to collect, analyze, and disseminate threat information. At that time, some FBI managers described the FBI's analytical capability as "broken." Others on terrorism-related commissions and in Congress have suggested that the FBI's intelligence capability was virtually nonexistent. Specifically, the FBI had difficulty pulling information together from a variety of sources, analyzing the information, and disseminating it. In other words, the FBI lacked the ability to "connect the dots" or create a mosaic of information. Moreover, the FBI lacked the capability to prepare a strategic or "big picture" intelligence estimate or threat assessment. Our September 2002 report concluded that the FBI lacked a professional corps of intelligence analysts with a defined career path, standards for training or experience, or a system for effectively deploying and utilizing analysts to assess priority threats at either the tactical (investigative or operational) level or the strategic (long-term or predictive) level.

Until June 2002 when the CIA detailed managers and analysts to the FBI to help establish a professional intelligence function, the FBI did not have Reports Officers similar to the CIA's Collection Management Officer. Reports Officers glean intelligence, summarize the information, and disseminate the information to those with operational responsibilities. According to the Section Chief of the FBI's Terrorism Reports and Requirements Section, who is a CIA manager on detail to the FBI, the greatest challenge to building the FBI's intelligence reporting capability is the hiring and training of qualified Reports Officers. The Section Chief emphasized that it is better to do the staffing right rather than quickly, and she estimated that it would take about a year to fully staff the section. At the time of our audit, in February 2003, the section had 12 Reports Officers out of an authorized staffing level of 96 FBI-wide, including field offices. Of the 12 Reports Officers on board, 5 were recent college graduates, a few were from the FBI's Surveillance Operations Group, a few were GS-14 FBI Intelligence Operations Specialists, and 1 was a former military intelligence officer. In addition to those Reports Officers already on board, an additional 20 were undergoing background checks. According to the Section Chief, the work of Reports Officers is the type of work that people with the right fundamental skills or experience can learn. As a result, the Section Chief has focused on recent college graduates, people with government experience, and people with experience in terrorism issues.

Once hired, the new Reports Officers will need to be trained. Because the Reports Officer position is new to the FBI, the FBI needs to create a training program. At the time of our audit, the FBI Academy at Quantico did not offer appropriate training, so a new training curriculum had to be developed. The Terrorism Reports and Requirements Section Chief recognized the need for such a program and developed the framework for a Reports Officers' training program. The plan was to contract out for the training. The Section Chief envisioned four 2-week regional classes, followed by a 30- to 60-day detail to FBI headquarters to gain a hands-on perspective. Advanced training will be needed once the section is operational for three to five years. In contrast, [CLASSIFIED INFORMATION REDACTED].

The hiring of analysts has been slowed by issues concerning security clearances and pay. Intelligence agencies throughout the government are competing for the same pool of qualified applicants.

The Section Chief of one of the International Terrorism Sections stated that the FBI's newly created analytical capability is already aiding FBI operations. FBI officials said that in the 1990s, the FBI did not know how to do counterterrorism analysis but the current analysts program is moving forward. The analysts work for the Chief of the Counterterrorism Analysis Section, and he sets the analysts' priorities. The FBI does not yet have a formalized system for requesting analytical products but it was working on one. While the FBI is modeling the organization and function of its analytical component on the CIA, the FBI cannot completely mirror the CIA's analytical operations because the CIA's IT system "pushes," or automatically sends, information to those with a need to know. The FBI's systems require Reports Officers and analysts to "pull," or search for, information they need to complete an analysis or report.

Policies and Procedures

When we began our audit, the FBI did not have policies or procedures to guide FBI managers and personnel in what information should be shared or disseminated, with whom the information should be shared or disseminated, and in what manner. In June 2003, the new Executive Assistant Director for Intelligence launched a 10-week initiative to develop Concepts of Operations for each of 9 core intelligence functions, including information sharing. These plans, described in more detail in Finding 2, provide a vision for reinventing the FBI's intelligence program and correcting

existing weaknesses. The Concepts of Operations also provide a framework for developing formal policy and procedures and give FBI managers guidance through broad principles for information sharing. The FBI is in the process of developing an FBI-wide enterprise architecture. In conjunction with the enterprise architecture, the FBI should develop a process map to define the current state and end state for its information-sharing processes and an implementation plan to put its Concepts of Operations into action. We believe that such a structure is necessary to ensure that the FBI's dissemination efforts are consistent, meet the Director's expectations, and hold personnel accountable. Several managers told us that they had been busy trying to improve the FBI's intelligence capabilities and information sharing, and that policies and procedures would have to come later.

During the period of our audit, the process for disseminating intelligence was ad hoc and communicated orally from manager to staff. One CIA detailee characterized the informal process as disorganized, noting that information does not flow smoothly within the FBI, let alone externally. The detailee said it was a common occurrence to attend a meeting with another agency and learn about FBI-developed intelligence for the first time. As another example, the detailee noted that the CIA's Counterterrorist Center (CTC) produces 13,000 intelligence reports a year, all of which are sent to the FBI. In the eight months the CIA detailee had been at the FBI, the detailee had not received a single CIA intelligence report. The detailee said, "Information goes into a black hole when it comes into this building."

This official attributed the FBI's problems in disseminating information within the FBI to two factors. First, the FBI does not have written policies or procedures for disseminating intelligence. The lack of policies and procedures may impede the effective dissemination of intelligence and prevent FBI personnel from knowing what they can expect from different components within the FBI. Second, the FBI's information systems require a person with a need for information to search the FBI's databases to retrieve it. In contrast, the CIA's information systems "push" data to those whose profile meets the criteria.

The inability of intelligence agencies in general to disseminate information consistently has been recognized by other reviews. Both the Joint Inquiry that investigated the intelligence issues related to the September 11 attacks and the Gilmore Commission noted that information

sharing in general is not systematic and needs more attention and oversight.[19] The Staff Director of the Joint Inquiry Staff has testified that:

> No one will ever know whether more extensive analytic efforts, fuller and more timely information sharing, or a greater focus on the connection between these events would have led to the unraveling of the September 11 plot. But, it is at least a possibility that increased analysis, sharing and focus would have drawn greater attention to the growing potential for a major terrorist attack in the United States involving the aviation industry. This could have generated a heightened state of alert regarding such attacks and prompted more aggressive investigation, intelligence gathering and general awareness based on the information our Government did possess prior to September 11, 2001.[20]

When we inquired about the flow of intelligence within the FBI, the FBI did not have a flow chart and had to prepare a narrative description of the process to address our request. The creation of an enterprise architecture and a process map would help the FBI better understand and manage its information flow.[21]

Enterprise architecture is the organization-wide blueprint that defines an entity's functions and systems, including IT systems. It provides a comprehensive view – through models, narratives, and diagrams – of the interrelationships of an organization's operations and structures and how these structures align with the organization's mission.

In a February 2002 review of enterprise architecture used in the federal government, the GAO stated the following:[22]

---

[19] See the Gilmore Commission's (Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction) second and fourth reports, issued in December 2000 and December 2002.

[20] The testimony was before the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence on September 24, 2002.

[21] A process map is a visual aid for picturing work processes and shows how inputs, outputs, and tasks are linked.

[22] The report is entitled "Information Technology: Enterprise Architecture Use Across the Federal Government Can Be Improved" (GAO-02-6, February 19, 2003).

> The architecture describes the enterprise's operations in both: 1) logical terms, such as interrelated business processes and business rules, information needs and flows, and work locations and users; and 2) technical terms, such as hardware, software, data, communications, and security attributes and performance standards. It provides these perspectives both for the enterprise's current or "as is" environment and for its target or "to be" environment, as well as a transition plan for moving from the "as is" to the "to be" environment.

In our December 2002 report entitled, "Federal Bureau of Investigation's Management of Information Technology Investments," we recommended that the FBI continue its efforts to establish a comprehensive enterprise architecture. The FBI agreed with our recommendation and as of April 2003 was still working on establishing the enterprise architecture.

In September 2003 the GAO reported that the FBI does not yet have an enterprise architecture.[23] According to the GAO, the FBI acknowledges the need for an enterprise architecture and has committed to developing one in the fall of 2003. However, the FBI currently lacks the means for effectively reaching this end. For example, the FBI does not have an agency architecture policy, an architecture program management plan, or an architecture program management plan.

As discussed in Finding 2, the FBI has undertaken a number of initiatives to improve its ability to share information both within the FBI and externally. A major step forward is the recent development of Concepts of Operations for the FBI's core intelligence functions, including information sharing. These plans establish goals, provide broad principles, and lay the foundation for developing formal policies and operating procedures. Still, we believe the FBI would be better positioned to manage the changes to its information-sharing processes if it also conducted a process map for information sharing. In its Business Process Reengineering Assessment Guide, the GAO recommends that agencies complete such a map as part of their reengineering efforts:

> Agencies need to develop a common understanding of the processes they use to produce their products and services before they can set about to improve them. Like large private sector organizations,

[23] The report is entitled "Information Technology: FBI Needs an Enterprise Architecture to Guide Its Modernization Activities" (GAO-03-959, September 25, 2003).

agencies can have a confusing web of interconnected processes and sub-processes, many of which cut across several functional departments. It is important to define what the components of each process are, as well as the process' boundaries, dependencies, and interconnections with other processes.

As a start, the agency should map each of its core processes at a high level. High-level process mapping typically results in a graphic representation depicting the inputs, outputs, constraints, responsibilities, and interdependencies of the core processes. This high-level map provides managers and staff with a common understanding of how the processes work and how they are interconnected.

The FBI has many ongoing initiatives that affect its counterterrorism efforts. However, the FBI does not have a blueprint for either its current or intended information-sharing process. The new Concepts of Operations, while a worthwhile effort to delineate goals and provide guiding principles, do not constitute a blueprint that defines the current state and an end state for information sharing. In our judgment, such a blueprint or road map is necessary to ensure that: 1) all the processes are managed well, 2) the initiatives do not conflict or overlap, 3) each units' information-sharing responsibilities are clear to its personnel and other FBI personnel, and 4) the FBI's new IT systems meet the needs of those involved in the FBI's counterterrorism efforts.

Conclusions

The ability of the FBI to share information across sections, units, and offices within the FBI as well as with the intelligence community and state and local law enforcement agencies is critical to the nation's ability to prevent future acts of terrorism. The FBI has identified, and is working to correct, several of the major impediments to its ability to obtain, analyze, and disseminate intelligence and other sensitive information. These obstacles center on the need for IT improvements, a professional intelligence capability, overcoming security issues and perceptions concerning the sharing of information with state and local law enforcement agencies, and the establishment of policies and procedures for managing the flow of information. The recent development of Concepts of Operations for the key aspects of the FBI's intelligence program, including information sharing,

contributes toward a framework for the necessary policies and procedures to reinvent and institutionalize the program.

The flow of intelligence and other useful information allows everyone involved in combating terrorism to view the terrorist threat in a more complete context. For the FBI to meet its information dissemination responsibilities, it must continue to improve its analytical capabilities and its IT systems. In addition, the FBI must develop information-sharing policies, including the extent to which information can and should be disseminated to state and local law enforcement agencies.

Recommendations

We recommend that the Director of the FBI:

1. Using the Concepts of Operations as a framework, establish a written policy on – and procedures for – information sharing, including what types of information should be shared with what parties under what circumstances.

2. Ensure that the FBI-wide enterprise architecture currently under development is accompanied by a process map for information sharing that clearly defines the current state and an end for the information-sharing process so that the numerous information sharing initiatives can be coordinated and properly monitored and managed.

Finding 2: Improvements to Information Sharing

Following the September 11, 2001, terrorist attacks on the United States, the FBI Director established as the FBI's highest priority the prevention of future attacks. The Director realized that the FBI's antiquated IT systems, weaknesses in intelligence analysis and dissemination, and the existing CTD organizational structure itself were adversely affecting the FBI's ability to share intelligence and other information both internally and externally. In response to these recognized weaknesses, the FBI has taken, or is in the process of taking, various steps to more effectively share information within the FBI, with the intelligence community, and with state and local law enforcement authorities. Although many of the FBI's efforts to improve information and intelligence sharing are ongoing, we found that progress is being made along several fronts: 1) modernizing the FBI's IT systems, including a TS/SCI LAN, 2) establishing a professional intelligence capability, 3) reorganizing the CTD and establishing or expanding interagency task forces and other offices in part to allow for better information sharing both internally and externally, and 4) developing Concepts of Operations for improving the FBI's intelligence program, including information sharing.

Information Technology

As discussed in Finding 1, the FBI's archaic information systems have been the main impediment to the FBI's intelligence-sharing efforts. The majority of the FBI officials interviewed during our audit agreed that the FBI's limited and obsolete information systems, lack of compatibility with systems used by the rest of the intelligence community, and the lack of secure systems certified at the TS and SCI levels crippled intelligence sharing within the FBI and to and from the intelligence community. All the officials with whom we spoke expected that the IT improvements underway will greatly improve the FBI's ability to share intelligence and other information. To manage the all-important IT modernization effort, the Director hired seasoned IT professionals from outside the FBI.

Trilogy is the overarching IT project designed to modernize the FBI's systems. Trilogy is intended to upgrade the FBI's: 1) hardware and software – referred to as the Information Presentation Component, 2) communication networks – referred to as the Transportation Network Component, and 3) five most important investigations applications –

referred to as the User Applications Component. In March 2003, the FBI Director announced that the Trilogy wide area network deployment had been completed. According to the FBI, the Trilogy network replaces the FBI's outdated local area and wide area networks. The Trilogy network will enable new applications, such as the VCF, to replace the FBI's obsolete ACS case management system and lays the foundation for electronic information sharing with other agencies. The VCF is part of the user applications component of Trilogy. As described by the FBI, the VCF is the FBI's first real change in workflow and processes away from the legacy of paper and the processes of the 1950s. The FBI expects the VCF, scheduled to come on line in December 2003, to change the way agents and analysts perform their duties and to provide a model for further consolidation of systems and data. In addition to Trilogy and the VCF, the FBI is working on the development of the Secure Counterterrorism Prototype Environment (SCOPE). FBI officials told us that SCOPE will provide the FBI with data warehousing and data mining capability.

Subsequent to the September 11 attacks, the FBI focused on the need to share information both internally and externally. Recognizing its requirement for a secure system that is certified for processing TS/SCI level material, the FBI began a TS/SCI LAN project in February 2002. The TS/SCI LAN is not part of Trilogy, but the same wide area network supports both systems. According to the project manager, the FBI analysts found that given the paper-intensive aspect of the FBI's intelligence operation and the lack of a secure means of disseminating intelligence electronically, there was no assurance that everyone who needed to see intelligence information actually received it. The analysts also found that it was difficult to track information. The TS/SCI information-sharing problem was reported to the FBI Chief Information Officer at that time, a report was presented to the Director, the project was approved, and a budget was authorized.

The project manager told us that the TS/SCI LAN is a pilot project. She explained that the TS/SCI LAN is an external system that interfaces with the secure Joint Worldwide Intelligence Communications System (JWICS) and other classified systems used by the intelligence community. Everyone using the system can connect with the intelligence community and send classified material back and forth through CT-Link and other secure systems with e-mail capabilities. Access to other classified systems can be approved as needed.

The implementation of the TS/SCI LAN pilot was to be accomplished through the deployment of [CLASSIFIED INFORMATION REDACTED] terminals in three phases, to be completed in June 2003. The project manager said the FBI met its June 2003 goal for completing the project. After the LAN is successfully tested, the FBI plans to expand the pilot to the New York and Washington field offices. The field office expansion will be a separate project with a separate architecture. To conserve time and money, the project managers decided to use an existing DOD system that was already accredited and certified for TS/SCI.

Phase I, for [CLASSIFIED INFORMATION REDACTED] users, mainly intelligence analysts in the CTD, included engineering, design, development, hardware and software procurement, installation, testing, preliminary accreditation, and certification testing. Phase I was completed in December 2002. The TS/SCI LAN received interim authority to operate based on: documenting a security plan, identifying an information systems security officer, documenting the audit policy, and work on security risks as identified by the FBI's security staff. The system was certified and accredited at a protection level 2.[24] The level 2 certification and accreditation was approved, although the system was tested at a protection level 3 and the FBI is planning to eventually operate at level 3.

During Phase II of the pilot project, another [CLASSIFIED INFORMATION REDACTED] users were added in the CTD and in the Counterintelligence Division, the user requirements were reviewed, a Configuration Management Plan was developed, and the System Security Plan was completed. An FBI official told us that the Security Plan is, and will continue to be, a "living document" that will change with enhancements and requests made for system adjustments. In March 2003, Phase II was completed, and the FBI installed 21 more workstations than initially planned. At the time of our audit in March 2003, a total of [CLASSIFIED INFORMATION REDACTED] workstations were up and running, and the pilot project was in its third and final phase. During this phase, the implementation strategy calls for the installation of about [CLASSIFIED INFORMATION REDACTED] more workstations mainly in the CTD and in the Counterintelligence Division, for a total of at least [CLASSIFIED INFORMATION REDACTED] workstations.

[24] The National Security Agency (NSA) has established a 4-level protection rating, with level 1 being the least secure.

The TS/SCI LAN pilot project is a critical step toward improving the FBI's information-sharing capability. At the time of our audit, the pilot project appeared to be meeting its time and performance goals over the approximately 18-month project period. However, we did not independently assess the cost, schedule, and performance of the pilot project or determine user satisfaction. Expanding the TS/SCI LAN to the FBI's field offices will be an ambitious and costly endeavor that should be closely monitored by FBI management.

Intelligence Analysis and Dissemination

The FBI has undertaken several initiatives to develop and professionalize its intelligence operation and to improve information sharing within the intelligence community. These methods include personnel exchanges with other federal agencies, particularly the CIA, developing a cadre of professional intelligence analysts and Reports Officers, and establishing an Office of Intelligence independent of the CTD.[25]

The exchange of personnel with the CIA is one of the primary means by which the two agencies have attempted to improve their cooperation. According to an FBI Assistant Director, the exchange of personnel has brought to the FBI a highly qualified group of counterterrorism and intelligence experts to share their expertise. As of March 2003, the following CIA employees were detailed to the FBI: 4 managers, 25 analysts, and 30 full-time and 6 part-time officers to JTTFs throughout the country. In commenting on a draft of this report in September 2003, FBI officials stated that nearly all of the CIA personnel detailed to FBI headquarters have returned to the CIA.

The CIA is also represented on the National JTTF (NJTTF) in FBI headquarters, allowing for the direct exchange of information among the participating agencies. Before and after the 2001 terrorist attacks, CIA mangers have served as Deputy Section Chiefs in the FBI, and FBI managers have served as Deputy Directors of the CIA's CTC. In May 2004, both the CIA's CTC and the FBI's CTD are expected to co-locate to further facilitate information sharing between the two agencies. Since May 1, 2003, CIA and FBI representatives have also served together in the Terrorist Threat

[25] In September 2003 the FBI announced that it would manage a multi-agency Terrorist Screening Center that consolidates the various agency watch lists. The Center was established on December 1, 2003, but was not yet fully functional.

Integration Center (TTIC). The CIA representatives at FBI headquarters and at the JTTFs have access to classified CIA computer systems and intelligence. However, as mentioned previously, at the time of our audit the FBI's systems did not allow for the dissemination of TS or SCI information, nor was there any interface between FBI systems and the CIA's classified systems. Therefore, information is exchanged between FBI and CIA representatives through conversation, exchange of written intelligence products, and information taken from computer systems, cables, and other documents. Also, the two agencies share information twice daily through secure video teleconferences, which will be discussed in Finding 3 of this report.

The FBI is in the process of hiring analysts and Reports Officers for headquarters and field offices and has developed or revised position descriptions and established formal career paths to attract qualified personnel. However, the entire intelligence community is competing for qualified applicants. The FBI's plans for analysts have been evolving since completion of our audit work. According to the Counterterrorism Division Administrative and Resource Unit, as of March 2003 the FBI planned to have five types of positions involved in the FBI's intelligence work: 1) Intelligence Specialists, 2) Operations Specialists, 3) Reports Officers, 4) Technical Information Specialists, and 5) Case Management Assistants. At that time, the goal of the CTD was to hire a total of [CLASSIFIED INFORMATION REDACTED] support personnel, including [CLASSIFIED INFORMATION REDACTED] Intelligence Assistants, [CLASSIFIED INFORMATION REDACTED] Intelligence Operations Specialists, and [CLASSIFIED INFORMATION REDACTED] Intelligence Research Specialists, among others. Existing Intelligence Research Specialists, who were in grades GS-9 through GS-14, would be called Intelligence Specialists with promotion potential increased up to GS–15. Personnel hired for this position would be required to have college degrees. The former Intelligence Operations Specialist position was to be divided into two new positions: Operations Specialist and Reports Officer. These positions were to span grades GS–9 through GS-14. GS-9/11/12 Technical Information Specialists would be data miners who extract information from databases. The former Investigations Assistants would be called Case Management Assistants at the GS–6/7/8 level and would perform less complex searches and data extraction based on leads from the field offices. The position descriptions had been written for the GS-14 and GS-15 positions, and position descriptions for the other grades were in the process of being written at the

time of our audit work. A table detailing the status of the hiring process as of March 2003 can be found in Appendix 3.

The FBI's September 2003 Concept of Operations on "Human Talent for Intelligence Production" – developed since the Office of Intelligence assumed responsibility for the hiring, training, and promotion of analysts and Reports Officers – modified the CTD's approach to the hiring and career path of the analysts. The plan for analysts encompasses three positions and does not address the formerly-planned Technical Information Specialist and Case Management Assistant positions. The three positions discussed in the current plan are: Operations Specialists, Reports Officers, and Intelligence Analysts. In commenting on a draft of this report, FBI officials stated that the utilization of other supporting positions was being evaluated. Also, the officials clarified that the Intelligence Analyst and Reports Officer positions have full performance levels to GS-14, with competitive promotion to GS-15 possible in headquarters. The plan suggests the same grade structure for the Operations Specialist position, which currently has a full performance level of GS-14 at headquarters and GS-13 in the field offices. According to the plan, analysts who do not currently have a college degree will be encouraged to complete a 4-year degree program.

According to the Chief of the CT Administration and Resources Unit, hiring qualified people for the new Reports Officer positions has been very difficult, despite 60 applicants for each vacancy, because the only analogous position exists in the CIA. In order to hire the best possible personnel, the FBI's plan is to start from the bottom up and hire people at the lower grade levels and train them as Reports Officers. The FBI is also exploring the use of the Presidential Management Intern program to fill the positions. In February 2003, the Chief estimated that it will take from 12 to 18 months to fully staff the Terrorism Reports and Requirements Section. In addition, the Chief stated that although the FBI has a deployment plan to locate Reports Officers in the field offices as well as headquarters, a position description for the field Reports Officer position had not yet been developed. The deployment plan calls for locating four to five Reports Officers in the larger field offices, such as New York and Washington, and one to two in the other field offices.

While the FBI has identified the types of analyst positions required to enhance its intelligence analysis and reporting capabilities, established career paths, and was in the process of writing position descriptions, the actual hiring of the analysts has been problematic and slow. The reasons for

the lack of timely hiring center on identifying qualified applicants and doing the required background investigations necessary for the appropriate security clearances.[26]

As of March 2003, the FBI was in the process of developing a training program for the newly hired Reports Officers and analysts. The FBI was considering the CIA's model of selecting the analyst, providing formal training, and then placing the person on the job. Training was to include a 2-week course at the FBI's College of Analytical Studies and at least a 30-day assignment at FBI headquarters.[27] At the time of our audit, the FBI Training Division was working on a curriculum for analysts at the College of Analytical Studies, which will offer introductory, intermediate, and advanced courses. Some courses were already available – for example, a 1-day Arabic course intended to familiarize analysts with Islamic culture. The planned training includes bringing subject matter experts from the CIA to offer training.

In a further step to improve the FBI's intelligence capabilities and overall management, in April 2003 the Director named an National Security Agency (NSA) executive as the Executive Assistant Director for Intelligence, and an FBI Special Agent in Charge was promoted to Assistant Director of the new Office of Intelligence (OI), which is now a separate office from the CTD.

During his March 4, 2003, testimony before the Senate Committee on the Judiciary, the Director reported that the Executive Assistant Director for Intelligence was first and foremost responsible for ensuring that the FBI had the optimum strategies, structure, and policies in place to support the FBI's counterterrorism mission. The Director stated that the OI will cover all types of intelligence activities including counterterrorism, counterintelligence, criminal, and cyber and will be responsible for ensuring that the FBI is sharing information with its federal, state, and local partners. Further, OI was to be responsible for: 1) establishing and managing the careers and career development of analysts and Reports Officers throughout the FBI,

[26] In this audit we did not evaluate the adequacy of the number of analysts to be hired, the qualifications of analysts already hired, or the deployment and utilization of the analysts. The OIG plans to begin a separate audit of the hiring and training of the FBI's intelligence analysts in September 2003.

[27] The FBI established the College of Analytical Studies in October 2001 in Quantico, Virginia.

2) managing the FBI's intelligence requirements process, and 3) establishing and managing newly designated intelligence units composed of agents and Reports Officers located in each of the FBI field offices. The Assistant Director for Intelligence anticipated that the OI would task field office intelligence units to develop collection strategies to meet the FBI's intelligence requirements. In addition, the Assistant Director for Intelligence told us that the OI will have a Confidential Sources component to centralize under a standard policy the development and use of all human sources involving both criminal and terrorist activities.

Analysts and Reports Officers are physically located in the CTD (and certain other operating divisions and offices) and are under the operational control of the division. The OI will exercise administrative control over the analysts and Reports Officers and will manage their careers, including hiring, training, promotion, and placement. FBI officials said they did not anticipate any organizational friction over the split between operational and administrative control of the analysts and the Reports Officers.

Reorganization of the Counterterrorism Division

In part to improve counterterrorism operations and intelligence analysis and in part to enhance the exchange of information, in June 2002 the FBI began reorganizing the CTD and expanding the number of sections from two to nine. (See the CTD organizational chart of page 7 of this report.) The nine sections are located among two operational branches and one analysis branch under separate Deputy Assistant Directors. While the reorganization of the CTD itself represents a desire to improve information sharing, a number of sections and units began individual initiatives to enhance information-sharing processes. Because the reorganization illustrates one of the Director's key efforts to improve the flow of information both within the FBI and externally, a detailed description of each section and its initiatives for sharing intelligence information follows.

The Counterterrorism Operations Branch

The Deputy Assistant Director for the Counterterrorism Operations Branch manages the following five sections: 1) the Terrorist Financing Operations Section (TFOS), 2) Domestic Terrorism Operations Section (DTOS), 3) International Terrorism Operations Section I (ITOS I), 4) International Terrorism Operations Section II (ITOS II), and 5) Terrorism Reports and Requirement Section (TRRS).

The TFOS is an operating section that supports the other CTD operational sections by providing information on terrorist financing. This section was formed in response to the need for a more comprehensive, centralized approach to investigating terrorist financial matters. The TFOS mission is to identify, investigate, prosecute, disrupt, and incrementally dismantle all terrorist-related financial and fund-raising activities. The section is composed of four units: Radical Fundamentalist Financial Investigative Unit, Domestic WMD and Global Financial Investigations Unit, Global Extremist Financial Investigations Unit, and Financial Intelligence Analysis Unit.

At the time of our audit, the TFOS was in the process of identifying public, private, and government sources of information on terrorist financing. TFOS documents stated that in its efforts to improve the sharing of information within and outside the FBI, the TFOS was working on: 1) conducting a national and international outreach initiative to share information on terrorist financing methods with the financial and law enforcement communities, 2) developing capabilities to predict trends and patterns associated with terrorist activities, and 3) contacting the financial services industry in order to facilitate the exchange of knowledge and data concerning potential terrorist financial activities. In addition, according to TFOS managers, the section has established extensive liaison with key federal agencies and with state and local law enforcement agencies. The TFOS shares financing data and analyses with the intelligence community. To improve its working relationship with the JTTFs, the TFOS was in the process of identifying and training Terrorist Financing Coordinators to be located within each JTTF.[28] The coordinator is to ensure the consistent flow of terrorist financing information to and from the JTTFs. Further, the Financial Intelligence Analysis Unit of TFOS was acquiring project management software for managing tasks and assigning accountability. The Unit Chief stated that the software would help him manage and improve the sharing of information related to terrorist financing and would be compatible with the FBI's new Trilogy system.

The DTOS is one of the two sections remaining from the previous CTD structure. Under the new CTD organization, the DTOS is composed of the following four units:

[28] The JTTFs will be discussed in more detail later in this section of the report.

- Domestic Terrorism Operations – is responsible for investigating all domestic terrorist cases (not foreign-based or foreign supported terrorists), from right wing anti-government and white supremacist groups to left wing animal rights and environmental extremists and others such as the Macheteros revolutionaries in Puerto Rico.

- WMD/Unconventional Threats Operations Unit – assesses terrorist threats involving WMD and performs related investigations.

- WMD/Unconventional Threat Countermeasures Unit – is responsible for providing training and policy guidance to other FBI offices and to state and local first responders.

- Special Events Unit – works with the U.S. Secret Service and the Federal Emergency Management Agency in coordinating security for special events.

The FBI applies a broad definition of terrorism in the types of matters covered by the DTOS. In addition to domestic terrorists who might seek to create mass casualties to further their anti-government views, the DTOS also monitors and investigates any criminal activities associated with animal rights, environmental, and anti-abortion extremists, as well as by certain social protestors. According to the Section Chief, the activities of these types of social extremist groups have become more violent over the years. The Section Chief cited as an example the Animal Liberation Front's attacks against animal testing laboratories to protest animal testing.

To the extent that the FBI seeks to maximize its counterterrorism resources to deal with radical Islamic fundamentalist terrorism, WMD, and domestic groups or individuals that may seek mass casualties, we believe that FBI management should consider the benefit of transferring responsibility for criminal activity by social activists to the FBI's Criminal Investigative Division. Although the activities of such groups fall under the FBI's definition of domestic terrorism, a more focused definition may allow the FBI to more effectively target its counterterrorism resources. In commenting on a draft of this report, FBI officials disagreed that any part of the DTOS investigative activities, including property crime, should be considered for transfer to the Criminal Investigative Division. The officials stated that the activities of radical groups and individuals fall within the definition of domestic terrorism in Title 18, U.S.C. 2331(5). The officials further commented that domestic radicals have caused economic harm, and

such groups use methods similar to international terrorists such as in the areas of operational and communication security, fund raising, and money transfers.

To reduce manager's span of control, in the summer of 2002 the former ITOS was split into two separate operating sections. ITOS I was assigned al-Qaeda and other Sunni-type terrorist groups. The section is composed of the following three units: Regional/Extraterritorial, Continental United States (CONUS) I, and CONUS II. The ITOS I Section Chief told us that his section shares information with state and local law enforcement authorities primarily through the JTTFs. The fact that all JTTF members hold security clearances allows for the exchange of classified intelligence information. The JTTFs in turn provide information to FBI headquarters; FBI counterterrorism squads provide information on leads or investigations in the form of Urgent Reports and/or the more formal and slower EC. Information from the intelligence community arrives in the section [CLASSIFIED INFORMATION REDACTED]. However, according to the Section Chief, [CLASSIFIED INFORMATION REDACTED] from the intelligence community were not necessarily distributed to those FBI employees who needed the information. Pending IT improvements that may resolve the problem, at the time of our audit ITOS I was setting up a system so that when communications arrive at the FBI [CLASSIFIED INFORMATION REDACTED] would ensure that the information was forwarded to the proper FBI section.

The ITOS II is responsible for operations dealing with terrorism groups and State sponsors of terrorism other than Al-Qaeda and other Sunni fundamentalists. ITOS II has the following three units.

- Global Operations Unit – [CLASSIFIED INFORMATION REDACTED].
- Iran/Hizballah Unit – [CLASSIFIED INFORMATION REDACTED].
- Middle East Operations Unit – [CLASSIFIED INFORMATION REDACTED].

The ITOS II has a CIA manager serving as Deputy Section Chief, and an FBI manager is detailed to the CIA's CTC as a Deputy Director. According to the Section Chief, this interagency exchange facilitates coordination with the intelligence community at large. Not only does information sharing take place face to face, but [CLASSIFIED INFORMATION REDACTED]. As with the

CIA, a DOD representative is also located at the ITOS II, and an FBI employee is assigned to DOD. At the time of our audit, the FBI reported [CLASSIFIED INFORMATION REDACTED].

The ITOS II Section Chief told us that there are no restrictions on the sharing of information with other agencies in the intelligence community. He added that all parties recognize that some information is unique to an agency and its mission and that sources and methods may be deleted from the information.

Because the FBI does not have a system that allows for electronic review of all FBI documents, the ITOS II was experimenting with a quasi-electronic review using the existing internal e-mail system. Under this "work-around" system, a supervisor receives an e-mail with the document in question as an attachment. If the supervisor wants to make a change, he/she will be able to confirm that he/she has reviewed the document through an e-mail. Legal documents, highly classified information, and Foreign Intelligence Surveillance Act (FISA) related documents continue to be reviewed only as hard copies.

The TRRS is a new section designed to provide the FBI with an intelligence collection, analysis, and reporting capability. Although not fully staffed at the time of our audit, the section was led by an experienced CIA manager. When fully staffed, it will be composed of the following five units: Reports Policy and Asset Vetting Unit; Radical Fundamentalist Extremist Collection, Evaluation, Dissemination Unit; Global Middle East Extremist Collection, Evaluation, Dissemination Unit; WMD Unconventional Threat Collection, Evaluation, Dissemination Unit; and Domestic Collection, Evaluation, Dissemination Unit.

The TRRS is working with the CTD headquarters sections, field offices, Legal Attaches abroad, the intelligence community, and other customers to identify and address intelligence requirements and gaps. At the time of our review, the TRRS had produced and disseminated within the FBI and to intelligence agencies numerous products, including about 350 Intelligence Information Reports (IIRs). The IIRs will be further described and discussed in Finding 3 of this report.

The TRRS Section Chief is working on several initiatives to fully develop the TRRS and its analysts and Reports Officers. For example, she was developing a training plan for the Reports Officers, had written a

position description, was developing a proposal for a formal career path, and planned to develop a policy manual to make the section a professional intelligence reporting organization similar to the CIA's reporting operation.

The Operational Support Branch

The Deputy Assistant Director of the Operational Support Branch manages the CTD's administrative and resource functions, FBI detailees to other agencies, and the Foreign Terrorist Tracking Task Force, which is discussed later in this section of the report. The branch also manages the Counterterrorism Operational Response Section and the National Threat Center Section.

One main element of the Counterterrorism Operational Response Section is the NJTTF.[29] About 30 federal agencies are represented in the NJTTF. Participants include the intelligence agencies, DOD, Internal Revenue Service, DHS, and the Washington Metropolitan Police Department. According to the FBI, NJTTF members have security clearances and receive all intelligence and other information that their FBI counterparts receive. As part of its efforts to improve information sharing with state and local law enforcement, the FBI plans to establish a fellowship program to bring officers from different states into the NJTTF so they can see first hand what information is and is not available. The NJTTF also conducts special projects to share the results with state and local law enforcement agencies, such as determining: 1) the characteristics of "lone wolf" offenders, and 2) what can be done to identify terrorist sleeper cells. The NJTTF is also responsible for the "Gateway" or St. Louis pilot project, an effort to create a data warehouse of FBI, state, and local investigative case information for access by the FBI and participating state and local law enforcement agencies. Further details on the "Gateway" project are in Appendix 4.

After the September 11 terrorist attacks, the FBI established an Executive Watch in the SIOC to allow FBI executives to receive updates and information about terrorist events around the clock. Since then, a central threat unit evolved, and the National Threat Center Section (NTCS) was established in late 2002 and then reconfigured early in 2003 to include the: 1) Threat Monitoring Unit, 2) Terrorist Watch and Warning Unit, and

[29] The other elements of the Counterterrorism Operational Response Section are the Fly-Away Rapid Deployment Teams and the Military Liaison and Detainee Unit.

3) Counterterrorism Watch Unit (CT Watch). Although the NTCS has neither an investigative nor an analytical role, the section performs limited initial analysis to determine the validity of a threat and which operational unit needs to be notified for investigation or other operational response. The NTCS also provides input to the Director's Briefing, including the Threat Matrix. The Director's Briefing and the Threat Matrix are discussed in Finding 3 of this report.

According to the Chief of the Threat Monitoring Unit, the unit was initially known as the Threat Analysis Operations Group and, because all of the September 11 attacks involved hijacked aircraft, the group tracked only aviation threats. Eventually the group began collecting data on all threats. Under the CTD reorganization, the Threat Analysis Operations Group became the Threat Monitoring Unit with expanded responsibilities for threat monitoring and information sharing. The Threat Monitoring Unit is neither an operational unit nor an analytical unit, since the unit does not initiate leads or have a role in prosecutions. An FBI official described it as a "conduit." The mission of the Threat Monitoring Unit is to ensure that operational units within the FBI and agencies with counterterrorism responsibilities outside of the FBI receive information on terrorist threats. According to the Unit Chief, once information on a threat is passed to the appropriate operational unit, the Threat Monitoring Unit continues to communicate with the operational unit until the threat reaches one of four outcomes: 1) mitigation, 2) determination the threat is not credible, 3) the threat is investigated to the point where there are no more actionable leads, or 4) the threatened event actually occurs.

The Unit Chief told us that the Threat Monitoring Unit created a database of all credible threats it had received since September 11, 2001. The database includes a description of each threat and its resolution. As of March 2003, the unit had chronicled about 2,500 threats in this database. The system has key word search capability and [CLASSIFIED INFORMATION REDACTED]. Currently, the database is only available within the FBI. However, the Threat Monitoring Unit is planning to disseminate the data [CLASSIFIED INFORMATION REDACTED].

The Terrorist Watch and Warning Unit, established in March 2002, is responsible for providing state and local law enforcement agencies with warnings about terrorist threats and for maintaining the FBI's Terrorist Watch List in the National Crime Information Center (NCIC) system. The unit also has input to the color-coded threat warning system managed by

the DHS. To accomplish its mission of sharing FBI information with state and local law enforcement agencies nationwide, the unit disseminates weekly unclassified Intelligence Bulletins, Quarterly Threat Assessments, and periodic National Law Enforcement Telecommunications System (NLETS) messages to state and local law enforcement agencies on a "law enforcement sensitive" basis. The information disseminated in these products includes background on terrorist groups, their activities, and their methods of operating. These products will be further described and discussed in Finding 3 of this report.

The Terrorist Watch and Warning Unit's Terrorist Watch List responsibilities entail placing names of terrorist suspects from the FBI's Violent Gang and Terrorist Offender File into the NCIC for access by law enforcement officers who, through traffic stops or arrests, may encounter a terrorist suspect. In addition to the name of the possible terrorist, the NCIC entry includes guidance of what action the law enforcement officer should take: detain the person, arrest the person, or call the local JTTF. As of March 2003, there were approximately 5,000 names listed in the Terrorist Offender section of the Violent Gang and Terrorist Offender File. Of those 5,000, about 2,500 are international terrorism suspects, about 1,300 are detainees, and about 1,200 are domestic terrorism suspects. The list is continuously updated.

The CT Watch Unit receives and screens incoming threat information. The staffing of CT Watch includes a watch commander, two watch officers, two Intelligence Operations Specialists, two investigation research specialists, one representative from the Threat Monitoring Unit, one representative from the Terrorist Watch and Warning Unit, and two supervisory special agents. The watch commander, watch officer, and Intelligence Operations Specialist positions are staffed 24 hours a day, 7 days a week. All other positions are staffed 16 hours a day, 7 days a week.

According to the Chief of the CT Administrative and Resource Unit, the NTCS assumed responsibility for both the SIOC staff and facility in March 2003. The Chief of the NTCS had pointed out that although the SIOC was not initially intended to be a counterterrorism operations center, roughly 95 percent of the events that have required the use of the SIOC facility have been related to terrorism.

In addition to each unit's initiatives, the Chief of the NTCS told us that he is in the process of writing a concept of operations that will outline a system for the flow of information within the section. He said he also is developing a protocol to scrub information on intelligence sources and methods from the threats database to allow the information to be placed [CLASSIFIED INFORMATION REDACTED] for dissemination outside of the FBI.

The Counterterrorism Analysis Branch

The third branch in the current CTD organization is the Counterterrorism Analysis Branch. The Deputy Assistant Director for Counterterrorism Analysis manages the Counterterrorism Analysis Section and the Communication Exploitation Section. The branch also includes a Strategic Assessment and Analysis Unit, Production and Publications Unit, and Presidential Support Group (subsequently transferred to the Office of Intelligence).

As with the TRRS, at the time of our audit the Counterterrorism Analysis Section was in the process of being formed to help bring to the FBI a more comprehensive and professional intelligence analysis capability. The section was managed by an experienced CIA official on detail to the FBI and had 25 CIA analysts on one-year details to support the CTD's operational sections, chiefly ITOS I, ITOS II, and DTOS. To permanently staff the section, the FBI was in the process of recruiting analysts and providing them with a career path. When fully staffed, the section is expected to have the following five units: Domestic Sunni Extremist Unit, Shia/Middle East Analysis Unit, Foreign Links/Global Targets Analysis Unit, Domestic Terrorism Analysis Unit, and WMD and Emerging Weapons Analysis Unit.

The Communication Exploitation Section was established [CLASSIFIED INFORMATION REDACTED]. The section has four units: [CLASSIFIED INFORMATION REDACTED].

According to the Section Chief, [CLASSIFIED INFORMATION REDACTED]. The Section Chief told us that any information gleaned is immediately shared among three organizations: the CIA for Outside Continental U.S. (OCONUS) leads on terrorists, the FBI for CONUS leads, and the DOD for force protection.

[CLASSIFIED INFORMATION REDACTED]. The Section Chief told us that the FBI partners with [CLASSIFIED INFORMATION REDACTED].

[CLASSIFIED INFORMATION REDACTED]. The Section Chief told us that [CLASSIFIED INFORMATION REDACTED]. He added that any threat-related information is then disseminated, [CLASSIFIED INFORMATION REDACTED], to FBI units responsible for issuing warnings and taking operational action. [CLASSIFIED INFORMATION REDACTED].

At the time of our audit, [CLASSIFIED INFORMATION REDACTED] was in the process of building the necessary infrastructure to better manage and disseminate intelligence. The unit was responsible for setting up [CLASSIFIED INFORMATION REDACTED]. The Section Chief told us that an upcoming [CLASSIFIED INFORMATION REDACTED]. The system will allow an FBI headquarters supervisor to track the progress of a field office in the following areas: [CLASSIFIED INFORMATION REDACTED]? This initiative, which affects eight FBI divisions, had been approved at the Executive Assistant Director level and at the time of our audit was awaiting the approval of the Deputy Director.

Task Forces

As indicated previously in this report, the FBI has established several types of task forces to aid its ability to perform its high-priority mission of preventing terrorist attacks and to facilitate the sharing of information with participating federal, state, and local agencies. In addition to the NJTTF discussed earlier in this section of the report are the local and the regional JTTFs and the Foreign Terrorist Tracking Task Force.

The Joint Terrorism Task Forces

To enhance its responsiveness to the terrorist threat and to provide for direct sharing of intelligence and other information, the FBI has increased the number of JTTFs from 36 in 2001 to 84 in 2003. In addition to FBI personnel, JTTFs include state and local law enforcement officers and representatives of various federal agencies. The JTTFs are supervised by FBI Supervisory Special Agents and are locally managed by the Special Agent in Charge or Assistant Directors in Charge of the respective field office. The first formal JTTF was established in New York City in 1980. The task forces vary in size from office to office and are structured in relation to the terrorism threat dealt with by each office. Examples of

federal law agencies participating in the JTTFs on a part-time or a full-time basis include the former Immigration and Naturalization Service (INS); former Customs Service; U.S. Secret Service; Naval Criminal Investigative Service; Bureau of Alcohol, Tobacco, and Firearms; U.S. Marshals Service; and U.S. Department of State's Diplomatic Security Service among others.[30] The JTTFs generally have about 40 to 50 people assigned to them; however, some, such as New York, have as many as 500 people. At the time of our audit approximately 1,245 FBI agents, 650 state and local law enforcement officers, and over 400 federal agency representatives served full-time in JTTFs. Additional members participate in the JTTFs on a part-time basis. All JTTFs (and FBI field offices) are responsible for investigations involving international terrorism, domestic terrorism, WMD, and national infrastructure protection.

According to several FBI officials, JTTFs routinely share intelligence and other information within the task force, the members of which all have TS security clearances. State and local law enforcement agencies may pass along information to their home agencies on a cleared and need-to-know basis. However, as discussed in Finding 1, many higher-level state and local law enforcement officials have not applied for security clearances and do not have lawful access to the information available to the JTTF participants. The information-sharing method varies from one JTTF to another, but is largely informal and based on direct discussion or the exchange of hard copy documents. Again, the FBI's IT problems prevent the electronic dissemination of classified information.

The FBI is working on standardizing the mechanism for sharing information with state and local law enforcement agencies through the JTTFs. Any threat information developed by the JTTFs is to be communicated directly to the CT Watch Unit in FBI headquarters. Some local JTTFs have their own information-sharing initiatives. For example, the Dallas and Houston JTTFs have begun a project to notify state and local law enforcement agencies of terrorism threats through pagers with text messaging capability.

[30] A number of these agencies, including the INS, Customs Service, and Secret Service are now part of the Department of Homeland Security.

Foreign Terrorist Tracking Task Force

On August 6, 2002, the Attorney General directed that the Foreign Terrorist Tracking Task Force be formally consolidated with the FBI's CTD. The Foreign Terrorist Tracking Task Force operates under a Section Chief within the CTD's Operations Support Branch, who also has the title of task force Director. Homeland Security Presidential Directive 2 states that the mission of the task force is to: 1) deny entry into the United States of aliens associated with, suspected of being engaged in, or supporting terrorist activity; and 2) locate, detain, prosecute, or deport such aliens already present in the United States. The Foreign Terrorist Tracking Task Force has three units: 1) the Tracking and Detection Unit, 2) the Flight Training Security Unit, and 3) the Alien Security Advisory Unit.

Within the Foreign Terrorist Tracking Task Force, the Tracking and Detection Unit has the core function of preventing and detecting the entry of terrorists into the United States. The Tracking and Detection Unit's primary analytical process is to compare a list of known terrorists and supporters with data sets of public and private providers. The Flight Training Security Unit is responsible for implementing Section 113 of the Aviation and Transportation Security Act.[31] The Alien Security Advisory Unit largely supports the former INS in implementing the National Security Entry Exit Registration System, the Congressionally mandated system that requires registration of certain males from certain countries between certain ages. The main work of the task force is to compare aggregated data sets in an attempt to identify and locate known terrorists or their supporters. To accomplish this the task force uses the Department of State's Tipoff system, the Terrorist Offender portion of the NCIC, and I-94 data collected by the from non-immigrant aliens.[32]

[31] Section 113 directed the Attorney General to conduct background investigations and assess the risk of aliens who want to train as pilots – and receive FAA certification – of planes weighing over 12,500 pounds.

[32] The I-94, or Arrival-Departure Record, shows the date a person arrived in the United States and the "admitted until" date. An I-94 that has been approved by an immigration agent serves as proof that the person arrived in the country legally and did not overstay.

The Office of Law Enforcement Coordination

In April 2002, the Director appointed a former Chief of Police as the Director of the FBI's Office of Law Enforcement Coordination (OLEC). The OLEC was established to improve coordination and liaison between the FBI and the federal, state, and local law enforcement communities. The goals of the OLEC were to: 1) build partnerships with the law enforcement community, 2) enhance the FBI's customer service to the law enforcement community, 3) ensure the administrative effectiveness of the OLEC team, and 4) measure and evaluate performance. The OLEC's strategic plan included among its objectives: 1) provide general counterterrorism guidance to state and local law enforcement, 2) help clarify the roles of various law enforcement community members in the fight against terrorism, 3) promote information sharing in the law enforcement community through Law Enforcement Online and other technologies, and 4) help state and local law enforcement operationalize their response to the Homeland Security Advisory System.

According to OLEC documents, the OLEC provides advice and guidance to FBI executives regarding the utilization of state and local law enforcement expertise and resources in criminal, cyber, and counterterrorism investigations, and recommends policies and programs to enhance the FBI's relationships with its state and local partners. The OLEC coordinates the Director's Law Enforcement Advisory Group and certain aspects of the FBI's intelligence and technology efforts with state and local law enforcement. Additionally, the OLEC serves as the FBI's primary point of contact for national law enforcement organizations such as the International Association of Chiefs of Police, the National Sheriffs Association, and the Fraternal Order of Police. The OLEC is also responsible for liaison with the Department of Justice's Office of Justice Programs and Office of Community Oriented Policing Services.

The Terrorist Threat Integration Center

In January 2003, during his State of the Union Address, the President announced an initiative to better protect the nation by continuing to close the "seam" between the analysis of foreign and domestic intelligence on terrorism. The President asked the Director of Central Intelligence (DCI) and the Director of the FBI to work with the Attorney General and the Secretaries of Homeland Security and Defense to develop the unified TTIC. The purpose of the center is to merge and analyze terrorist-related

information collected domestically and abroad in order to form the most comprehensive possible threat picture. Although the center is not to engage in information collection, it can establish requirements for the participating agencies. Specifically, the center is to:

- optimize the use of terrorist threat related information, expertise, and capabilities to conduct threat analysis and inform collection strategies;
- create a structure that ensures information sharing across agency lines;
- define the criteria and standards for terrorist threat reporting;
- be responsible and accountable for providing terrorist threat assessments to national leadership;
- play a lead role in overseeing a national counterterrorism tasking and requirements system and for maintaining shared databases; and
- maintain an up-to-date database of known and suspected terrorists that will be accessible to federal and non-federal officials and entities, as appropriate.

The TTIC was officially established on May 1, 2003, and is led by a former Deputy Executive Director of the CIA. He was appointed by the DCI in consultation with the FBI Director, the Attorney General, and the Secretaries of Homeland Security and Defense, and he reports to the DCI. The center began operating with 50 personnel from the Department of State, DOD, DOJ/FBI, DHS, and other intelligence community agencies. The TTIC was expected to have a staff of 150 by October 2003. The TTIC now produces the Threat Matrix and, with FBI input, the Presidential Terrorism Threat Report.

According to the FBI Director, the TTIC will be crucially important to the success of the FBI mission. He said that he views the center as an important resource that will provide the FBI and other federal intelligence and law enforcement entities with integrated analysis of information from all sources, which can be quickly shared with state and local law enforcement.

On May 1, 2004, the TTIC is expected to co-locate with elements of the FBI's CTD and the CIA's CTC. The joint facility will accommodate

[CLASSIFIED INFORMATION REDACTED] TTIC personnel and [CLASSIFIED INFORMATION REDACTED] employees from the CTC and CTD. In testimony before the Senate Committee of the Judiciary on March 4, 2003, the FBI Director stated that this co-location will:

- speed the creation of compatible information infrastructure with enhanced capabilities, expanded and more accessible databases, and greater [data] network sharing on counterterrorism issues;

- enhance interaction, information sharing, and synergy among U.S. officials involved in the war against terrorism;

- potentially allow for the FBI and the CIA to manage more effectively their counterterrorism resources by reducing overhead and redundant capabilities; and

- further enhance the ability of comprehensive, all source analysis to guide their collection strategies.

He further stated that the co-location will afford greater opportunity to the FBI and the intelligence community to enhance the coordination of operations against terrorist targets inside and outside the United States.

Concepts of Operations

In May 2003, Director Mueller appointed an Executive Assistant Director for Intelligence. One of her first initiatives was an effort to reevaluate how the FBI structures and conducts its intelligence operations. This 10-week initiative produced Concepts of Operations that provide a framework for improving each of nine core intelligence functions defined by the FBI. The FBI's Office of Intelligence, in cooperation with the FBI's headquarters' divisions, created the plans. As of September 2003, four Concepts of Operations had been approved and issued to the field offices, and five of the plans were in draft. Five of the nine plans discuss information sharing and intelligence dissemination, including one draft plan specifically dealing with information sharing. The nine Concepts of Operations are entitled:

- Community Support (draft as of August 2003)
- FBI Intelligence Assessment Process (final in August 2003)

- FBI Intelligence Requirements and Collection Management Process (final in August 2003)
- FBI Field Office Intelligence Operations (final in August 2003)
- Forecasting Intelligence Program Operational Requirements (draft as of August 2003)
- Human Talent for Intelligence Production (final in September 2003)
- Integrated Information Sharing (draft as of July 2003)
- Intelligence Production and Use (draft as of July 2003)
- Intelligence Program Budget Formulation Process (draft as of August 2003).

The FBI's Concepts of Operations are a significant first step toward revamping and institutionalizing the FBI's intelligence processes by establishing a vision for the various components of the intelligence program and related information-sharing processes. The plans vary in their degree of specificity, but all establish a basic framework. Additional work is required to develop the procedures required to implement the plans. Also, the plans are not yet incorporated into formal FBI policy. Other aspects to be considered include an assessment of any budgetary implications to carrying out the plans and the timeframes for accomplishing the overall end state of the intelligence program reinvention process. We noted that some of the plans include language that could be adopted into formal FBI policy manuals. For example, the draft Integrated Information Sharing Plan lists the following eight guiding principles that the FBI expects to apply to its information sharing strategy.

- All FBI data is to be shared within the FBI, with very few exceptions.

- The ownership of FBI information is corporate; no individual division or employee "owns" FBI information.

- The FBI will have a single, integrated information space, in which the default will be to share with agencies with due consideration for the protection of sources and methods, and the security and prosecutive objectives of investigations.

- The FBI will not filter information internally but instead will create an overarching FBI-wide policy that balances the need for cross-correlation with the risks of misuse.

- The view of what the FBI collects and what the FBI creates will look very similar.

- All data collected must also be recorded, searchable, retrievable, and easily cross-correlated.

- FBI employees will have the ability to conduct federated queries across multiple systems to identify relationships.

- Technology will be in service of people instead of people in service of technology. The FBI must have interconnectivity with Intelligence Community systems. Additionally, the FBI must leverage existing technologies instead of rebuilding them.

The information sharing plan recognizes the need for the development of an associated policy, as follows:

> The OI will be the primary author of high-level information sharing policy for the FBI. Intelligence capability is the ability to transform raw data into actionable information. For this reason, the OI has a policy level interest in the accessibility of raw data as well as finished intelligence products. It is the intention of the OI to produce and update this policy with the input and participation of all relevant headquarters and field divisions. These include not only the operational divisions but much of the "support" infrastructure as well.

Conclusions

In recognition of its longstanding weaknesses and to accomplish its highest priority of preventing future terrorist attacks, the FBI has begun a number of initiatives that, in time, should improve its ability to share intelligence and other sensitive information both within the FBI and externally. To solve its problem with processing and sharing information classified above the Secret level, the FBI is implementing a TS/SCI LAN pilot program in addition to the Trilogy project and its VCF and SCOPE components. Because of the importance and difficulty of these FBI IT projects, we believe they require continued close monitoring by FBI management, including the expansion of the TS/SCI LAN to the FBI's field offices.

In addition, the FBI is working to improve its relationship with other members of the intelligence and law enforcement communities. To accomplish this, the FBI exchanged personnel with the CIA, DOD, and other federal agencies and is working closely with other agencies in the NJTTF, the JTTFs, and the TTIC. Still, differences in organizational cultures and operating methods may continue to impede the free flow of information, at least in the short term. The FBI Director's emphasis on information sharing and interagency cooperation should, over time, help break down the barriers between the FBI and other agencies that in the past have prevented a more seamless counterterrorism effort. To improve its relationship with state and local law enforcement, the FBI established the Office of Law Enforcement Coordination and has developed law enforcement sensitive products, which are discussed in Finding 3. These attempts to reach out to state and local law enforcement officials have been helpful but have not remedied concerns of some officials that the FBI too often withholds information. The FBI's plan to have state and local law enforcement representatives rotate into the NJTTF may help state and local law enforcement officials better understand the limited nature of intelligence on terrorist groups and activities.

A major effort is underway to hire and train Reports Officers, Intelligence Analysts, and Operations Specialists. To attract and retain the highest qualified individuals, the FBI has rewritten position descriptions, established career paths, and at the time of our audit was in the process of developing a training plan. However, progress has been slow in hiring qualified analysts. The OIG plans to conduct a separate audit of the hiring and training of FBI analysts beginning in September 2003.

In less than a year, the FBI has expanded the CTD from two to nine sections. New sections were created for terrorism financial review, terrorism reporting, counterterrorism analysis, and communications analysis. The FBI's greater organizational emphasis on counterterrorism is an appropriate step toward the goal of transforming the FBI into an agency that can prevent terrorism as well as investigate terrorist acts after the fact. The FBI's new organizational structure should also facilitate information sharing through units established for that purpose. FBI management should monitor the operating relationship between the CTD and the newly-created Office of Intelligence to ensure coordinated action and adequate support of the CTD's mission on the one hand and proper training and utilization of analysts on the other hand. Also, the CTD's Domestic Terrorism Operations Section should focus on threats involving weapons of mass destruction and preventing domestic terrorist attacks aimed at creating mass casualties or

damaging critical infrastructure. We believe that the FBI should consider assigning other investigations involving, for example, social protests and property crimes committed by environmental, animal rights, and other radical groups and individuals to the FBI's Criminal Investigative Division.

The recent development of FBI-wide Concepts of Operations to improve the overall intelligence function in the FBI is a good and necessary beginning toward establishing guidance and laying the foundation for formal policy and procedures on information sharing. The plans provide broad guiding principles for information sharing and collectively can serve as a springboard for reinventing the FBI's intelligence program.

Recommendations

We recommend that the Director of the FBI:

3. Consider transferring responsibility for investigating crimes committed by environmental, animal rights, and other domestic radical groups or individuals from the Counterterrorism Division to the Criminal Investigative Division, except where a domestic group or individual uses or seeks to use explosives or weapons of mass destruction to cause mass casualties.

4. For each Concept of Operations, develop an implementation plan that includes a budget along with a time schedule detailing each step and identifying the responsible FBI official.

FINDING 3: Dissemination of Intelligence and Information

The FBI has established nine primary methods of disseminating intelligence and other information, either within the FBI or to the intelligence and state and local law enforcement communities. Our analysis showed that the four most informative and detailed methods were those that disseminated highly classified information: the Director's Briefing (since replaced by the more general Director's Daily Report), Intelligence Information Reports, intelligence assessments or estimates, and twice daily secure teleconferences. However, distribution of the intelligence products was limited to FBI components and certain federal agencies. Internally, the Director instituted the concept of Urgent Reports, which enable FBI field offices to convey information in memorandum format directly to senior FBI management. The content of the Urgent Reports was not limited to counterterrorism, and the urgency of the reports was sometimes questionable. The four methods of communicating with state and local law enforcement agencies – Intelligence Bulletins, Quarterly Terrorist Threat Assessments, NLETS messages, and Terrorist Watch List submissions to the NCIC database – disseminate information on a law enforcement sensitive basis. While much of the unclassified information provides state and local law enforcement agencies with useful background and awareness, the information typically is not actionable nor does it necessarily focus on the high risks associated with radical Islamic fundamentalist terrorism. The reality is that specific, actionable information is often unavailable to the FBI. Still, to the extent that classified information may aid the preparedness efforts of state and local jurisdictions, the FBI should continue to encourage state and local officials to apply for security clearances, and to the extent possible, provide classified information to cleared state and local officials who have a need to know.

Director's Briefing and Report

At the time of our field work, the FBI Director received each morning a detailed Top Secret Director's Briefing consisting of four or five sections:

1) Threat Matrix; 2) Operational Highlights; 3) Counterterrorism Update; 4) Summary of Significant Intelligence; and 5) FISA. However, in responding to a draft of this report in September 2003, FBI officials informed us that the Director's Briefing has been replaced by a Director's Daily Report, which eliminates all elements of the former Director's Briefing except the Threat Matrix. As described to us, the Daily Report no longer has a sole focus on counterterrorism. FBI officials described the Daily Report as an FBI-wide summary of significant information arranged by the Director's priorities, including criminal, cyber, and counterintelligence items.

We did not review the new Daily Reports because the FBI initiated the reports after the completion of our audit work. However, during our audit we reviewed Director's Briefings between February 27, 2003, and March 13, 2003. The Director's Briefing was a fluid document that varies according to the Counterterrorism Division's need to inform the Director about sensitive intelligence, and the Director's desire to be kept informed about FBI counterterrorism operations. As an intelligence product, the Director's Briefing demonstrates the FBI's ability to cull intelligence reporting and disseminate only the most important intelligence to its leadership. Because much of the information included in the Director's Briefing is extremely sensitive – Top Secret, SCI, or "eyes only" – the information was not disseminated to the FBI's field offices, partly because the FBI did not have the ability to electronically transmit Top Secret information either within headquarters or to its field offices. Further, most field offices do not have approved facilities to store SCI materials.

Threat Matrix

The Threat Matrix was a joint CIA-FBI product compiled by the CIA. After our audit work was completed, the Threat Matrix was compiled by the TTIC. The matrix summarizes significant reporting from the intelligence community concerning new or updated terrorist threats over the previous 24 hours. A separate threat report summarizing the most important information provided on the matrix is given to the President. The matrix includes a preliminary assessment of each intelligence item and a summary of the actions taken in response. For each item or threat, the following information is included: source, target, alleged group, type of threat, description and analysis, and action taken. Some copies of the Threat Matrix contained handwritten notes indicating referrals to FBI offices. We noted that the Threat Matrix has improved since our previous audit of the FBI's counterterrorism program in September 2002. For example, the matrix now

contains more analysis of the credibility of a given threat, its relationship to other threats, and the terrorist organization's capability to carry out the threat.

The threats listed in the matrices we reviewed dealt almost exclusively with international terrorism. For the 16-day period we reviewed, the number of threats included in each matrix varied from 2 to 19, and averaged about 11. The entries on the matrix were derived from a number of sources and methods. As a result, some entries do not constitute threats as much as they represent significant reporting from intelligence agencies. [CLASSIFIED INFORMATION REDACTED]. Multiple reports about the same threat were combined, and all sources of information were listed.

For the period we reviewed, nearly 80 percent of the threats dealt with U.S. interests abroad. Of the U.S. interests abroad, [CLASSIFIED INFORMATION REDACTED]. Another 10 percent of the entries dealt with targets in the continental United States. Because of the small sample size, the most often targeted facilities can only be categorized as critical infrastructure, [CLASSIFIED INFORMATION REDACTED]. For the remaining 10 percent of the entries, the threat did not indicate a specific target. The threat may have been generalized, [CLASSIFIED INFORMATION REDACTED].

Operational Highlights

The Operational Highlights section was organized according to investigative subject areas – international terrorism, domestic terrorism and WMD – and chronicled major developments in the FBI's casework. The most complete entries were divided into three subheadings: current situation, background, and investigative plan. A few entries contained only the current situation.

The international terrorism investigations portion of the Operational Highlights covered such items as [CLASSIFIED INFORMATION REDACTED].

The domestic terrorism investigations portion of the Operational Highlights covered such items as violations of the Freedom of Access to Clinic Entrances Act and the use of explosives.

Typical of the investigations discussed in the WMD portion of the Operational Highlights were threats of anthrax attacks, suspicious powder

leaking from envelopes, and substances missing or stolen from a university laboratory.

Counterterrorism Update

The Counterterrorism Update section was not always included in the Director's Briefing. When the section is included, it covers new issues, updates, and resolved issues. The update essentially mirrors the Operational Highlights section.

Intelligence Summary

The Intelligence Summary contained significant intelligence community reporting [CLASSIFIED INFORMATION REDACTED]. The summary included a short narrative description of an intelligence item, followed by supporting documentation or analysis. The supporting documentation was typically a printout [CLASSIFIED INFORMATION REDACTED].

In general, the SCI-level Intelligence Summaries updated the Director on what the FBI knows through intelligence community reporting [CLASSIFIED INFORMATION REDACTED].

Foreign Intelligence Surveillance Act

The FISA portion of the Director's Briefing contained an SCI-level summary regarding surveillance on terrorist suspects.

Intelligence Information Reports

The FBI's Terrorism Reports and Requirements Section of the Counterterrorism Division prepares IIRs to disseminate to the appropriate FBI offices, intelligence agencies, and other federal agencies. The IIRs contain specific intelligence that may be actionable or useful in analyzing terrorist activities and "connecting the dots." We reviewed a judgmental sample of 22 Secret level IIRs issued between March 3, 2003, and March 26, 2003. The reports varied in length from 3 to 14 pages, with generally one page listing recipients and one page providing a point of contact and administrative information. The reports state the subject and characterize the credibility of the source. The reports were issued in the form of classified cables.

Although dissemination of the reports varied by content, standard recipients included the intelligence community, certain military components, the White House, and the State Department. FBI dissemination always included the Director, but varied by topic, with some reports provided to specific field offices and Legal Attachés and other reports disseminated to all field offices.

Nearly all of the sampled IIRs related to international terrorists or terrorist activities. A few reports related to [CLASSIFIED INFORMATION REDACTED]. One report seemed to have a criminal focus, but it alluded to an unsubstantiated threat to the President. The information in the reports seemed to be as detailed as possible and would provide recipients with potentially useful information for follow-up or operational action. The reports are not analyzed intelligence or necessarily validated, and this fact is made clear in the reports. The IIRs are not broad threat assessments, intelligence estimates, or finished intelligence products. Rather, the IIRs disseminate specific intelligence to parties that need to know and may need to act quickly on the information. Also, in some cases the FBI is requesting recipients to determine if they have additional information on the topic that can be provided to the FBI.

We conclude that the IIRs are a good means by which the FBI is disseminating specific intelligence. However, the distribution of the reports is necessarily limited to those with appropriate security clearances and a need to know. Consequently the information contained in the IIRs generally would not be disseminated to state and local law enforcement agencies except through a JTTF or unless modified for distribution on a law enforcement sensitive basis.

Intelligence Assessments

The FBI has begun to produce formal, strategic or long-range intelligence assessments in addition to the shorter and more tactical IIRs. We reviewed one major intelligence assessment, or estimate, entitled "The Terrorist Threat to the U.S. Homeland: An FBI Assessment", which also is available in an unclassified law enforcement sensitive version, dated January 2003.[33] The Secret/SCI version is a 65-page document, compared to 27

[33] The assessment fulfilled the recommendation in our September 2002 audit report, 02-38, entitled "Review of the Federal Bureau of Investigation's Counterterrorism Program: Threat Assessment, Strategic Planning, and Resource Management" that the FBI complete a national-level threat assessment.

pages in the unclassified version, that provides a detailed national threat assessment and addresses the likelihood of terrorist attack as well as methods, targets, casualties, and sources. The assessment begins with a three-page "Key Judgments" section, followed by detailed analyses including risk tables (for example, a "Threat and Vulnerability Matrix") and descriptions of terrorist groups and their intentions and capabilities. The assessment describes risks in categories of high, medium, and low. The assessment discusses WMD, but not in great detail. The FBI plans to issue a separate report on the chemical and biological agents most likely to be used in a terrorist attack.

Secure Video Teleconferencing System

Twice daily, FBI CTD officials confer with their counterparts in the intelligence community and with other federal agencies through the Secure Video Teleconferencing System (SVTS). Following the attacks of September 11, the FBI and the CIA started the SVTS sessions to discuss the threats of the day. Initially, the Threat Monitoring Unit represented the FBI at the SVTS, but that responsibility has now transferred to the CT Watch Unit. Participation in the SVTS varies by the nature of the threat being discussed, although from 8 to 15 agencies typically participate. Participating agencies have included: the Department of Justice, FBI, CIA, DHS, Department of Energy, DOD, NSA, Department of State, Federal Aviation Administration, Transportation Security Administration, Coast Guard, Customs Service, Secret Service, and the Postal Service. An FBI official told us that during the SVTS, the agencies discuss unusual or suspicious events that have happened during the past day and examine the events for any nexus to terrorist activity. He stated as an hypothetical example a drunk airline passenger who assaults a flight attendant. Because causing a disruption on an airplane could be a part of an attempt to take over the airplane, the incident would be discussed during the SVTS to determine whether or not there is a terrorist nexus. If the group determined that the incident was related to terrorism, the representatives would be assigned tasks for the investigation or the operational response. The status of the threat is then discussed at subsequent SVTS. In the cited example, however, the assault is not likely to be linked to terrorism, so the issue would not be discussed in subsequent SVTS unless some terrorism connection was discovered.

Although we did not observe any of the sessions, FBI officials explained that the regularly scheduled video conferences were a useful tool for sharing intelligence and other information with other agencies on a

real-time basis. We concur that secure video conferencing is a useful method for direct and timely discussion and exchange of information on potential terrorist activities and resulting counterterrorism actions.

Urgent Reports

After the September 11 terrorist attacks, the Director instituted the concept of Urgent Reports, which allow field offices to provide information directly to senior FBI managers in e-mail format with a formal EC to follow. The written report is often preceded by a telephoned report to FBI headquarters. We reviewed a sample of 42 Urgent Reports issued during March 2003. The FBI received between 1 and 9 reports daily for the period we reviewed. The reports, which averaged one to two pages in length, covered a variety of topics, ranging from criminal investigations to terrorism cases. The Urgent Reports are addressed to the Director, with copies to the Deputy Director and to the FBI's Counterterrorism Watch Unit. Additional recipients vary depending on the topic. Also, the Counterterrorism Watch Unit may distribute the Urgent Report further based on its judgment of what FBI units might need to be aware of the information.

Our analysis of the 42 sampled Urgent Reports found that relatively few were directly related to specific threats of [CLASSIFIED INFORMATION REDACTED] terrorism but instead covered a wide variety of mostly criminal matters. Also, many did not appear to be urgent matters that needed to be brought to the Director's immediate attention. Of 11 reports with an actual or suspected international terrorism connection (26 percent of the total we reviewed), 6 reports discussed 2 al-Qaeda members, 1 reported on the sentencing of Hizballah members, 1 covered a suspected casing incident, 2 dealt with threats over the internet (including a threat to the White House), and 1 was about an incident at a water facility that was found not to be terrorism-related. Overall, the 42 Urgent Reports covered:

- nine bomb threats;
- five airport screening incidents and one update;
- two unruly airline passengers, one hijack threat;
- four burglary, robbery, theft, or extortion cases and one update;
- one missing juvenile, one recovered juvenile;

- two gang activity cases;
- one voter fraud and one indictment of a former public official;
- one local police department news;
- one arrest of a former FBI agent;
- one trespassing case with a terrorism concern;
- one paperwork discrepancy involving biological material;
- one threat to use chemical materials;
- one threat involving potential terrorist surveillance of targets;
- one report on sentencing of Hizballah members; and
- two al-Qaeda investigations and four follow-ups.

Intelligence Bulletins

FBI Intelligence Bulletins are prepared by the Terrorist Watch and Warning Unit under the National Threat Center Section. The Bulletins are issued weekly to some 18,000 law enforcement agencies nationwide to provide information on selected topics from FBI counterterrorism investigations and analyses. The Unit Chief estimated that roughly one-third of the information contained in the Intelligence Bulletins was formerly classified but revised into a law enforcement sensitive version. The Bulletins, which average between one and two pages in length, do not provided threat assessments other than citing the national color-coded threat level. Threat assessments are issued quarterly in a separate document (discussed below), and any immediate threat information is conveyed through the NLETS or by direct contact with state and local law enforcement officials. Intelligence Bulletins (and other law enforcement sensitive information) are disseminated to state and local law enforcement

authorities through NLETS, LEO, the Regional Information-Sharing System, and facsimile.[34]

We reviewed a sample of 15 weekly Intelligence Bulletins issued between December 2002 and March 2003. The Intelligence Bulletins vary in their relevance to the threat of international terrorism and in their specificity of guidance to law enforcement agencies. The Bulletins usually request that suspicious activities be reported to the local JTTF even if such activities are criminal or protest-oriented rather than radical Islamic fundamentalist terrorism. Of the 15 Bulletins we reviewed, 6 gave concrete and actionable guidance on terrorism and 3 provided general information or called for vigilance. Six Bulletins were not related to the high-risk presented by international terrorists. It should be noted that Intelligence Bulletins not related to international terrorism may still provide information desired by state and local law enforcement, such as the tactics of social protesters.

In our opinion, the Bulletins are a worthwhile attempt to provide general information and guidance to state and local law enforcement agencies. However, the Bulletins are somewhat "hit and miss" in terms of providing guidance on what specific actions to take or what terrorist characteristics to be aware of. The declassification of information for release through the Bulletins necessarily reduces the specificity of the information. Further, the Bulletins are not "alerts" that advise law enforcement agencies to take particular actions; instead the Bulletins are more an effort to inform and provide awareness should law enforcement personnel encounter a situation mentioned in a Bulletin. According to FBI officials, the FBI must limit the types of information that can be shared widely with the greater law enforcement community because such information frequently finds its way to the news media. As discussed in Finding 1 of this report, among the difficulties in sharing intelligence with state and local officials are, in addition to IT limitations, the following: 1) lack of appropriate security clearances by would-be recipients; 2) non-FBI originator control over intelligence, including the need to protect sensitive sources and methods of collection; 3) lack of a secure means of transmitting classified information; and 4) lack of approved secure storage capability. Additionally, FBI officials point out that there is seldom direct intelligence on a threat against a specific target, but that if such a threat were identified the state and local authorities would be notified

[34] The Regional Information-Sharing System is composed of six regional centers that share intelligence and coordinate efforts against criminal networks that operate across jurisdictional lines.

immediately regardless of whether the information was classified. However, FBI officials stress that more sensitive, classified information is available to state and local law enforcement representatives who serve with FBI agents on JTTFs and have Top Secret security clearances.

Two contrasting examples of Intelligence Bulletins appear in Appendices 5 and 6: one that, in our opinion, provides useful information to state and local law enforcement agencies on international terrorism issues and one that does not.

Quarterly Terrorist Threat Assessments[35]

The Quarterly Terrorist Threat Assessments, prepared by the Terrorist Watch and Warning Unit under the FBI's National Threat Center Section, are issued to law enforcement agencies nationwide. The purpose of the reports, which range in length from 19 to 28 pages including a 3-page Appendix, is stated in the September-December 2002 report: "a strategic overview of the current terrorist threat against the United States, a general description of civil disturbance threats and protester tactics, and a global antipathy report." We reviewed five Quarterly Terrorist Threat Assessments dated September-December 2002 (two reports), March 2003 (two reports), and April 2003 (one report) to evaluate the content and the potential of the information to state and local law enforcement agencies.

The September-December 2002 report format is a series of bullets under the following headings: Terrorism Threat (including a subheading entitled WMD), Civil Disturbance (subheadings Potential Protest Practices & Tactics, Protest Organization, Improvised Body Armor and Shields, Stink Bombs and Pyrotechnics, False Identification & Impersonation, Surveillance of Law Enforcement, Targeting of Law Enforcement, Assessment Summary), Antipathy Report (subheadings Africa, Americas, Asia, Europe & Western Asia, Middle East), and Transnational Issues. An Appendix section covers scope, dissemination restrictions, and methodology.

The reports for February-March 2003, updated March 2003, and April 2003 reports are narrative in format with the following content: Strategic Overview, Terrorist Threat (subheadings for International Terrorism,

[35] The exact title of this document varied somewhat, but the most commonly used title was the Quarterly Terrorist Threat Assessment.

Activities and Targeting, Domestic Terrorism, Activities and Targeting, Civil Disturbance, WMD, and Assessment Summary).

The Quarterly Terrorist Threat Assessments are "rolling" assessments in that much of the information is repeated from report to report with some new information added to the new quarterly report. The interim reports within a quarter are nearly identical except for any changes to the national threat level changing. Much of the information provided to state and local law enforcement agencies through the assessments could be described as general awareness, and much of the information on al-Qaeda provides a good background on the methods employed by such terrorist organizations. In some cases law enforcement is provided with information that could be actionable at the initiative of the law enforcement agency, such as looking into security at general aviation airports or perhaps asking scuba trainers or equipment providers about suspicious clients. However, the assessments do not make such direct suggestions to law enforcement agencies about specific steps that should be taken to either thwart or investigate potential terrorists or what local JTTFs might already be investigating. Further, although the reports assess the general threat, they do not provide law enforcement with an assessment of risk in terms of what scenarios may be more likely or of greater probability of occurring and what counterterrorism activities would be recommended.

The five reports we reviewed covered various topics on international terrorism (as well as domestic terrorism and protestor activities). For example, the reports discuss al-Qaeda's operational methods and capabilities and warn of terrorists' interest in using small aircraft for suicide attacks and developing scuba capability. The reports also state al-Qaeda's focus on returning to previous targets that were unsuccessfully attacked, which could signal a threat to any remaining September 11 targets such as the White House.

E-Mail Messages

The FBI periodically sends e-mail messages of one to three pages in length to other federal, state, and local law enforcement agencies using the NLETS. We reviewed a sample of 11 NLETS messages issued by the FBI's CTD between September 11, 2001, and March 21, 2003, to determine the content and evaluate the usefulness of the information to state and local law enforcement agencies. The NLETS messages varied in their relevance to the threat of international terrorism and in their specificity of guidance to law

enforcement agencies. The messages usually requested that suspicious activities be reported to the local JTTF, the nearest field office, or FBI headquarters. Of the 11 messages reviewed, 5 were "Be On The Lookout For" (BOLO) alerts for specific individuals. Of the five BOLO alerts, three were for individuals considered armed and dangerous who possibly presented a terrorist threat to the United States. Another BOLO message stated that although the FBI had no specific information connecting the named individuals to terrorism, they were being sought for questioning. The remaining BOLO canceled a previous alert. Of the remaining six NLETS messages, three concerned changes in the national threat advisory level between "significant risk of terrorist attacks" (yellow) and "high risk of terrorist attacks" (orange) and general information on why the threat level was changed. For example, a September 2002 message cited the establishment of al-Qaeda cells in Southeast Asia, the preparation of suicide bombers for attacks against U.S. interests, and the possibility of al-Qaeda operatives using the September 11 anniversary to launch attacks. The other three messages concerned a terrorist threat advisory following the events of September 11, 2001, an advisory to remain vigilant over the Fourth of July 2002 holiday, and an advisory concerning al-Qaeda's interest in targeting the nation's fuel infrastructure.

The FBI's NLETS messages offer a method of providing immediate general information to state and local law enforcement agencies. Specifically, NLETS is used to inform the law enforcement community of terrorist threats and the general factors leading to changes in the national threat advisory level as well as naming and describing individuals sought by the FBI. Because the FBI knows of a general threat but not a specific target to cite in the messages, the advisories urge a heightened alert. Guidance regarding an increase in the color-coded national threat level is general such as the need to coordinate security efforts with other law enforcement agencies and to be prepared to execute contingency procedures such as relocating to alternative sites or dispersing the workforce. In the case of BOLO messages, the FBI instructs law enforcement agencies to either detain the individual or obtain further guidance from the FBI or the local JTTF.

Terrorist Watch List

According to Unit Chief, the FBI's Terrorist Watch and Warning Unit posts the names of some 5,000 terrorists from the FBI's Terrorist Watch List on the NCIC database, which can be accessed by state and local law enforcement personnel. The Watch List information is derived from the FBI's

Violent Gang and Terrorist Organization File. If a local law enforcement agency produces a "hit" from the NCIC check, the system provides guidance how to handle the individual: detain, arrest, or notify the FBI. Of the 5,000 names on the FBI's Watch List, about half are international terrorist suspects. In April 2003 the GAO reported that federal agencies maintain 12 different watch lists.[36] One of the watch lists cited was the FBI's Violent Gang and Terrorist Organization File. The GAO recommended that the DHS lead an effort to consolidate and standardize the disparate watch lists. In the meantime, we believe that the FBI's effort to post terrorists' names on the NCIC, begun in March 2002, can help prevent local police from releasing terrorist suspects.

Conclusions

The FBI has taken a number of measures to more effectively share intelligence and other information on the terrorist threat. Communications within the FBI, and to and from the intelligence community in particular, have improved through Intelligence Information Bulletins and formal intelligence assessments. For top FBI management, the Director's Briefing provided highly-classified, specific intelligence to the extent such information is available. We have not reviewed the Daily Reports that recently replaced the Director's Briefing, but the reports appear to serve a similar purpose. Although Urgent Reports allow field offices to work around the time-consuming and unwieldy EC process, the subject of the messages varies from potential terrorist activity to much less urgent matters. Given the continuous stream of information flowing to senior FBI leadership, we believe that only the most serious and urgent matters should be brought to the immediate attention of the Director and other senior managers.

The most problematic aspect of the FBI's efforts to improve information sharing concerns state and local law enforcement. The FBI's weekly Intelligence Bulletins, Quarterly Terrorist Threat Assessments, and periodic NLETS messages are only partially effective in providing actionable information. Frequently the information being shared on terrorism could be described as background; often the subject of the FBI's communications is not the high risk of radical Islamic fundamentalist terrorism but social protests or the criminal activities of environmental or animal activists. Still,

[36] The report is entitled "Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing" (GAO-03-322, April 15, 2003).

the FBI is limited as to what intelligence and information it can provide state and local law enforcement agencies on terrorists and their activities, either because specific threats and targets are not known to the FBI or because lack of security clearances by state and local officials or other national security concerns prevent the sharing of more detailed information. We believe the FBI should continue to encourage state and local law enforcement officials to apply for security clearances and provide cleared officials with relevant terrorist threat information on a need-to-know basis either in writing if the recipient has approved storage containers or through periodic classified briefings.

Recommendations

We recommend that the Director of the FBI:

5. Issue guidance on Urgent Reports so that top FBI managers' attention focus on the most important matters of national security and public safety.

6. Focus the content of Intelligence Bulletins and Quarterly Terrorist Threat Assessments to provide – to the extent possible – actionable information on the high risk of international terrorism and any domestic terrorist activities aimed at creating mass casualties or destroying critical infrastructure, rather than information on social protests and domestic radicals' criminal activities.

STATEMENT ON MANAGEMENT CONTROLS

In planning and performing our audit, we considered the FBI's management controls for the purpose of determining our auditing procedures. This evaluation was not made for the purpose of providing assurance on the FBI's management controls as a whole. We noted, however, certain matters that we consider to be reportable conditions under Government Auditing Standards.

Reportable conditions involve matters coming to our attention relating to significant deficiencies in the design or operation of management controls that, in our judgment, could adversely affect the FBI's ability to effectively manage the program. As discussed in the Findings and Recommendations sections of this report, we found that: 1) there were no written policies and procedures to guide the flow and dissemination of information relating to the FBI's counterterrorism efforts, and 2) efforts to communicate with state and local law enforcement agencies too often did not focus on the higher risk of radical Islamic fundamentalist terrorism and the potential for mass-casualty attacks.

Because we are not expressing an opinion of the FBI's management controls as a whole, this statement is intended solely for the information and use of the FBI in managing the program.

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS

We have audited the FBI's intelligence and information-sharing efforts related to counterterrorism. The audit generally covered the period September 2001 through April 2003, and included a review of the FBI's identification of impediments to intelligence and information sharing, actions taken to improve intelligence and information sharing, and dissemination methods. The audit was conducted in accordance with Government Auditing Standards.

In connection with the audit and as required by the standards, we reviewed procedures, activities, and records to obtain reasonable assurance about the FBI's compliance with laws and regulations that, if not complied with, we believe could have a material effect on the program operations. Compliance with laws and regulations applicable to the program is the responsibility of the program's management.

Our audit included examining, on a limited test basis, evidence about laws and regulations. The specific laws for which we conducted tests are contained in:

- Title 28, United States Code, Section 533;
- National Security Directive 207;
- Presidential Decision Directive 39; and
- Presidential Decision Directive 62.

The FBI complied with the laws and regulations cited above. With respect to those transactions not tested, nothing came to our attention that caused us to believe that the FBI was not in compliance with the referenced laws.

Appendix 1

OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

The primary objectives of the audit were to determine the extent to which the FBI: 1) identified impediments to the sharing of counterterrorism-related intelligence and other information, 2) has improved its ability to share intelligence and other information both within the FBI and to the intelligence community and state and local law enforcement agencies, and 3) is providing useful threat and intelligence information to other law enforcement agencies.

Scope and Methodology

The audit was performed in accordance with Government Auditing Standards, and included tests and procedures necessary to accomplish the audit objectives. Generally our audit focused on the FBI's efforts to improve the dissemination of intelligence and other information from September 2001 through September 2003.

In conducting this audit, OIG staff interviewed or received briefings from the Executive Assistant Director for Intelligence, the current and former Assistant Director of the FBI's Office of Intelligence, and senior managers in the Counterterrorism Division, including the Assistant Director at the time, the three Deputy Assistant Directors, eight Section Chiefs, and four Unit Chiefs. OIG staff interviewed or obtained briefings from FBI managers responsible for information technology improvements, the monitoring of re-engineering projects, and coordination with state and local law enforcement agencies. In addition, we analyzed samples of formal FBI intelligence and other information products disseminated to the intelligence community and to state and local law enforcement agencies. We also obtained and reviewed FBI documents on the flow of intelligence, staffing of intelligence analysts, re-engineering projects, state and local law enforcement coordination, IT improvements, and other efforts designed to improve information sharing. OIG staff also interviewed representatives of the Central Intelligence Agency who were detailed to the FBI as managers in the Counterterrorism Division. In addition, we reviewed congressional testimony and the reports of counterterrorism commissions dealing in part with intelligence and information sharing.

To avoid duplicating other ongoing audit work, we restricted our audit scope to information and personnel available at FBI headquarters. Consequently, we did not perform audit work at, or interview officials of, intelligence agencies, state and local law enforcement agencies, JTTFs, FBI field offices, or others. However, we did interview selected intelligence agency officials assigned to FBI headquarters.

Appendix 2

ABBREVIATIONS

ACS	Automated Case File System
BOLO	Be On The Lookout For
CIA	Central Intelligence Agency
CONUS	Continental United States
[CLASSIFIED INFORMATION REDACTED]	
CTC	CIA Counterterrorist Center
CTD	Counterterrorism Division
DCI	Director of Central Intelligence
DCID	Director of Central Intelligence Directive
DHS	Department of Homeland Security
DOD	Department of Defense
DOJ	Department of Justice
DTOS	Domestic Terrorism Operations Section
EC	Electronic Communication
FISA	Foreign Intelligence Surveillance Act
GAO	General Accounting Office
GS	General Schedule
IIR	Intelligence Information Reports
INS	Immigration and Naturalization Service

IT	Information Technology
ITOS	International Terrorism Operations Section
JTTF	Joint Terrorism Task Force
JWICS	Joint Worldwide Intelligence Communications System
LAN	Local Area Network
LEO	Law Enforcement Online
NCIC	National Crime Information Center
NJTTF	National Joint Terrorism Task Force
NLETS	National Law Enforcement Telecommunications System
NSA	National Security Agency
NTCS	National Threat Center Section
OCONUS	Outside Continental United States
OIG	Office of the Inspector General
OLEC	Office of Law Enforcement Coordination
OI	Office of Intelligence
ORCON	Originator Controlled
PDD	Presidential Decision Directive
PENTTBOM	Pentagon/Trade Towers Bombing Investigations
SCI	Sensitive Compartmented Information

SCOPE	Secure Counterterrorism Operational Prototype Environment
SIOC	Strategic Information and Operations Center

[CLASSIFIED INFORMATION REDACTED]

SVTS	Secure Video Teleconferencing System
TFOS	Terrorist Financing Operations Section
TRRS	Terrorism Reports and Requirements Section
TS/SCI LAN	Top Secret/Sensitive Compartmented Information Local Area Network
TTIC	Terrorist Threat Integration Center
WMD	Weapons of Mass Destruction

Appendix 3

Counterterrorism Division Status of Personnel as of 3/19/03

Types of Positions	Intelligence Assistants	Budget Analysts	Supv. Mgmt. & Budget Analyst	Intelligence Operations Specialists	Supervisory Intelligence Operations Specialists	Evidence Technician	Presidential Support Assistant	Security Specialist	Management Assistant	Financial Analyst	Mgmt. & Program Analyst	Total
Goal												
On Board												
Need to Hire												
In Background	CLASSIFIED INFORMATION REDACTED											

Types of Positions	Supervisory Management & Program Analyst	Special Assistant	IT Specialist	Visual Information Specialist	Editor, Designer, Production Specialist	Intelligence Research Specialist	Supervisory Intelligence Research Specialist	Secretary	Technical Information Specialist	Supply Technician	Computer Scientist	Total
Goal												
On Board												
Need to Hire												
In Background	CLASSIFIED INFORMATION REDACTED											

Types of Positions	Program Analysts	Section Chief	Assistant Section Chief	Total
Goal				
On Board				
Need to Hire				
In Background	CLASSIFIED INFORMATION REDACTED			

Source: CTD Administrative and Resources Unit Chief

CTD Program Resources

CT Field Program	Agent Positions	Support Positions	Total Positions
Fiscal Year 2002 Actuals	CLASSIFIED INFORMATION REDACTED		
Fiscal Year 2003 Funded			
FY 2003 Base			
FY 2003 Program Increase			
Reports Officers			
Subtotal: FY 2003 Program Increase			
Total: FY 2003 Funded			
Fiscal Year 2004 Request to Congress			
FY 2004 Base			
FY 2004 Program Increase			
Agents			
Investigative Support			
Technical Support			
Clerical Support			
Intelligence Research Specialists			
Subtotal: FY 2004 Program Increase			
Total: FY 2004 Request to Congress			
CT Headquarters Program	**Agent Positions**	**Support Positions**	**Total Positions**
Fiscal Year 2002 Actuals	CLASSIFIED INFORMATION REDACTED		
Fiscal Year 2003 Funded			
FY 2003 Base			
FY 2003 Program Increase			
Agents			
Reports Officers			
Subtotal: FY 2003 Program Increase			
Total: FY 2003 Funded			
Fiscal Year 2004 Request to Congress			
FY 2004 Base			
FY 2004 Request to Congress			
Intelligence Operations Specialists			
Reports Officers			
Intelligence Analysis Assistant PM			
Special Assistants			
Computer Scientists			
Attorneys			
Information Technology Advisors			
Management & Program Analysts			
Editors			
Visual Information Specialists			
Technical Information Specialists			
Personnel Management Specialists			
Training Specialists			
Financial Analysts			
Program Analysts			
Secretaries			
Administrative Assistants			
Evidence Technicians			
Intelligence Assistants			
Management Assistants			
Supply Technicians			
IOS (Internet Tips)			
Subtotal: FY 2004 Program Increase			
Total: FY 2004 Request to Congress			

Source: CTD Administration and Resources Unit Chief

Department of Justice

FOR IMMEDIATE RELEASE **AG**
WEDNESDAY , OCTOBER 9, 2002 **(202) 616-2777**
WWW.USDOJ.GOV **TDD (202) 514-1888**

ATTORNEY GENERAL JOHN ASHCROFT UNVEILS GATEWAY INFORMATION-SHARING PILOT PROJECT IN ST. LOUIS, MISSOURI

WASHINGTON, D.C. - Attorney General John Ashcroft today unveiled the Gateway Information-Sharing Project (ISI), a pilot program that integrates investigative data from federal, state and local law enforcement agencies into one database that will ultimately be accessible to all participating agencies via secure Internet. This program is the result of cooperation between the Illinois State Police, St. Louis Metropolitan Police Department, St. Louis County Police Department, Missouri State Highway Patrol, St. Clair County Sheriff's Office, Collinsville, Illinois Police Department, Southern Illinois Police Chiefs Association, St. Louis Area Police Chiefs Association, Federal Bureau of Investigation, and the United States Attorneys' Offices of the Southern District of Illinois and Eastern District of Missouri. St. Louis Joint Terrorism Task Force.

"Today, at a time when our nation is fully engaged in a war on terrorism, information has never been more important," Attorney General Ashcroft said. "It is the key to prevention - not just of terrorism, but also of crime. This Information-Sharing Initiative will be a vital tool to the federal, state, and local law enforcement officers who dedicate their lives to keeping our communities and our nation safe."

The St. Louis Intelligence Center began in 1999 when the U.S. Attorneys for Eastern Missouri and Southern Illinois, together with federal, state and local law enforcement, created a joint intelligence center to explore the possibility of a shared data warehouse, designed to combat drug trafficking and violent crime. Over the past year, these projects have merged into the Gateway ISI. In April, the FBI initiated

the first phase of the pilot project in St. Louis, and launched pilot projects in San Diego, Seattle/Portland, Norfolk, and Baltimore.

The Gateway ISI marks the first time that the FBI has entered records in a data warehouse containing investigative data from local and state law enforcement agencies. The first phase included records from the St. Louis FBI field office, the St. Louis Metropolitan Police Department, and the Illinois State Police. The project is managed by an Executive Board consisting of federal, state and local law enforcement executives from participating agencies in Southern Illinois and Eastern Missouri districts, along with United States Attorneys Miriam Miquelon and Raymond Gruender.

"The Gateway ISI makes `real time' law enforcement a reality," said Miriam Miquelon, United States Attorney for the Southern District of Illinois. "By allowing law enforcement agencies to share information, this technology enables officers to make swift threat assessments and expedite apprehension of criminals."

The Gateway ISI merges investigative files and records from all levels of law enforcement into a single, searchable data warehouse. It provides investigators and analysts the ability to search the actual text of investigative records for names, addresses, phone numbers, scars, marks, tattoos, weapons, vehicles, and phrases. It also graphically depicts the relationships between these factors. Each agency that enters data into the warehouse will be able to access it through four levels of security access.

"Information that was previously fragmented and would take analysts months to collate will be connected within seconds," said Ashcroft. "This revolutionary system will enable investigators to identify intelligence gaps, and to see tangible links between seemingly unrelated investigations."

Though still a pilot project, the Executive Board expects the St. Louis Gateway ISI to be fully operational within 60 days. If successful, the project could serve as a model for a nationwide information- sharing initiative.

"We are very proud that the Gateway Information-Sharing Initiative may become the model for a national program of information-sharing between federal, state and local law enforcement," said Ray Gruender, the United States Attorney for the Eastern District of Missouri. "We

hope this project will continue to develop and become a powerful tool not only in our efforts to prevent and disrupt terrorism but also in our efforts to fight drug crime, violent crime and fraud throughout the nation."

02-589

Appendix 5

LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED

LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED

LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED

Source: CTD Executive Staff

Appendix 6

LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED

LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED

Source: CTD Executive Staff

Appendix 7

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

December 10, 2003

The Honorable Glenn A. Fine
Inspector General
Office of the Inspector General
United States Department of Justice
Room 4322
950 Pennsylvania Avenue, Northwest
Washington, D.C. 20530

Dear Mr. Fine:

I would like to thank you for providing the Federal Bureau of Investigation (FBI) the opportunity to respond to your report entitled, "The FBI's Efforts to Improve the Sharing of Intelligence and Other Information."

I recognize the substantial challenge the Office of the Inspector General (OIG) has in producing timely reports on complex issues such as this. The audit process, by its nature, is slow and often results in findings and recommendations that no longer reflect the realities of today. This challenge is even more difficult when assessing FBI operations because of the rapid changes it continues to undergo to optimally position itself to address the evolving threats to our Nation.

The FBI is grateful to the OIG team that produced this report for agreeing to assess additional information after they had completed their initial audit. As a result, this report was able to document some of the tremendous progress the FBI has made in its national intelligence program. Ideally, we would like for the report to again be updated to provide a status of intelligence and information sharing efforts in the FBI. However, I realize that there must be a closing point to these audits. That said, I believe the report would provide a more complete picture if it included the following:

- Field Intelligence Groups have been established in all 56 FBI field offices with personnel dedicated full time to the intelligence process including the sharing of intelligence and other information;

- a multi agency Terrorism Screening Center has been established and is now operational;

Mr. Glenn A. Fine

- a nation-wide alert system using text messaging technology to alert senior law enforcement leaders of new terrorism-related information has been established and is operational;
- performance metrics have been established to assess the sharing of information bureau-wide;
- a detailed blueprint of the FBI's intelligence and other information sharing process has been completed;
- executive boards for each of the 84 Joint Terrorism Task Forces have been established to institutionalize the exchange of counterterrorism-related intelligence at the executive level on a regular basis;
- a teleconferencing capability is being used by several SACs to provide periodic unclassified briefings and updates to local, state and federal law enforcement agencies;
- an FBI presence on Intellink has been established and the FBI is posting its intelligence reports and analytical products up to the TS/SCI level, providing intelligence community-wide access;
- an FBI presence on SIPERNET has been established and the FBI is posting its intelligence reports and analytical products up to the Secret level, providing federal agency-wide access;
- an FBI web page on Law Enforcement Online (LEO) is in the final stages of being completed and the FBI will post sensitive but unclassified reporting and intelligence products that will be accessible to local, state, tribal and federal law enforcement personnel;
- LEO has been connected to the nation-wide Regional Information Sharing System Network (RISSNET) which substantially expands local and state law enforcement access to FBI reporting and intelligence products;
- FBI analysts have been provided comprehensive training since 9/11/2001 which has included specific training on the sharing of intelligence and other information;
- an automated intelligence collection capabilities baseline assessment has been developed;

Mr. Glenn A. Fine

- The Global Intelligence Working Group, which is led by local law enforcement, serves as the advisory board to provide expert advice on the FBI's efforts to share intelligence and other information.

- a daily intelligence production board has been established to manage FBI-wide production of intelligence;

- a standard template and process has been established to integrate into the FBI's Intelligence collection and production process the Intelligence Information needs of local, state and tribal law enforcement agencies throughout the U.S.

- SES managers at FBIHQ and all Assistant Special Agents-in-Charge have received detailed briefings and training on the Intelligence Program including the sharing of Intelligence.

I want to thank you again for your efforts in producing this report, and we welcome the opportunity to discuss in detail the progress the FBI continues to make in this area.

As you requested, the report's recommendations were provided to appropriate representatives of the Counterterrorism (CT) and Criminal Investigative Divisions as well as the Office of Intelligence. Their comments are set forth below.

Recommendation #1

OIG Recommendation: Using the Concepts of Operations (CONOPs) as a framework, establish a written policy on - and procedures for - information sharing, including what types of information should be shared with what parties under what circumstances.

FBI Response: The FBI agrees with this recommendation and has already drafted written policy and is currently drafting procedures for information sharing using the Intelligence CONOPs as a framework. The FBI expects the written policy to be issued in January 2004 and written procedures implementing the policy to be issued in March 2004.

Recommendation #2

OIG Recommendation: Ensure that the FBI-wide enterprise architecture currently under development is accompanied by a process map for information sharing that clearly defines the current state and an end for the information-sharing process so that the numerous information sharing initiatives can be coordinated and properly monitored and managed.

Mr. Glenn A. Fine

FBI Response: The FBI has already completed a detailed blueprint and process map on its intelligence and information sharing process.

Recommendation #3:

OIG Recommendation: Consider transferring responsibility for investigating crimes committed by environmental, animal rights, and other domestic radical groups or individuals from the CT Division to the Criminal Division, except where a domestic group or individual uses or seeks to use explosives or weapons of mass destruction to cause mass casualties.

FBI Response: The FBI has given this recommendation considerable thought and has come to the conclusion that transferring the noted responsibilities would have a detrimental effect by diluting the intelligence base directed to both domestic and international terrorism matters.

Title 18, U.S.C. 2331(5) defines Domestic Terrorism as activities that -

(A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State;

(B) appear to be intended --

(i) to intimidate or coerce a civilian population;

(ii) to influence the policy of a government by intimidation or coercion; or

(iii) to affect the conduct of a government by mass destruction, assassination, or kidnaping; and

(C) occur primarily within the territorial jurisdiction of the United States.

The goals of "social activists" are to effect social and/or political change through their constitutionally protected rights. When these "social activists" turn to the use (or threatened use) of force or violence, they become domestic terrorists. The goals of these criminals fall directly in line with the definition of a terrorist group as defined by federal law.

Domestic terrorists have caused considerable damage to the U.S. economy through their criminal acts. Terrorist groups, whether international or domestic, often use similar methods and patterns regarding operational and communication security, fund raising, money transfers and other recruitment and support statements. It is important to maintain responsibility for investigating domestic terrorists within the FBI's CT Division

where there is a broad experience base to counter their criminal activities.

The FBI addresses all terrorism related matters, both international and domestic, through a threat based approach, establishing intelligence collection, analysis and dissemination measures with an integrated operational response. Examples of such are CT Watch, the Joint Terrorism Task Forces (JTTF), the Fly Team and the Document Exploitation Unit.

A significant initiative of the CT Division is the creation and establishment of the JTTFs across the country as a primary means of addressing all terrorism threats and a mechanism to expand and enhance intelligence and information sharing among agencies. The FBI does not agree with the transfer of Domestic Terrorism out of the CT Program, which is an intrinsic part of CT on-going field operations. The FBI serves as the lead agency in all JTTFs. The JTTF Program is an integral part of each of the FBI's 56-field offices, which includes agent and analytical support. These individuals not only support the JTTF's but also all CT investigations within the field office. The JTTF program integrates tactical and investigative resources and expertise for critical incidents, which necessitates an immediate response from law enforcement authorities. To transfer the Domestic Terrorism portion of the CT field operation to the Criminal Division would diminish the FBI's efficiency by causing a duplication of effort between the CT Division and the Criminal Division, where the CT Division already has the support structure established. Within the field office, the JTTF's provide the ability to combine the expertise of state and local law enforcement and other federal government entities. This concept provides the CT Program with a surge capability providing an influx of expertise, operational guidance, and actionable intelligence in the furtherance of FBI's Domestic and International Terrorism Program objectives.

The JTTF concept has proven to be the most successful way to address terrorism intelligence operations and criminal investigations, when warranted, through an interagency approach involving the law enforcement and public safety community. In the past several years the CT Division's efforts in developing these task forces has broadened the interagency liaison and communications, eliminated any duplication of effort, and combined federal, state, and local law enforcement resources in the fight against terrorism. Information sharing is an intrinsic element that has enabled the FBI, nationwide law enforcement and the federal government to share information.

Recommendation #4:

Mr. Glenn A. Fine

OIG Recommendation: For each CONOPs develop an implementation plan that includes a budget along with a time schedule detailing each step and identifying the responsible FBI official.

FBI Response: The FBI has developed an implementation plan for each relevant Intelligence Concept of Operations. The plans include a time schedule and the identities of each responsible official. To this end, the Office of Intelligence has assigned a senior detailee from the Intelligence Community to act as a Special Advisor for implementation to the Executive Assistant Director for Intelligence. The implementation steps are being tracked by a team that is dedicated to this purpose, to assist FBI managers who are responsible for implementation.

One of the CONOPs we developed addresses the budget process for building an enterprise-wide intelligence program. The CONOPs takes all actions and capabilities outlined in the individual CONOPs and costs them. We will complete this CONOPs by early January. Once we have done so, we will add a budget section to each individual CONOPs.

Recommendation #5:

OIG Recommendation: Issue guidance on Urgent Reports so that top FBI managers' attention focuses on the most important matters of national security and public safety.

FBI Response: Executive Assistant Director Wilson Lowery directed the Records Management Division (RMD) to conduct an analysis of the Urgent Reports System. RMD assembled a review team that examined the content, format, delivery method, dissemination, timeliness and record-keeping aspects of Urgent Reports and identified six recommendations for improvements. The team's report and recommendations are currently under review and are awaiting approval.

Recommendation #6:

OIG Recommendation: Focus the content of Intelligence Bulletins and Quarterly Terrorist Threat Assessments to provide - to the extent possible - actionable information on the high risk of international terrorism and any domestic terrorist activities aimed at creating mass casualties or destroying critical infrastructure, rather than information on social protests and domestic radicals' criminal activities.

FBI Response: The FBI has thoroughly reviewed this recommendation and has concluded that if adopted it would actually impede the sharing of relevant information with our

local and state partners. The intent of the Intelligence Bulletin is to reach a wide-ranging law enforcement audience.

In the aftermath of the terrorist attacks of September 11, 2001, federal cooperation with state and local law enforcement became a paramount objective for the prevention of future terrorist incidents. The Intelligence Bulletin provides the most current and relevant terrorist-related intelligence information to a broad spectrum of users, totaling more than 18,000 recipients nationwide. Areas of focus include international and domestic terrorism, and weapons of mass destruction (including chemical, biological, radiological, and nuclear weapons). Select Bulletins also provide actionable guidance in advance of large-scale protests or international events (e.g., World Trade Organization, International Monetary Fund, UN General Assembly) where the potential for criminal activity exists. These events offer an attractive stage for individuals, extremist groups, and even terrorist groups to exploit an otherwise peaceful gathering to advance their own agenda through violent means. To date, 139 items have been published in 91 Bulletins. The chart on the following page provides a breakdown of past Bulletin items:

Intelligence Bulletin Areas of Focus	**# of Items**
International Terrorism	77
Domestic Terrorism	19
Weapons of Mass Destruction/ Threats to Critical Infrastructure	18
Large-Scale Protests and International Events	15
Criminal Activity with Potential for Terrorist Exploitation	5
Homeland Security Advisory System Threat-Level Adjustment	5
Total	139

Quarterly Threat Assessment

Whereas the local JTTFs provide actionable information to law enforcement on a daily basis for operational purposes, the

Mr. Glenn A. Fine

Quarterly Threat Assessment is a strategic document intended for coordination and planning. The Quarterly Threat Assessment covers four threat categories: international terrorism, domestic terrorism, weapons of mass destruction, and civil disturbance. The assessment gives greatest emphasis to international terrorism.

In addition to your request for comments on the report's recommendations, you also requested the FBI provide a sensitivity and classification review for the information contained in the report. The results of these reviews are included as enclosures with this letter.

Please contact me or Deputy Assistant Director Kevin Perkins should you have any questions regarding this matter.

Sincerely yours,

S C McCraw

Steven C. McCraw
Assistant Director
Inspection Division

8

Appendix 8

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

We provided the draft audit report to the FBI for review and comment. The response from the FBI is incorporated as Appendix 7 of this final report. Our analysis of the FBI's response to specific recommendations is provided below. In addition to responding to the recommendations, the FBI provided additional comments and listed improvements it says it has made since the completion of the audit.

At the FBI's request we analyzed and incorporated into the audit report significant developments in the FBI's intelligence sharing program that occurred subsequent to the completion of a draft of this report. After our audit fieldwork was completed, we met with FBI intelligence officials at their request in September 2003 and provided them an opportunity to raise any additional changes that the FBI was making in its intelligence sharing capabilities. We subsequently incorporated the changes they identified in the final report.

The FBI's response states that the audit process by its nature is slow and implies that this report's findings and recommendations no longer reflect "realities". In addition, the FBI cited in its response 17 additional items which it said should be included in the report to make it more complete. However, none of these were cited to us by the FBI in the comments made in September 2003 on an earlier draft of this report. Moreover, while we agree that the FBI is making positive changes in the intelligence sharing process, we disagree with both the general comment about the audit process and the implication about the findings and recommendations of this report. We recognized that the FBI has made and will continue to make changes in its information-sharing process; however, the fact that the FBI's intelligence program is evolving is made clear in the audit report and does not detract from the accuracy and relevance of our findings.

With regard to the 17 additional items cited by the FBI, many are already discussed in the report, others are still in the planning or development stages, and others are not recent initiatives. For example, the FBI cites the establishment of Field Intelligence Groups in all 56 field offices. However, the report discusses the FBI's

intelligence capabilities and staffing on a number of pages, including 18, 29-31, and 46. Completing the establishment of intelligence groups may be a recent development.

The FBI cites the establishment of a presence on "Intellink" and "SIPERNET". Assuming these references are meant to be to "Intelink" and "SIPRNET," they do not appear to be recent developments. On June 10, 1998, Michael A. Vatis, Deputy Assistant Director and Chief of the FBI's National Infrastructure Protection Center, testified before the Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information that:

> We are currently in the process of designing an information architecture that will serve our mission needs. This will consist of analytical tools; computer resources; and connectivity to other federal government agencies, State and local governments, and private sector incident response teams and companies. In the meantime, we are relying on existing communications capabilities including: INTELink for access to intelligence information; SIPRNet and ADNet for communication with the Department of Defense; the National Law Enforcement Telecommunications System (NLETS) and Law Enforcement On-Line (LEO) to communicate with State and local law enforcement; the Awareness of National Security Issues and Response (ANSIR) program for communicating with industry; and FBInet for communication within the FBI.

Further, we mention SIPRNET on pages 38 and 40 of the report and Intelink on page 54.

The FBI cites completion of a web page on Law Enforcement Online (LEO) as an important step in sharing sensitive information. However, the LEO system itself is not a recent initiative. The FBI's August 2000 Law Enforcement Bulletin stated that:

> Every day across the country, law enforcement, criminal justice, and public safety professionals are "signing on" to Law Enforcement Online (LEO), a secure Intranet communication system built and maintained

> by the FBI, to share sensitive information. They rely on LEO as their primary tool to communicate or obtain mission critical information, to provide or participate in online educational programs, and to participate in professional special interest or topically focused dialog.

We mention LEO on pages 44 and 59 of the report. The FBI also cites the connection of LEO to the Regional Information Sharing System Network (RISSNET). RISSNET is mentioned on page 59 of the report.

The FBI cites that training has been provided for analysts since September 11, 2001. The report on pages v, 19, 31, 37, 49 and 50 discusses the FBI's ongoing efforts to develop an analyst training program.

The FBI cites the multi-agency Terrorist Screening Center, administered by the FBI, which is described as being operational. Although the establishment of the Terrorist Screening Center was announced in September 2003 and began operations on December 1, 2003, the FBI has stated that the initial capabilities of the Center will be limited. We have added a notation on the Terrorist Screening Center to the report.

The FBI cites the Global Intelligence Working Group as its advisory board on intelligence sharing. However, the internet homepage for the this group describes it as an initiative not of the FBI but of the Office of Justice Programs:

> The IACP [International Association of Chiefs of Police] Criminal Intelligence Sharing Report contained a proposal to create a National Criminal Intelligence Sharing Plan ("Plan"). The most central and enduring element of the Plan advocated by Summit participants was the recommendation for the creation of a Criminal Intelligence Coordinating Council comprised of local, state, tribal, and federal law enforcement executives. The Council's mandate would be to establish, promote, and ensure effective intelligence sharing and to address and solve, in an ongoing fashion, the problems that inhibit it. In fall 2002, in response to this proposal, the U.S. Department of Justice, Office of Justice Programs (OJP), Bureau of Justice Assistance (BJA), authorized the formation of the **Global Intelligence Working Group (GIWG)**, one of several

issues-focused working groups of the Global Advisory Committee (GAC). [Emphasis added.]

In sum, many of the FBI's stated improvement efforts are either discussed in the report or have been underway for years and have not yet come to fruition. As stated above, we anticipate that the FBI will continue to make progress in these areas.

Recommendation Number:

1. **Resolved.** This recommendation is resolved based on the FBI's plan to establish written policy and procedures for information sharing using the Concepts of Operations as a framework. This recommendation can be closed when we receive and review the policy and procedures for information sharing, including what types of information should be shared with what parties under what circumstances.

2. **Resolved.** This recommendation is resolved based on the FBI's statement that it has developed an information-sharing process map to accompany the FBI's enterprise-wide architecture, currently under development. This recommendation can be closed when we receive and review a copy of the FBI-wide enterprise architecture and process map for information sharing that clearly defines the current and end states for the information-sharing process so that the numerous information-sharing initiatives can be coordinated and properly monitored and managed.

3. **Closed.** This recommendation is closed based on the FBI's statement that it has given the recommendation considerable thought but concludes that transferring some of the investigations currently handled as domestic terrorism would dilute the intelligence base directed to both domestic and international terrorism matters. In its response, the FBI states that international and domestic terrorist groups often use similar methods and that the Counterterrorism Division is best suited to counter the criminal activities of domestic groups that fall under the definition of domestic terrorism. The FBI response also details the operations of the Joint Terrorism Task Forces and states its concerns that the efficiencies offered by the task forces would be diminished if the Criminal Division were to

assume responsibility for cases classified as domestic terrorism. Although we are closing this recommendation, we continue to believe that the FBI should continue to assess whether there may be substantive advantages to transferring responsibility for the investigation of certain crimes committed by domestic groups or individuals to the Criminal Division thereby allowing the Counterterrorism Division and the Joint Terrorism Task Forces to concentrate on the greater threat to national security of international terrorism and the use of weapons of mass destruction. We believe that the FBI's priority mission to prevent high-consequence terrorist acts would be enhanced if the Counterterrorism Division did not have to spend time and resources on lower-threat activities by social protestors or on crimes committed by environmental, animal rights, and other domestic radical groups or individuals (unless explosives or weapons of mass destruction are involved).

4. **Resolved.** This recommendation is resolved based on the FBI's development of implementation plans for each relevant Intelligence Concept of Operations Plan, including a time schedule and the designation of the responsible official, and the FBI's plan to add a budget section to each Concept of Operations Plan. However, the FBI's response does not include a time schedule for completing the planned action, and such a schedule should be included in the FBI's next corrective action response. This recommendation can be closed when we receive and review documentation of the implementation plans that include budgets, time schedules, and designation of the responsible official.

5. **Resolved.** This recommendation is resolved based on the FBI's action to complete an analysis of problems related to the Urgent Reports and to identify and recommend changes to improve the process. The FBI's response notes that the analysis and recommendations are currently under review, but does not include a time schedule for completing the action. Such a schedule should be included in the FBI's next corrective action response. This recommendation can be closed when we receive and review documentation of the changes made in the Urgent Reports process to focus top management's attention on the most important matters of national security and public safety.

6. **Closed.** This recommendation is closed. The FBI stated that it thoroughly reviewed the recommendation and concluded that if adopted the recommendation would impede the sharing of information with its state and local partners. In its response, the FBI states that Intelligence Bulletins reach a broad spectrum of users and that actionable intelligence should be conveyed through Joint Terrorism Task Forces. We agree that actionable intelligence can and should be shared with state and local law enforcement agencies through Joint Terrorism Task Forces, but the FBI has also provided actionable information and terrorism awareness topics through its Intelligence Bulletins, and we believe it should continue to do so. Further, we believe that a more general or routine law enforcement advisory is the better means of disseminating general public safety and crime-related information so that those involved in preventing or responding to acts of terrorism can concentrate their attention and efforts on high-consequence matters. However, in light of the FBI's substantive disagreement with this recommendation, and because the FBI appears to have carefully considered our recommendation, we are closing this recommendation. But we continue to recommend that the FBI consider focusing, to the extent possible, the content of Intelligence Bulletins and Quarterly Terrorist Threat Assessments on actionable international terrorism and any domestic terrorist activities aimed at creating mass casualties or destroying critical infrastructure.