A Report by a Panel of the
NATIONAL ACADEMY OF PUBLIC ADMINISTRATION for the U.S. Congress and the Federal Bureau of Investigation

TRANSFORMING *the* FBI
Progress and Challenges

January 2005

NATIONAL ACADEMY OF
PUBLIC ADMINISTRATION

A Report by a Panel of the

NATIONAL ACADEMY OF
PUBLIC ADMINISTRATION

for the U.S. Congress and the Federal Bureau of Investigation

January 2005

TRANSFORMING THE FBI:

Progress and Challenges

Panel
Dick Thornburgh, *Chair**
Robert M. Alloway*
Frank J. Chellino
Martin C. Faga*
Kristine M. Marcy*
Robert J. O'Neill, Jr.*

* *Academy Fellow*

Officers of the Academy

Project Staff

J. William Gadsby, *Vice President, Academy Studies*
Arnold E. Donahue, *Project Director*
Edward L. Federico, Jr., *Senior Project Advisor* and *Interim Project Director*
Edward Springer, *Senior Project Advisor*
Jonathan C. Tucker, *Senior Research Analyst*
Martha S. Ditmeyer, *Senior Program Associate*

The views expressed in this report are those of the Panel. They do not necessarily reflect the views of the Academy as an institution.

National Academy of Public Administration
1100 New York Avenue, N.W.
Suite 1090 East
Washington, DC 20005
www.napawash.org

First published in January 2005.

Printed in the United States of America.

ISBN 1-57744-113-3

Academy Project Number: 2032-000.

Contract No. JFBI04027.

FOREWORD

The terrorist attacks of September 11, 2001 fundamentally altered the priorities of the Federal Bureau of Investigation. Since that time, the FBI has worked to transform itself from a traditional law enforcement agency, focused primarily on investigating crimes after the fact, to a key agency in the nation's counterterrorism effort, focused primarily on preventing terrorist acts. Director Robert Mueller moved first to reorganize FBI headquarters to address the immediate demands of the new priorities, and then sought to institutionalize those priorities organization-wide through new hiring, training and management.

More broadly, the FBI has worked to build its intelligence capabilities to support its counterterrorism and counterintelligence programs, as well as its traditional law enforcement programs. These efforts have entailed a large-scale campaign to hire, train and reorient the management of intelligence analysts and related support staff.

The FBI also has mounted an ambitious initiative to improve its security program in response to the findings and recommendations of the Commission for the Review of FBI Security Programs (Webster Commission) and the RAND study, *Reinforcing Security at the FBI*, which sought to improve security in the wake of Robert Hanssen's treason and reassess the task of security post-9/11.

The National Academy of Public Administration appreciates the opportunity to play a role in this historic transformation, and looks forward to participating in the FBI's continuing efforts to enhance its capabilities as the leading domestic intelligence agency.

C. Morgan Kinghorn
President

TABLE OF CONTENTS

APPENDICIES

FIGURES AND TABLES

ACRONYMS

BICS	Background Investigation Contract Service
CXS	Communications Exploitation Section
DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
FinCEN	Financial Crimes Enforcement Network
FISA	Foreign Intelligence Surveillance Act
ICE	Immigration and Customs Enforcement (part of DHS)
ITOS	International Terrorism Operations Section
OI	Office of Intelligence (FBI)
SCIF	Sensitive Compartmented Information Facilities
TFOS	Terrorist Financing Operations Section
TRRS	Terrorism Reports and Requirements Section
WMD/DT	Weapons of Mass Destruction / Domestic Terrorism

EXECUTIVE SUMMARY

In the more than two years since it began its work, the National Academy of Public Administration's (Academy) Panel on FBI Reorganization has examined the FBI's transformation, including its divisional reorganizations and major process, personnel, and cultural changes. In 2002, the Academy Panel endorsed the thrust of Director Mueller's priorities and reorganization and made specific recommendations designed to improve the prospects for success. The Panel continued monitoring implementation of the FBI's new strategic priorities and its reorganization plan during the following year, offering in June 2003, recommendations to speed implementation and improve the likelihood for success.

Chapter One of this report provides an overview of the FBI's transformation, external reviews and recommendations for change, and this Panel's overarching findings, conclusions and recommendations concerning FBI transformation and the war on terrorism. Recommendations in three principal areas are:

- **Domestic Intelligence:** This Panel, like the 9/11 Commission, is convinced that the FBI is making substantial progress in transforming itself into a strong domestic intelligence entity, and has the will and many of the competencies required to accomplish it. **The Panel recommends that FBI continue to be the key domestic intelligence agency responsible for such national security concerns as terrorism, counterintelligence, cyber, and transnational criminal activity.**

- **Joint Operations:** Joint operations, whether managed by the FBI or other federal, state, and local authorities, are becoming the norm, and this trend is likely to continue. **The Panel recommends that the concept of joint operations, whether through joint task forces or other similar approaches, be applied more broadly to other critical law enforcement activities.**

- **Information Sharing:** Although 9/11 has served as a powerful and at least temporary antidote to excessive information controls, information sharing remains largely ad hoc and is not adequately recognized in law or fully regularized in process. Strong executive branch leadership, and possibly statutory guidance, may be required to institutionalize information sharing. **The Panel endorses the 9/11 Commission's recommendation that "the President should lead a government-wide effort to bring the major national security institutions into the information revolution and coordinate the resolution of legal, policy, and technical issues across agencies to create a 'trusted information network'." The Panel further recommends that the FBI component of this trusted network should be implemented as soon as possible and be extended to state and local law enforcement agencies with respect to counterterrorism information.**

Chapter One also includes findings and recommendations pertaining to the FBI's technological investments, human resources, strategic management, and performance measurements to assist in its transformation.

The Academy's current work stemmed from its previous reviews, as well as active consultation with House Appropriations Subcommittee on Commerce, Justice, State and the Judiciary, and with the FBI. This year, the Panel was asked to examine the following areas: Counterterrorism, Office of Intelligence, and Security. Key recommendations from Chapters Two, Three, and Four pertaining to these three areas are discussed below. A full listing of recommendations from Chapters Two, Three, and Four, as well as Chapter One, are provided in an attachment at the end of the Executive Summary.

COUNTERTERRORISM

The Panel's review of the FBI's progress in building its counterterrorism program focused on headquarters Counterterrorism Division, field structure and operations, and information sharing. The Panel believes the FBI has greatly strengthened its counterterrorism program through centralization of leadership and building its headquarters management capabilities to include a new and more active role in overseeing and coordinating counterterrorism cases; integration of its intelligence and law enforcement operations in headquarters as well as in many of its field offices; coordination with other federal, state, and local law enforcement agencies, the intelligence community, foreign governments, and the private sector; information technology systems; and workforce realignment. However, there are a number of areas that would benefit from additional attention.

The Counterterrorism Division at FBI headquarters has built important operational support capabilities. These activities include logistical and administrative support and special information support. The creation of a Fly Team has allowed headquarters to provide timely and expert support to field offices in the U.S. and to partners abroad. The FBI, through its Terrorist Screening Center and Counterterrorism Watch, is able to provide state and local law enforcement and federal screeners with real time database checks to identify known or suspected terrorists, to guide actions and to coordinate timely responses by local joint terrorism task forces. However, some shortcomings remain in this system: the quality of the Terrorist Screening Center database is a continuing challenge and the database is not being used by screeners working for all federal agencies, such as the Transportation Security Administration, or by screeners in the private sector, particularly the airlines. **The Panel recommends the rapid development of a single watch list of known or suspected terrorists and its use by all counterterrorism screening operations.**

The FBI's integration of its law enforcement and intelligence operations includes the adoption of policy and process changes that help ensure that its law enforcement priorities are used to support intelligence-based efforts to identify and disrupt terrorist organizations. As a matter of policy, all counterterrorism cases are now opened as intelligence cases. This policy is supported by a new case classification system that changes the initiation process of investigations from an initial "criminal" case classification to the intelligence-oriented "international terrorism" classification.

In an effort to institutionalize the priority on intelligence gathering in the field, the FBI has proposed criteria—developing sources and the quality of information they provide—for evaluating the performance of counterterrorism agents. These criteria are just a beginning. Further development of a new scheme for evaluating the performance of counterterrorism agents, including criteria and weighting, needs to be undertaken. Moreover, new intelligence-related performance criteria are not yet recognized in the field. Field staff was generally unable to articulate any specific criteria to be used to evaluate the performance of agents working counterterrorism. **The Panel recommends that immediate steps be taken to develop an initial scheme for evaluating the performance of counterterrorism agents in the field, that it be incorporated into agent training, and updated as needed.**

The FBI has made striking advances in its willingness and ability to work jointly with other federal, state, and local law enforcement agencies. Through its use of the joint terrorism task forces, it has been able to increase greatly its capability to address counterterrorism goals. The number of personnel devoted to counterterrorism has grown due partly to increased participation of FBI partners in the task forces. Further, the FBI has been able to capitalize on the complementary legal authorities of its federal partners and the local knowledge of police forces, as well as their own complementary legal authorities. State and local task force participants testified to dramatic, positive changes in their working relationship with the FBI.

At the same time, joint terrorism task forces operate in a diverse and growing population of law enforcement organizations involved with counterterrorism operations. The FBI faces a significant challenge in developing productive working relationships with this emerging network of state and local entities. This task is further complicated by the management of Department of Homeland Security (DHS) grants that support state and local counterterrorism initiatives and sometimes appear to promote competition to perform similar counterterrorism activities. This could discourage joint operations, lead to duplication of effort, and even undermine a coordinated counterterrorism effort. The basis for awarding grants has not seemed to have a coordinated counterterrorism effort as the goal. **The Panel recommends that the FBI work with the Congress and the relevant DHS components to ensure that funding such activities is conditioned on the development of a coordinated effort with the FBI field offices.**

The FBI has just begun to develop performance measures to track progress in meeting its counterterrorism program goals. Individual measures have been proposed. Some are reasonable. Others are less relevant. Although this limited progress is understandable in the midst of the FBI's efforts to organize and staff the program, performance measures are an important next step in the transformation process. **The Panel recommends that the FBI improve its performance measures, making sure that they are clearly linked to the satisfaction of its strategic goals and objectives.**

INTELLIGENCE

Since the events of 9/11, Director Mueller has taken major steps to integrate intelligence into the FBI's mission. In early 2002, he established a small, largely administrative Office of Intelligence, placed an analytic center in the Counterterrorism Division, secured help from the CIA by having 25 analysts detailed to assist the FBI, and initiated an analyst training course modeled on CIA's approach. In January 2003, Director Mueller formally established both a separate Office of Intelligence (OI) and an intelligence program that provided the opportunity to centrally manage the FBI's core intelligence functions.

The FBI views its intelligence production mandate as part of a two-pronged set of related responsibilities: providing intelligence information and analyses involving terrorist threats and national security crimes against the United States, and ensuring that citizens' constitutional rights are protected. As such, the FBI's intelligence work is threat based, but constitutionally bound. The FBI's intelligence role also reflects the heightened priority assigned to countering terrorism and espionage; the increased importance of before-the-fact prevention of activities inimical to U.S. security in these areas; and the increased delegation of after-the-fact reactive investigations of many actual or alleged illegal activities to other federal, state, and local law enforcement authorities. The key recommendations below will help strengthen the FBI's intelligence mission.

The FBI is well on its way to establishing an intelligence structure, policies, processes, and a program to fill the gap in domestic intelligence on terrorism. OI's structure is evolving and will continue to do so as staff is acquired. It has made progress in establishing an intelligence analyst cadre and it is beginning to augment intelligence staff both at headquarters and in the field. The basics of the FBI's intelligence cycle have been defined and are being fleshed out. Field Intelligence Groups are in place in all field offices, though some are sparsely staffed. OI's plan appropriately emphasizes management, rather than daily operational and most production responsibilities, which have largely been decentralized to operating divisions and field offices. **The Panel recommends that OI continue to emphasize intelligence management and that it not become encumbered by detailed operational and production responsibilities**.

Threat assessments are a notable weak point in the nation's domestic intelligence capability. Community-wide products addressing the nature, range, likelihood, and target of longer-term terrorist threats are very limited. Although the FBI updated its U.S. threat assessment approximately one year ago, the intelligence community's threat assessment is severely outdated. During our field interviews, state and local officials expressed considerable frustration about the availability and quality of threat assessments. They commented that the limited availability of threat assessments had led them to rely on alternative approaches, such as lists of key assets and infrastructure elements, equal sharing of grant funds, and vulnerability studies—rather than applying resources based on known or suspected threats. Moreover, there seems to be considerable confusion at the state and local level about the respective roles of the FBI, DHS, Terrorist Threat Integration Center, and state and local authorities in producing threat assessments. Confusion among state and local officials as to who is responsible for doing threat assessments seems to reflect confusion among federal agencies about the scope of their responsibilities. Although the Homeland Security Act of 2002 assigns a component of DHS, infrastructure information analysis and protection (IAIP), authority to do threat assessments, the

FBI and CIA seem unsure of the scope of DHS' authority and responsibility for intelligence analysis. At the same time, the Homeland Security Act of 2002 also assigned the FBI specific responsibility to provide state, tribal and local law enforcement organizations with intelligence on terrorist threats.

The 9/11 Commission concluded that hard choices must be made when allocating scarce resources and recommended that risk-based priorities be established and funding made available to implement protection measures. Yet, this is difficult to accomplish in the absence of generally agreed upon threat assessments.

While DHS is assigned authority to do threat assessments, the current administrative reality militates against DHS performing them. At this time, the IAIP has not developed the intelligence capacity to perform the threat assessment function. Moreover, the entire intelligence structure as currently set up, and as proposed by the 9/11 Commission is at odds with the statutory language providing authority to DHS to do domestic threat assessments. Given the current structure, the intelligence community, not DHS, is in the best position to determine the threat "from abroad" to US interests, and the FBI is specifically assigned responsibility to assess and communicate threats based in the United States and has the capability to do so now. Therefore, **the Panel recommends that the FBI perform domestic threat assessments and continue to develop its capability to do so.**

In-depth strategic collection and analyses efforts tend to be deferred at the FBI. This tendency reflects the realities of a still small analytical staff and the heavy demands for operational support. However, even after a larger analytical staff is built, the tendency will be for immediate operational demands to push out strategic analyses. These analyses must be emphasized and nurtured**. The Panel recommends that the FBI work with headquarters and field personnel to develop a production program focused on strategic analyses. Its work should be coordinated with the Terrorist Threat Integration Center and the intelligence community's National Intelligence Production Board.**

The FBI treats requirements for the internal collection and production of information as action items for its operational and analytical components. It treats similar assignments to other intelligence agencies as requests for information. This approach, as in other intelligence community agencies, fosters over-reliance on capabilities directly under its control and tends to minimize friction with other collection or production agencies. Because of the increased linkage of foreign and domestic intelligence activities concerning terrorism, the treatment of internal and external taskings should be made more uniform to avoid duplicating existing capabilities external to the FBI and increased collection and production efficiencies. **The Panel recommends that the FBI rely on American intelligence agencies operating abroad to meet their covert foreign intelligence needs and that those agencies rely on the domestic intelligence capabilities of the FBI, rather than develop redundant capabilities.**

SECURITY

The FBI has made significant progress in developing a viable security organization with an evolving structure that is meeting the demands of establishing a new division within the FBI. A significant number of new personnel have been hired, and a security officer cadre is being professionalized to meet the demands of an intelligence-driven agency. Security policies are being developed that implement a risk management approach to security, and a significant number of technology system certifications and accreditations have been made. While the FBI has made these significant strides in developing a viable security program, a fully mature Security Division remains several years away. To assist in this development, the Panel has made several recommendations, including the following:

The FBI's strategic goal for security is to establish an enterprise-wide program that includes protection of the FBI from compromise of its employees, its communications and information, and physical attack. To implement this strategy, the Security Division has a five-year plan, covering 2001 to 2006, with its fiscal year 2004 portion included in the FBI's current overall five-year strategic plan. **The Panel recommends that the FBI develop performance measures for all essential elements of security operations.**

During interviews with personnel security investigation staff, reliable quantitative management data could not be provided to make judgments regarding management's accomplishments and needs. This problem stems in part from inadequate information technology systems. **The Panel recommends that the Security Division complete a management information system that provides accurate and adequate statistical information on security.**

Numerous security policies have been developed and issued via executive communications. However, headquarters and field personnel interviewed often were not aware of these policies. This is due in part to the lack of a complete up-to-date listing of policies in one place, where the policies may be referenced systematically. A new web-based security manual is due to be completed in November. **The Panel recommends that the new security policy manual be completed and issued as soon as possible.**

The FBI's process enables the Director of Security to certify the security of an information technology system, and the Chief Information Officer to accredit it. The system's user or owner is not formally involved in this process. Last year, the Academy Panel recommended that the user or owner be responsible for accreditation and agree to accept any security risks. Although the Chief Information Officer's involvement is necessary, the current process does not recognize the responsibility of risk that should be borne by the user or owner. **The Panel recommends that system users or owners be formally involved in the accreditation process with the Chief Information Officer and the Security Division.**

The FBI uses the Background Investigation Contract Service to obtain required background information on individuals. The Webster Commission recommended consolidating security investigations and adjudications in a new Office of Security. A decision about which division—

Administrative Services or Security—has managerial responsibility for BICS is needed. **The Panel recommends that security investigation and adjudication responsibility (for security, as well as suitability) be placed within one division, regardless of which division is selected.**

The Webster Commission recommended that the FBI's personnel security process be automated. Yet the FBI's system for processing security background investigations, re-investigations, and adjudications continues to be paper intensive. Lack of automation creates inefficiencies that are partially responsible for the length of time taken to complete the security clearance process. Likewise, the BICS process should be automated and integrated with the application/background investigation programs. **The Panel recommends that whichever division is given responsibility for security investigations and adjudication, that division give high priority to accelerating automation of the personnel security process.**

LISTING OF ALL REPORT RECOMMENDATIONS

A total of 37 recommendations are made in Chapters One, Two, Three, and Four. A list of recommendations for each chapter is provided below.

CHAPTER ONE–THE FBI'S TRANSFORMATION

Seven recommendations are made in Chapter One. A full discussion of these recommendations is provided at the end of the chapter, starting on page 20.

The Panel recommends that the FBI continue to be the key domestic intelligence agency responsible for such national security concerns as terrorism, counterintelligence, cyber, and transnational criminal activity.

The Panel recommends that the concept of joint operations, whether through joint task forces or other similar approaches, be applied more broadly to other critical law enforcement activities.

The Panel endorses the 9/11 Commission's recommendation that "the President should lead a government-wide effort to bring the major national security institutions into the information revolution and coordinate the resolution of legal, policy, and technical issues across agencies to create a 'trusted information network'." The Panel further recommends that the FBI component of this trusted network should be implemented as soon as possible and extend to state and local law enforcement agencies with respect to counterterrorism information.

The Panel recommends that the FBI's enterprise architecture and information technology systems under development be broadened to ensure state and local connectivity.

The Panel recommends that the FBI devote increased emphasis to these human resource planning needs. More specifically, the FBI should develop intelligence career alternatives for analysts, agents, and support personnel. But given the integration of intelligence, operations, and support activities and the extent of proposed cross-training of agent recruits and supervisor agents, the FBI needs to consider alternatives that develop highly flexible and mobile career paths integrated within a single personnel system.

Panel recommends, at a minimum, that the FBI move to, and Congress support, a multi-year resource planning system for critical technical systems and key personnel skills. In addition, it recommends that FBI personnel, including agents, be increasingly involved in external management and technical training programs, such as those sponsored by leading public and international affairs schools, The Brookings Institution, and the Department of Defense.

The Panel strongly recommends that performance measurement be increasingly incorporated as a fundamental management tool within the FBI.

CHAPTER TWO–COUNTERTERRORISM

Nine recommendations are made in Chapter Two. A full discussion of these recommendations is provided at the end of the chapter, starting on page 43.

The Panel recommends that the process by which FBI headquarters levies special requests on the field be reviewed to determine whether it might be managed so as to minimize disruption to ongoing counterterrorism cases.

The Panel recommends the rapid development of a single watch list of known or suspected terrorists and its use by all counterterrorism screening operations.

The Panel recommends that immediate steps be taken to develop an initial scheme for evaluating the performance of counterterrorism agents in the field, that it be incorporated into agent training, and updated as needed.

The Panel recommends that senior FBI officials meet with the appropriate state and local officials to resolve outstanding jurisdictional conflicts to ensure the coordination of counterterrorism operations in the field.

The Panel recommends that the FBI work with the Congress and the relevant DHS components to ensure that funding such activities is conditioned on the development of a coordinated effort with the FBI field offices.

The Panel recommends that the U.S. Attorney General provide clear guidance that Anti-terrorism Advisory Councils focus on coordination and dispute management and that they dedicate at least one Assistant U.S. Attorney to the task.

The Panel recommends that field offices be given policy and funding support to ensure that meaningful integration of analysts and operations is established, maintained, and nurtured.

The Panel recommends that the FBI promote the sharing of information on best practices for state watch and warning systems among state and local law enforcement and that it work with the relevant DHS components to accomplish this.

The Panel recommends that funded headquarters positions be fully staffed and reliance on temporary duty assignments of field personnel be significantly reduced.

The Panel recommends that the FBI improve its performance measures, making sure that they are clearly linked to the satisfaction of its strategic goals and objectives.

CHAPTER THREE–INTELLIGENCE

Eight recommendations are made in Chapter Three. A full discussion of these recommendations is provided at the end of the chapter, starting on page 66.

The Panel recommends that the Office of Intelligence continue to emphasize intelligence management and that it not become encumbered by detailed operational and production responsibilities.

The Panel recommends that the FBI perform domestic threat assessments and continue to develop its capability to do so.

The Panel recommends that the FBI consider reexamining its internal personnel processes and policies to determine possible impediments to staffing, as well as identifying more flexible hiring authorities that would facilitate staffing.

The Panel recommends that in-person interviews with candidates be mandated when hiring analysts.

The Panel recommends that the FBI work with headquarters and field personnel to develop a production program focused on strategic analyses. Its work should be coordinated with the Terrorist Threat Integration Center and the intelligence community's National Intelligence Production Board.

The Panel recommends that the FBI rely on American intelligence agencies operating abroad to meet their covert foreign intelligence needs and that those agencies rely on the domestic intelligence capabilities of the FBI, rather than develop redundant capabilities.

The Panel recommends that the FBI develop regular processes that promote sharing, such as tear-line products and information technologies. It specifically endorses the findings and recommendations of the 9/11 Commission concerning the need for improvements in information sharing and the potentially helpful role that incentives (and penalties) could play in the process.

The Panel recommends that the Administration and Congress adopt a multi-year appropriation process to address the need for sustained investment in some of these key areas.

The Panel recommends that the FBI develop intelligence career alternatives covering all intelligence analysts as soon as possible. Given the integration of intelligence, operations, and support activities and the extensive law enforcement and intelligence cross-training recommended by the 9/11 Commission for new recruits and supervisory agents, the Panel recommends that the FBI consider alternatives that enable highly flexible and mobile career paths within a single personnel system.

CHAPTER FOUR–SECURITY

Twelve recommendations are made in Chapter Four. A full discussion of these recommendations is provided at the end of the chapter, starting on page 82.

The Panel recommends that the FBI develop performance measures for all essential elements of security operations.

The Panel recommends that the Security Division complete a management information system that provides accurate and adequate statistical information on security.

The Panel recommends that the new security policy manual be completed and issued as soon as possible.

The Panel recommends that each manager's performance appraisal include a critical element that relates to the manager's understanding of security rules and procedures and the security awareness of his or her subordinates.

The Panel recommends increased support staff, and physical and technical security resources for the field offices to implement the FBI's strategic plan relating to security.

The Panel recommends that security investigation and adjudication responsibility (for security, as well as suitability) be placed within one division, regardless of which division is selected.

The Panel recommends that whichever division is given responsibility for security investigations and adjudication, that division give high priority to accelerating automation of the personnel security process.

The Panel recommends that the FBI supplement BICS by utilizing additional private contractors who specialize in background investigations for the federal government when attempting to clear large numbers of applicants or contractor personnel.

The Panel recommends that system users or owners be formally involved in the accreditation process with the Chief Information Officer and the Security Division.

The Panel recommends that the FBI request additional funding to adequately address the current deficiency of SCIF space over the next five years.

The Panel recommends that the FBI adopt explicit procedures to monitor classified national security information sharing to ensure that necessary sharing occurs and that the discretion demanded by the practical need to share is not abused.

The Panel recommends that when selecting new security officers, the Security Division specifically address their qualifications and credentials for managing security of

information technology systems, as well as provide information system security training for current security officers.

INTRODUCTION

THE ACADEMY AND THE FBI

In May 2002, Congressman Frank Wolf, Chair of the House Appropriations Subcommittee on Commerce, Justice, State, the Judiciary and Related Agencies, asked the National Academy of Public Administration (Academy) and several other organizations to review the reorganization of the Federal Bureau of Investigation (FBI). At that time, FBI Director Robert Mueller already had begun the task of reorienting his organization in the wake of the events of September 11, 2001. For the FBI, the immediate post-9/11 response was to reallocate temporarily a very large percentage of its personnel—more than 60 percent of its field agents—and resources to investigate the attacks on the Pentagon and the Twin Towers, which collectively became known as PENTTBOM. To guard against future acts by suspected perpetrators, Director Mueller announced a new strategic focus for the FBI in Fall 2001. It emphasized the importance of preventing, not just solving, terrorist acts and established a new set of priorities to guide FBI field operations. These priorities are remarkably straightforward, providing an early perception of the direction of change deemed necessary for the FBI.

FBI PRIORITIES

1. Protect the United States from terrorist attack.
2. Protect the United States against foreign intelligence operations and espionage.
3. Protect the United States against cyber-based attacks and high-technology crimes.
4. Combat public corruption at all levels.
5. Protect civil rights.
6. Combat transnational and national criminal organizations and enterprises.
7. Combat major white-collar crime.
8. Combat significant violent crime.
9. Support federal, state, county, municipal, and international partners.
10. Upgrade technology to successfully perform the FBI's mission.

Of the items listed above, the first eight address programmatic priorities and the remaining two—law enforcement cooperation and technology upgrade—address supporting priorities. Together, these priorities have become the cornerstone of building the new FBI. They are headlined on the FBI website, prominently displayed at headquarters and field offices, and firmly implanted in the consciousness of FBI employees.

In a sense, these priorities were not strikingly new when announced in 2001. The counterterrorism mission took on increased importance following the 1993 garage bombing at the World Trade Center, the 1995 bombing of the Murrah Federal Building in Oklahoma City, the terrorist attacks on Khobar Towers in Saudi Arabia, and the twin truck bombings of U.S. embassies in Nairobi, Kenya and Dar es Salaam, Tanzania. However, FBI resources committed to counterterrorism were limited in the pre 9/11 environment. A small counterterrorism unit had been established in Washington, though the bulk of FBI agents and activities dedicated to that mission was concentrated in New York. Almost all international terrorism action items were referred to that office for follow-up action.

In the more than two years since it began its work, the Academy Panel on FBI Reorganization (whose members are listed in Appendix A) has examined the FBI's transformation, including its divisional reorganizations and major process, personnel, and cultural changes. In its June 2002 congressional testimony, the Panel endorsed the thrust of Director Mueller's reorganization, including the creation of several divisions, and made specific recommendations designed to improve the prospects for success. At that time, Chairman Wolf and Director Mueller both agreed that the Panel would continue to monitor implementation of the FBI's new strategic priorities and its reorganization plan during the following year. The Panel reported on the progress made in June 2003, offering additional recommendations that might speed implementation and improve the likelihood for success. Chapter One addresses those recommendations in greater detail.

At Chairman Wolf's request, the Academy also convened an informal task force to review proposals that would affect the FBI's budget structure and personnel and pay authorities; the proposals were being considered as part of the FBI's Fiscal Year 2005 appropriations process. In conjunction with representatives of the FBI, Department of Justice (DOJ), Government Accountability Office (GAO), and Congressional Research Service (CRS), the task force addressed six proposals designed to improve the FBI's budget, personnel, and pay systems. The Academy's president testified on them in June 2004, and several are included in the FBI's pending appropriations bill.

THE ACADEMY PANEL'S CURRENT TASK

The Academy Panel's current task stemmed from its previous reviews, as well as active consultation with House Appropriations Subcommittee staff and the FBI. This year, the Panel was asked to examine the following areas:

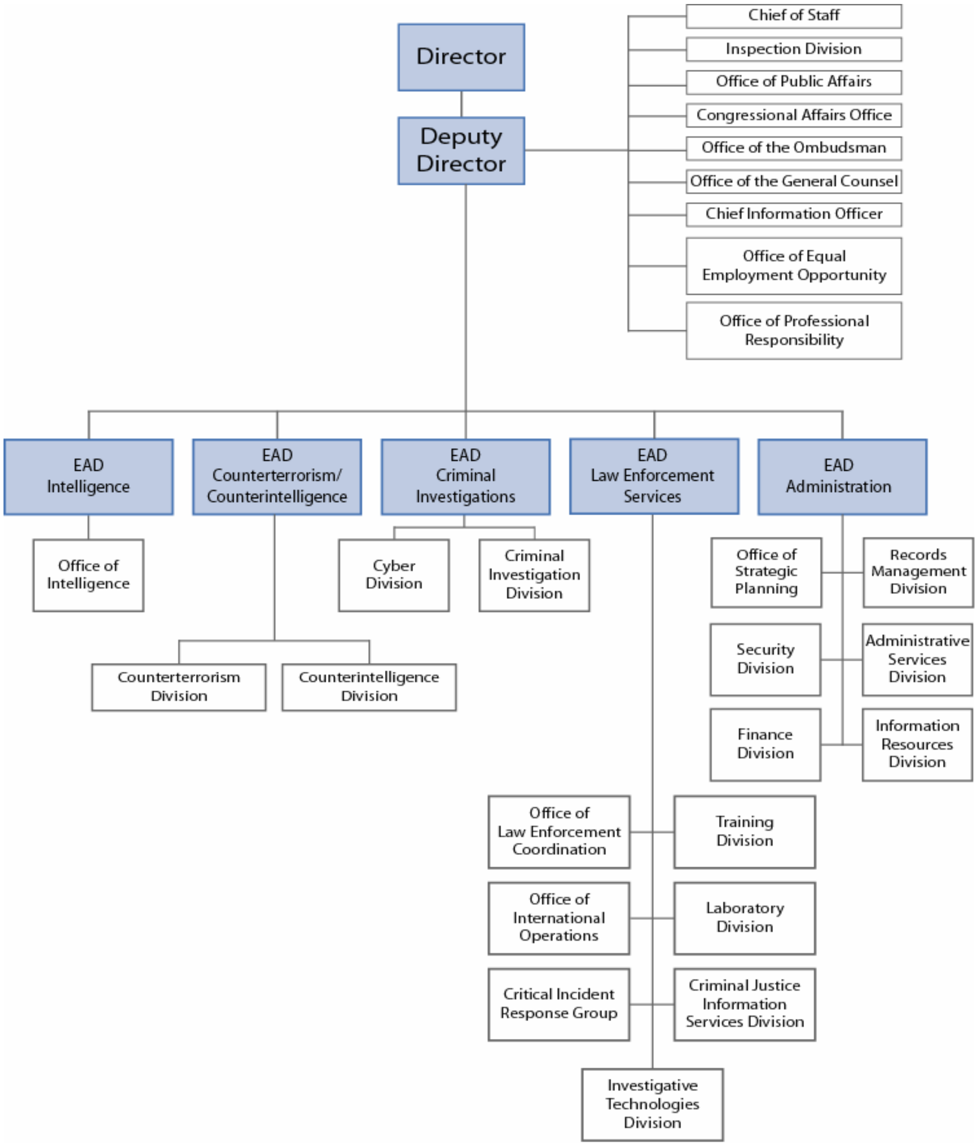
- **Counterterrorism Division.** The Panel was asked to provide an update on changes made in the Counterterrorism Division. Specifically, it was to assess the FBI's processes and technologies for sharing counterterrorism information, both internally and externally with state/local law enforcement agencies, first responders, and foreign partners.

- **Office of Intelligence.** The Panel was asked to review the FBI's progress in forming and developing this office. It was to focus on the office's structure, concepts of operations, integration of its activities with other intelligence community activities, and processes for intelligence collection, analysis, and dissemination.

- **Security.** The Panel was asked to evaluate the FBI's progress in adopting the security recommendations of the Webster Commission and the Rand Report. It was to assess progress made in establishing and implementing security policies and carrying out the Security Division's program plan.

The FBI organization chart in Figure 1 below shows the three major components that cover these areas. They are considered fundamental to the FBI's transformation and critical to its efforts against terrorism in the United States and abroad. The Panel has not reviewed most of the Director's immediate staff structure or several other important organizational components. However, the Panel's previous work addressed the *Chief Information Officer*, the *Cyber Division*, *Investigative Technologies* within Law Enforcement Services, and *Records Management* within Administration. An updated assessment of these components is not part of the Panel's current review.

Figure 1. Organization of FBI Headquarters


Director
Deputy Director
Chief of Staff
Inspection Division
Office of Public Affairs
Congressional Affairs Office
Office of the Ombudsman
Office of the General Counsel
Chief Information Officer
Office of Equal Employment Opportunity
Office of Professional Responsibility
EAD Intelligence
EAD Counterterrorism/ Counterintelligence
EAD Criminal Investigations
EAD Law Enforcement Services
EAD Administration
Office of Intelligence
Cyber Division
Criminal Investigation Division
Counterterrorism Division
Counterintelligence Division
Office of Strategic Planning
Records Management Division
Security Division
Administrative Services Division
Finance Division
Information Resources Division
Office of Law Enforcement Coordination
Training Division
Office of International Operations
Laboratory Division
Critical Incident Response Group
Criminal Justice Information Services Division
Investigative Technologies Division

In addition, the Panel is developing criteria that could be used to shape the FBI's field structure. This task is to focus on reviewing the existing field office and resident agency structure and suggesting criteria that the FBI could use to assess the structure in light of changing priorities, technologies, and case management approaches. The report on this task has been deferred until early 2005 to enable a more intensive and immediate focus on the areas addressed herein.

METHODOLOGY

The Panel has relied on its 2002 and 2003 work concerning the FBI's reorganization, pace of implementation, and rationale for change. It has benefited from regular briefings by key FBI officials, including Director Mueller and assistant directors of the key components. Panel members, individually and collectively, and the project staff also have enjoyed considerable familiarity and contact with individuals and organizations that offer independent judgments on the areas covered in this study, as well as the larger issues of intelligence, law enforcement, and homeland security strategy and organization.

Specific research and study methodologies employed by the Panel included:

- review of studies, monographs, and reports—listed in Appendix C—by other public, non-profit, and private institutions, including their findings, conclusions, and recommendations

- review of extensive material provided by the FBI on its budget, strategic plan, personnel, security, concepts of operations for intelligence, and other matters

- detailed interviews with FBI headquarters and field staff, particularly in the areas of counterterrorism, intelligence, and security

- selected interviews with individuals outside the FBI, including officials from the Office of Management and Budget (OMB), Central Intelligence Agency (CIA), the Departments of Justice and Treasury, and GAO, and state and local homeland security and law enforcement officials

The recent 9/11 Commission report and other counterterrorism and intelligence studies since 9/11 have served to enlighten this study. Chapter One explores the relevance of their findings, conclusions, and recommendations.

ORGANIZATION OF THIS REPORT

Chapter One provides an overview of the FBI's transformation, external reviews and their recommendations for change, and this Panel's overarching findings, conclusions and recommendations. The remainder of the report devotes a separate chapter to each major subject the Panel was tasked to address. Chapter Two covers Counterterrorism, perhaps the most critical of the assigned review tasks. Chapter Three addresses Intelligence, the essential element for transforming the FBI from a reactive, after-the-fact criminal investigative agency to a proactive, before-the-fact preventive entity. This function, initially focused on countering terrorism, is vital for such other national security activities as counter-intelligence and cyber crimes. Chapter Four addresses Security, a key enabling capability for success in counterterrorism and intelligence activities, and the pace with which the FBI's plans for improvements are being implemented at headquarters and in the field.

The report's appendices provide additional and more detailed information about the study, the Panel members and staff, the FBI's intelligence plan, and the Webster Commission's recommendations. A selected bibliography and list of individuals and/or position contacted are also included.

CHAPTER ONE
THE FBI'S TRANSFORMATION

ORGANIZATIONAL CHANGE AND TRANSFORMATION

The FBI is in the process of transforming itself. Once dominated by reactive, after-the-fact investigation of alleged or known crimes largely by individuals or organized domestic groups, its mission has changed greatly. Now, it is increasingly becoming characterized by proactive, before-the fact prevention of suspected terrorism or other crimes by nations or organized foreign groups. To be sure, the FBI will continue to carry a heavy criminal workload, as it has for a century and as Director Mueller has recognized in his priorities. The FBI will be called upon to guide and support these tasks, but execution will be much more distributed. As the national security portion of its mission comes to dominate, the FBI will need to rely on other federal, state, and local law enforcement entities to pick up an increased share of its more traditional tasks.

Intelligence, a peripheral matter in most traditional criminal investigations, is integral to a prevention-focused mission. Learning from external sources about threats and uncovering those threats by actively targeting potential terrorists are fundamental. The former requires elaborate mechanisms for cooperation and collaboration with other entities, the US. foreign intelligence community, foreign law enforcement organizations, and other federal, state, and local law enforcement entities. The latter thrives on active outreach into those areas from which terrorism is likely to arise; this outreach frequently is done in cooperation with other law enforcement organizations, but occasionally is unilateral.

For foreign terrorism, familiarity with the international environment is needed, as are close relationships with the intelligence community, foreign law enforcement entities, nation states, and even groups within individual states that have radically different ideologies and perspectives. Similarly, intelligence information collection domestically often depends on strong connectivity with other federal, state, and local agencies. This approach shares some similarity with the FBI's traditional handling of cases in conjunction with law enforcement entities at all levels, but it dictates a much closer interdependence on many areas remote from most local law enforcement entities.

Traditionally, the management of cases, with some exceptions, has been left to the individual field offices of the FBI. However, the events of 9/11 emphasized the need for greater inter-office and inter-agency coordination. Cases of terrorism and national security require a central capability to coordinate operations and to provide intelligence analysis that helps connect disparate information and data. Although execution of the vast majority of operations should remain decentralized, it must be coordinated and overseen centrally.

Further, the goals of traditional criminal investigation and more current terrorist prevention are different. FBI agents and managers long have measured their success on arrests, prosecutions, and convictions, standard benchmarks for law enforcement investigative activities. These traditional measures are largely irrelevant to the prevention mission in terrorism and other areas of national security. The new paradigm places priority on intelligence information collection and analysis, not prosecution. Indeed, prevention may compromise prosecution and conviction in some cases. Investigators may undertake covert activity to provide the best source of information about attacks or other actions; prosecution in such cases may have to be foregone in favor of the greater goal of prevention. Occasionally, that activity may provide the essential information that ultimately enables prosecution of a larger target.

Meeting the demands of the counterterrorism and national security mission places a premium on information technology, the backbone communications and information processing system that supports rapid integration of data from multiple sources. Information technology enables analysts to connect the dots, integrating increasing volumes of information. Disparate, isolated bits of information demand a capacity to create a mosaic, an analytical picture that combines these bits and provides a high confidence basis for preemptive or preventive action.

The personnel skills mix also changes with the FBI's new priorities. There is greater demand for non-agent personnel with specialized skills such as analysts, linguists, technical experts, and surveillance specialists who must be hired, trained, nurtured, and promoted. Also, new skills are demanded of special agents. Just as the FBI hired agents with backgrounds in accounting and finance to meet the demands of white collar crime, the FBI is now seeking agents with the skills and experience appropriate to meet the demands of its new mission priorities.[1] Moreover, these new priorities require agents who can and will work effectively with the new non-agent professionals. Also, they must work together within short time frames demanded by interventions to prevent terrorist acts, in contrast to the lengthier process of accumulating evidence that defines traditional criminal cases aimed at prosecution .

The changes in FBI operations, technology, and personnel place a premium on strategic management at headquarters, which had been accustomed to a more limited administrative management role. Mixing the ingredients of intelligence information collection and analysis, field agent operations, recruitment and training of personnel with the right skills, and management of information technology projects often global in scope and comprehensive in detail requires a heightened level of strategic management. Project management skills in contract management, personnel acquisition, career development, intelligence analysis, or operational integration are increasingly important and vital to the success of the FBI's mission.

Finally, these cumulative changes require a substantial adjustment in organizational culture and personal values. The dedicated, intelligent, self-reliant field agent now must become part of a larger institutional mechanism in which he or she continues to play a major role, but whose success increasingly is measured in collaborative and cooperative terms. As new intelligence processes and information and operations integration take hold, new values—both personal and

[1] Language skills, notably in Arabic and Farsi, are undoubtedly necessary if agents are to be effective in counterterrorism operations. As noted in Chapter Three, intelligence is now the primary focus of counterterrorism operations and the FBI has identified the development of human intelligence sources as a basis for evaluating special agent performance. Given that terrorists operate through communities speaking these languages, proficiency in the relevant languages is essential to identifying, recruiting, and managing sources with useful information. Training and recruitment of special agents with relevant language skills is an issue that deserves consideration in subsequent reviews.

institutional—emerge. Incentives and reward structures must be created to support the growth of these values.

The FBI is carrying out this transformation not during a period of peace and tranquility, but amid a maelstrom of high pressure demands and increased tempo of operations. Operational demands arising from changes in homeland security alert status, heavy support for Operation Iraqi Freedom, additional requirements for the Olympics, and protection needs at political conventions and for candidates have obviously impacted the pace of transformation. If the pace is too slow, the risk of losing momentum is palpable. If it is too fast, the risk increases that one or more critical building blocks will be out of phase, jeopardizing needed changes.

EXTERNAL REVIEWS AND RECOMMENDATIONS FOR CHANGE

Much of the impetus for the FBI transformation originated internally, certainly with Director Mueller's restatement of priorities and his original reorganization proposal. Numerous outside groups and external reviews also have aided the transformation process through critical appraisals and insights. These include reviews by the Academy Panel and GAO, Congress and a presidential commission, and others. They are summarized below to provide a sense of the range of assessments and recommendations, and their impact on shaping and refining the FBI's initiative to reform and restructure itself.

The Panel's Initial Review of the FBI Reorganization

In May 2002, Director Mueller asked Congress to formally address a fundamental reorganization of the FBI that reorganized the Counterterrorism Division and created four new divisions. These divisions are charged as follows:

- The Counterterrorism Division is devoted to preventing future ones in the United States, as well as to investigating terrorist acts already perpetrated.

- The Cyber Division is focused on computer-related crime and terrorism aimed at the information technology infrastructure underpinning the operations of public and private organizations in the U.S.

- The Security Division was created in response to past counterintelligence failures and the growing need to accommodate classified national security intelligence information in counterterrorism and counter-intelligence activities.

- The Records Management Division was created to address the FBI's serious shortcomings in records management exposed by investigative records associated with the Oklahoma City bombing and the conviction and postponed execution of Timothy McVeigh.

- The Investigative Technologies Division, was created to place greater emphasis on technologies needed to support investigative activities and to improve management of these activities in its Forensics Laboratory by reducing span of control.

In response to Chairman's Wolf's request, the Academy formed its Panel on FBI Reorganization, composed of distinguished Academy experts, to intensively examine the FBI's proposed reorganization and associated funding changes. In a short time, the Panel and project staff conducted a detailed review of the rationale associated with the proposed organizational realignments, examined previous studies addressing terrorism, security, and FBI management, and met with Director Mueller and his key staff concerning the revised strategic focus. Funding adjustments required to execute the reorganization also were examined and addressed.

The Panel endorsed the proposed reorganization, the creation of the five new divisions, and the proposed reallocation of funding. The Panel **warned, however, that the reorganization "is the beginning—not the end" and commenced "a long-term process of institutional and cultural change."** The reorganization on which Director Mueller had embarked, the Panel noted, provided "**an overarching framework within which other personnel, institutional, and operational changes can be accomplished."** The Panel recognized that reorganization must be accompanied by the changes in personnel, administrative processes, and further resource reallocations. **It urged the FBI to adopt an approach that set out an explicit management agenda and timetable to implement these ancillary changes implicit in the Director's comment about the reorganization,** such as:

- **Improving headquarters accountability for counterterrorism** and counterintelligence investigations. The Panel specifically endorsed the importance of prevention, rather than prosecution, in the field of terrorism.

- **Increasing information sharing** internally and externally with other federal agencies, state and local law enforcement entities, and international partners. The Panel emphasized that major information sharing improvements were critical.

- **Reassigning and recruiting personnel** to fill gaps and developing personnel and evaluation systems that recognize specialized expertise and reward innovation.

- **Improving analytical and managerial training.**

- **Upgrading the FBI's outdated information technology**. The Panel was particularly concerned with the apparent fragmentation of management control over information technology resources, the need to closely monitor progress on the FBI's developmental information technology project (Trilogy), and the need to address counterterrorism shortfalls in data capture and analysis systems.

The Panel also encouraged the FBI to develop performance measures to assess the pace at which the reorganization was meeting its goals and to adopt external review processes that provide independent perspectives on reaching organizational objectives.

The Panel's Monitoring of the Pace of Implementation

The House Appropriations Subcommittee approved the proposed reorganization and associated funding changes. In so doing, it asked the Academy Panel to continue its review and monitor the pace of the reorganization during the following year. The Panel and project staff developed an approach which minimized intrusion on the FBI's work, but entailed executive-level briefings, including meetings with Director Mueller, principal deputies, and heads of the new divisions. In coordination with subcommittee and GAO staff, the Panel worked with GAO to divide tasks to avoid duplicative information requests and interviews. GAO addressed strategic planning, personnel recruitment and training, and internal controls, and conducted extensive field office interviews. The Academy focused on evolving headquarters division changes, including the steps needed to implement the reorganization, as well as information sharing, information technology, and drug enforcement.

In its June 2003 report to Congress, the Panel recognized some early signs of success: the widespread acceptance, both at headquarters and in the field, of the Director's priorities, the infusion of top-notch outside talent in areas where critical skills were needed, and the continuing resource reallocation to meet the FBI's greatest needs. The Panel tempered its assessment, however, warning that "institutional transformations do not occur overnight and involve major cultural change."

The Panel emphasized five areas that it believed were critical to successful transformation. These were:

- **Counterterrorism.** The Panel found solid progress in structuring and improving counterterrorism operations and providing intelligence support to the Counterterrorism Division. Its recommendations focused on the continued need for close coupling between counterterrorism and the FBI's other law enforcement activities. **It urged an explicit strategy for information sharing and the development of explicit performance measures.**

- **Intelligence.** The Intelligence office was created in early 2003 to help develop and manage an intelligence career structure for analysts and other intelligence personnel, establish and manage intelligence processes, and interface with the intelligence community, including the Director of Central Intelligence's Community Management Staff. The Panel acknowledged that it was premature to judge the office's initial success, but **recommended that priority be assigned to requirements definition, collection assignment, and collection evaluation. It urged that intelligence remain a small staff component aggregating the FBI's management functions related to intelligence** and isolating it from the immediate operational and analytical intelligence tasks by assigning them to other FBI elements.

- **Information Technology.** The Panel noted some initial positive signs, but warned that the FBI's success in using modern information technology to fulfill its mission is still open to question. It noted that the Virtual Case File was the most difficult part of its ambitious Trilogy initiative; the need for training and continued information technology modernization was evident. **The Panel recommended that the FBI document and maintain an enterprise architecture, strengthen the role of its Chief Information Officer, and develop an ongoing modernization program with annual funding.**

- **Process Re-engineering Projects.** The FBI created 40 process re-engineering projects to accompany its reorganization, partially in response to the Panel's earlier recommendation to develop a systematic management approach. The projects covered headquarters processes in such areas as project and personnel management, headquarters and field organizational structures, technology, culture/values, and policies. **The Panel recommended that this re-engineering process continue as a means to stimulate management action and monitor progress. It also emphasized the need for performance measurement and outside expertise and assistance to aid this initiative.**

- **Advanced Science and Technology.** The Panel acknowledged the pace of technological advances and the growing importance of information technology, cyber intrusions, and investigative technologies applicable to investigations and intelligence. **It applauded the FBI's new Science and Technology Advisory Board and recommended adding a technology supplement to the FBI's strategic plan.**

The Panel also addressed areas supporting FBI's transformation, such as security, records management, investigative technologies, consolidation of cyber crime investigations, and resulting offsets in drug enforcement. Again, the **Panel emphasized the overriding importance of information sharing** as the FBI transforms itself and becomes the lead domestic agency in preventing terrorism and performing other national security functions, and retains its preeminence in criminal law enforcement. Finally, **the Panel emphasized the importance of changing the FBI culture by shifting emphasis from the agent's traditional values of independence, determination, strong camaraderie, and professionalism to ones of joint collaboration, interagency cooperation, and information sharing.**

Congressional and Other National Inquiries and Studies

The Academy Panel has not conducted its assessments in a vacuum. Numerous national, state, and local inquiries have explored in considerable depth the circumstances of 9/11 and deficiencies in intelligence, law enforcement, and emergency services. The Panel did not explore the details of the events preceding 9/11, but instead focused on Director Mueller's prescribed organizational, policy, process, and resource changes, and examined the pace and extent of these changes. Nonetheless, the Panel's work has benefited significantly from the increasingly detailed and thorough exploration of the events surrounding 9/11 and the recommendations resulting from these inquiries. There are a host of reports, including:

- New York City's inquiry into its emergency preparedness and response

- Markle Foundation's Task Force report on *Protecting America's Freedom in the Information Age*

- Council on Foreign Relations studies of the state of homeland security

- Numerous GAO reports on the FBI, homeland security, and the government's counterterrorism activities

- Internal DOJ studies of FBI management and Inspector General reports on FBI operations and activities

- Detailed CRS and Rand monographs on alternative domestic intelligence structures and other democracies' experiences and practices in this area

The Joint Inquiry conducted by the House and Senate Intelligence committees and the 9/11 Commission's hearings, staff statements, and report directly addressed FBI shortcomings and suggested reforms. Following extensive security vetting, the former was publicly released in 2002, while the latter was published in July 2004. Their major findings, conclusions, and recommendations, summarized below, have been considered throughout the Panel's assessment and have helped to inform its findings and recommendations.

The Joint Inquiry of December 2002

The *Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001* was undertaken jointly by the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence. Its findings, conclusions, and recommendations covered a broad array of activities conducted by the U.S. intelligence community, specifically the CIA, National Security Agency (NSA), Department of Defense, Department of State, and the FBI. As with the subsequent 9/11 Commission report, it endorsed a statutory Director of National Intelligence separated from CIA and other intelligence agencies with management, budgetary, and personnel responsibilities for the intelligence community, presumably including the FBI's national security-related activities.

Beyond this overarching recommendation, the Joint Inquiry made numerous findings and recommendations with regard to the FBI itself, specifically:

1. **Lack of an effective domestic intelligence capability.** It recommended clearly designated national counterterrorism priorities, enforced field office adherence, and substantially increased penetration of terrorist organizations operating in the United States.

2. **Inconsistent quality in analysis and many inexperienced, unqualified, under-trained analysts lacking access to critical information.** It recommended significantly improving the FBI's strategic analysis capabilities to address these deficiencies.

3. **Reliance on outdated and inefficient technical systems with a community-wide absence of a central counterterrorism database.** It recommended solving the FBI's

persistent and incapacitating information technology problems, but did not offer specifics.

4. **Inadequate sharing of counterterrorism information within the intelligence community and serious information sharing problems with non-intelligence agencies, including state and local authorities.** It urged implementing mechanisms to maximize the exchange of counterterrorism information.

5. **A cultural mindset that perpetuated the "tyranny of the case file" and defaulted to law enforcement because of the difficulty of other approaches.** It recommended independent career tracks for counterterrorism agents and analysts, including a reports officer cadre to facilitate intelligence dissemination, supported by improved recruitment and training for these personnel.

The Joint Inquiry also found deficiencies in foreign language skills, insufficient collaboration between NSA and the FBI, a lengthy and difficult process that stifled the use of intercepts, and strategy voids in tracking terrorist financing and closing terrorist support networks. It made specific recommendations to address these deficiencies, as well. Further, it raised the possibility of a separate MI-5-type structure after it examines the FBI's progress in implementing reforms, the experience of other democratic nations, and the balance between enhancing national security and protecting civil liberties. Senator Richard Shelby, Vice Chairman of the Senate Select Committee on Intelligence, critiqued the combination of organizational, cultural, and technological impediments that led the FBI to a recurring pattern on information dysfunction. He examined the MI-5 approach, which would either assign the FBI's national security functions to a semi-autonomous organization under the FBI Director, or transfer them to the DHS.

In the area of counterterrorism, the Joint Inquiry addressed the development of DHS as an effective all-source terrorism fusion center focused on analysis in addition to its role within and beyond intelligence community boundaries. It also offered recommendations directly to the executive and legislative branches. To expand access and reduce inappropriate and obsolete barriers, it urged the President to review policies and procedures for national security classification. As for Congress, it encouraged consideration of legislation modeled on Goldwater-Nichols to instill "jointness" throughout the intelligence community through incentives for joint service among intelligence agencies and with their customers. It also encouraged Congress to investigate excessive classification, and recommended a national watch list center.

In many respects, the Joint Inquiry's recommendations mirrored the findings and recommendations of a mid-2002 report by the House Permanent Select Committee on Intelligence's Subcommittee on Terrorism and Homeland Security. Its report covered the full range of intelligence activities and agencies, with heavy emphasis on CIA and NSA. Yet it also addressed and criticized the FBI's counterterrorism efforts, including the policy of decentralizing investigations, especially against international terrorist targets, the lack of emphasis on preventing terrorist acts, ineffective counterterrorism analytical capability, critical shortages in language proficiency, and the reluctance to institute broader information sharing measures. **It called for a "clear strategy incorporating the personnel dimension, the technical dimension,**

and the legal dimension of the information sharing problem." It urged improvements in intelligence gathering, analytical capabilities, language proficiency, and an information technology implementation strategy that "incorporates plans to facilitate the necessary information sharing processes with the intelligence and homeland security communities." Needless to say, it found similar—in many cases, more severe—difficulties in CIA, NSA, and other intelligence agencies.

The 9/11 Commission Findings and Recommendations (July 2004)

The National Commission on Terrorist Attacks upon the United States, commonly known as the 9/11 Commission, examined in considerable detail the 9/11 attacks and several prior terrorist acts, and focused its findings and recommendations on counterterrorism strategy and proper government organization to implement its suggested strategy. Most of the Commission's strategy elements affect the FBI and foreign intelligence agencies only indirectly, such as:

- foreign policies affecting the United States and its relationships with Middle Eastern countries, including their economies and educational systems, media interaction with the people and considerations of coalition and allied cooperation

- domestic border and air passenger screening, visitor tracking, incident command, communications, and preparedness recommendations

Several strategy recommendations deal more directly with counterterrorism operations and intelligence, particularly those relevant to the FBI. These include:

- an aggressive attack on terrorism financing

- a focused effort that combines intelligence, operations, and law enforcement on targeting terrorism travel, both internationally and within the United States

- federal assistance to states and localities based on risk assessments

- privacy protection while maximizing information sharing

To implement these strategy recommendations, the 9/11 Commission offered findings and recommendations focused heavily on the structure of the intelligence community, with ramifications that reach far beyond the FBI. It called for an independent National Intelligence Director with considerable budgetary, personnel, and managerial responsibilities for intelligence activities of a "national" character, but excluding those of a "tactical" nature and those that support "joint military" operations. The post also would oversee a series of centers, particularly one placed in the Executive Office of the President to perform intelligence analyses and plan operations, but not execute counterterrorism activities. This National Counter Terrorism Center would incorporate and expand on the role of the Terrorist Threat Integration Center by including a warning function and adding net assessment and tasking to its intelligence functions.

Beyond the larger organizational construct, which includes significant changes in budget and congressional structure, another major recommendation directly affects the FBI. **The Commission directly addresses the issue, and discards the option, of creating a separate MI-5-type domestic intelligence organization, but supports institutionalizing a preventive counterterrorism posture within the FBI.** In the Commission's view, this includes:

- **a specialized workforce** consisting of agents, analysts, linguists, and surveillance personnel **steeped in intelligence and national security**
- **cross-fertilization of all senior managers as certified intelligence officers**
- **cross-training of all new agents**, with the option of having an entire career in national security or criminal justice, **advanced training, and mandatory assignments with other intelligence agencies**
- a **team approach that integrates analysts, agents, linguists, and surveillance personnel in the field**
- **field office deputies for national security**
- **recruiting and hiring processes that target relevant intelligence, technical, and language skills**

The 9/11 Commission admonished Congress to re-align the FBI's budget structure accordingly (as recommended by the Academy President in his congressional testimony and included in the House appropriations bill), to regularly review its programs and priorities, to fund the acceleration of secure field office facilities and communications, and to monitor implementation of the FBI's information sharing principles.

Regarding information sharing, the **Commission studies found no national strategy for sharing counterterrorism information. The report recommended incentives to do so and a better balance between security and shared knowledge.** It urged intelligence reporting and production that maximizes the number of recipients of information by **separating sources and methods data and providing wider access to distributed electronic files. Further, it called on the President to coordinate the legal, technical, and policy issues that require resolution to create a trusted information network that enables information sharing.**

TRANSFORMING THE FBI: STATUS OF CHANGES

This section provides a status report on the changes that the FBI has made in response to the recommendations made by a range of sources, including the Academy Panel, the Joint Inquiry, the 9/11 Commission, and others. It is intended to address the overall pace of the FBI's transformation during the last three years, not the specific counterterrorism, intelligence, and security areas that the Panel will address in later chapters.

Changing the FBI’s Strategic Focus

Director Mueller set a new strategic focus for his organization immediately following 9/11 that since has taken root at headquarters, in the field, and among personnel. The overriding priority assigned to the counterterrorism mission is reflected in his instruction to follow every counterterrorism lead to conclusion prior to moving on to other priorities. This is the norm in all FBI field offices, with other mission priorities generally falling into line with those enunciated by the Director. In this sense, the FBI’s strategic refocusing largely has been accomplished.

The FBI’s 2004-2009 strategic plan, released earlier this year, reinforces this focus by serving as a high-level road map of the strategic goals and objectives for its mission. Replacing an outdated 1998-2003 plan, it is the primary guide to the FBI’s efforts to remake and reengineer itself. In addition to forecasting the global environment, it identifies the primary drivers and factors expected to impact FBI operations in the next five years, including demographic, economic, technological, political, and cultural changes. Using this forecast, the plan addresses intelligence, the Director’s eight programmatic priorities, and law enforcement partnerships. It also addresses the human capital and other tools, primarily technology, needed to accomplish the mission.

Specific objectives and priority actions are identified for each area in the strategic plan, but the plan specifies no timetable or measures of accomplishment. Selected performance data are identified for some areas, but no specific performance targets are established. Some FBI-related performance measures are included in the DOJ Performance Plan for 2003, but most critical measures have no identified targets.

Overall, the FBI has given strategic focus to its mission and established clear priorities for its major activities; these are furthered by the detailed strategic plan objectives and priority actions for each mission area. Nonetheless, the lack of specific performance measures in the strategic plan continues to be a deficiency, one that the Panel has identified in its previous reports. Although a separate plan for the Office of Intelligence does identify specific goals and performance parameters for intelligence, it does not supply targets. This shortfall in performance measurement makes it extremely difficult to measure the FBI’s progress in achieving the transformation objectives underlying its actions.

Changing the FBI’s Structure and Processes

Approved in 2002, the FBI’s five new divisional structures have been established. Their components and operations are specified in increasingly elaborate structures and processes, and all are carrying out significant operational or support activities. The Office of Intelligence, added as a major structural component, has made major strides in identifying its strategy, goals, and performance parameters. As this Panel recommended, the office has accorded top priority to defining requirements, particularly with regard to international and domestic terrorism. Two other areas that the Panel emphasized have received more limited attention. Some collection assignments are evident, but more loosely tied to those of the intelligence community, and steps to set up a collection evaluation process remain rudimentary. As recommended, the Office of

Intelligence has remained a reasonably small staff office that aggregates the FBI's management functions related to intelligence, and has divested its terrorist tracking responsibility to the Counterterrorism Division.

In addition, opening most terrorism investigations as intelligence cases has substantially improved the ease of opening such cases and sharing information about them. This process has facilitated field reporting to headquarters, headquarters monitoring of counterterrorism cases on a near real-time basis, and integrating intelligence analysts with headquarters and field agents. This close coupling of FBI analysts and operators is virtually unique to the intelligence community, offering a major improvement akin to the 9/11 Commission's recommendation to create a National Counterterrorism Center that would include analysis and operational planning.

Other structural and process changes are proceeding more slowly. The Panel repeatedly has emphasized the importance of information sharing and the need for an explicit strategy to do so, particularly with respect to counterterrorism information. The Office of Intelligence has articulated clear information sharing principles, and headquarters efforts to share information with the intelligence community and field efforts to do so with state and local are increasingly extensive. Nonetheless, much of this activity appears to be based on temporary interagency personnel exchanges and the heightened consciousness of past failures. Information sharing has not yet been defined as a specific process or set of processes, which raises the potential that the current level of cooperation may never be institutionalized.

The Panel has underscored the importance of the management challenges associated with upgrading the FBI's information technology and specifically recommended strengthening the Chief Information Officer's role and developing an enterprise architecture tied into the FBI's strategic plan, possibly as a technology appendix. The Panel also noted the importance and difficulty of assuring timely implementation of the Virtual Case File case management system, the delivery of which has now been further delayed. The FBI's 2004-2009 strategic plan reflects these objectives and identifies priority actions, such as staffing a core team, defining an enterprise architecture, and developing a strategic plan for information technology with annual plan revisions and a three-year technology refresh cycle. Most important, a new Chief Information Officer, appointed in May 2004 following a year-long search, has been given responsibility for the planning, development, and acquisition management of information technology projects. The Chief Information Officer has promised an enterprise architecture by early 2005. He is also taking steps to improve the utility of the Trilogy backbone network by assuring it can securely handle various levels of classified information and to assure delivery of a viable Virtual Case File case management system, by pilot testing it in the New Orleans field office in the near term, as well as working with the Federal government-wide case management system initiative to lay the ground work for an effective system down the road.

Clearly, the lag in information technology is adversely affecting management functions and the pace of transformation. In field offices we visited, there was widespread disappointment over the delays in implementing the Virtual Case File system. Headquarters divisions and field offices are struggling to address performance measures. Staff attributed deficiencies in performance measurement in part to the lack of automation. Some had placed initiatives on hold pending arrival of Trilogy and Virtual Case File software because of the attention being devoted to those systems.

FBI's former Executive Assistant Director for Administration already had established a series of 40 process re-engineering projects, partly in response to the Panel's prior recommendation that the FBI adopt a systematic management approach that included time schedules, implementation progress measures, performance measures, and an annual external review. The Inspection Division oversees the re-engineering process, though implementation is heavily decentralized. During the last year, GAO has monitored the FBI's progress in completing decision-making and implementation associated with these re-engineering projects. FBI indicates that some projects are lagging, including Trilogy, a security manual pilot project, and career tracks for security personnel.

Delays in meeting personnel needs are the most commonly cited obstacle to faster transformation. Examples of hiring delays in hiring qualified individuals were described in various offices, and the loss of well-qualified candidates because of hiring delays is commonplace. A large percentage of positions were unfilled at the time of our visits. Valuable agent resources were diverted to accelerate background checks on applicants and speed personnel hiring. One would hope that a better personnel planning system will emerge from the 2004 experience.

Changing the FBI's Culture and Values

GAO, which has followed the development of the FBI's strategic human capital plan, currently is reviewing the draft plan which includes an abbreviated version of its objectives and priority actions included in the strategic plan. The Panel also has highlighted the importance of human resource planning as key to the success of the transformation; it has recommended recruitment of individuals with new skills, training improvements, career planning, promotions, and incentives. The FBI's development of a career track for intelligence analysts is an important step, and its Administrative Services Division has made major headway by bringing aboard nearly 2,000 support personnel and more than 1,000 new agents during the last year. In addition, the FBI has established expanded training programs in counterterrorism, intelligence analysis, and security and has continued to reach outside the organization for critical skills.

In recent years, the major personnel increases approved by Congress have clearly strained personnel hiring and clearance processes. Field agents were required to help by completing background investigation, and new agents were drafted to complete personnel files and adjudicate suitability determinations. Additional challenges are apparent in the difficulties of recruiting and retaining analysts given a competitive environment where other intelligence agencies enjoy greater pay flexibilities. Some of these difficulties are addressed in the pending House appropriations bill for the FBI that provides the Director with greater authority in setting pay, bonuses, and allowances.

Other factors, including a freeze on agent promotions for an extended period this year due to a review of the promotion system that was undertaken as a result of a legal settlement, have posed additional personnel strains forcing heavy reliance on temporary duty assignments to fill headquarters needs. The strains also are reflected in hiring some analysts without interviews, rapid turnover of top-level management, limited nationwide recruiting, and the field's limited understanding of performance criteria for counterterrorism agents. Both the FBI's Science and Technology Advisory Board and this Panel have highlighted the rapid turnover in leadership personnel; indeed, the Director's three-year tenure currently exceeds that of any of his headquarters subordinates. Rapid turnover in leadership personnel has highlighted the need for succession planning.[2] The 9/11 Commission's recommendation that the FBI create a career intelligence structure composed of analysts, linguists, agents, and support personnel would place additional demands on the FBI's personnel system. A concerted effort will be needed to construct such a system and ensure that it balances the career structures for personnel both inside and outside the intelligence career structure.

Cultural aversion to technology may be a legacy of the FBI's slow development and adaptation to rapidly evolving computer and communications technology. Increased integration into FBI work processes is critical, for both case management and support services. Younger agents, analysts, and support staff seem better prepared to adopt and utilize information technology in their work. Additional technical training, accompanied by more rapid deployment of useable systems, might help overcome legacy resistance.

Finally, human resources management will require increased attention if the FBI is to develop a skilled and agile workforce that is increasingly capable of meeting transformation needs. Career structures remain to be formed in several areas, succession planning appears limited, and new approaches to recruitment and selection still are being considered. Automating personnel records will help, but even some of these improvements await information technology improvements. Human resources management may require a major investment in additional personnel expertise and technologies to overcome persistent shortcomings and increased demands.

FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

Taken together, this Panel, the congressional intelligence committees, the 9/11 Commission, and other reviews point to several overarching findings, conclusions, and recommendations concerning FBI transformation and the war on terrorism. They include:

- **Domestic Intelligence.** In this era of asymmetric warfare, with its terrorism, cyber, and proliferation dimensions, there is nearly universal recognition of the need for a strong domestic intelligence entity to respond to a variety of threats. This entity requires a robust domestic intelligence collection capability and a strong analytic component covering international and domestic threats to the United States. The iterative processes inherent in the intelligence cycle—requirement, collection, analysis, and evaluation—are fundamental to success. More broadly, proactive, intelligence-driven operations geared toward preventing national security threats—such as terrorism—will come to dominate the reactive after-the-fact response to individual criminal activities that historically has

[2] Also, high turnover in leadership personnel has made it difficult to discern progress and continuity in reform efforts.

dominated federal law enforcement. Increased globalization and threats to national security emanating from abroad argue that this domestic intelligence entity requires strong collaborative relationships with the U.S. foreign intelligence community, foreign law enforcement entities, and a wide array of federal, state, and local law enforcement entities.

- This Panel, like the 9/11 Commission, is convinced that the FBI is making substantial progress in meeting this need and has the will and many of the competencies required to accomplish it. As the 9/11 Commission concluded, the demands for intelligence in the United States must be judiciously weighed against constitutional guarantees of civil liberties and Americans' traditional expectation of privacy. There are benefits to avoiding the significant delay associated with establishing a new MI5-type entity, hiring and training personnel, acquiring a headquarters, establishing a nationwide presence, building institutional relationships with state and local law enforcement at home and with foreign intelligence and other law enforcement abroad, and ensuring the legal and privacy protections accorded Americans. **The Panel recommends that FBI continue to be the key domestic intelligence agency responsible for such national security concerns as terrorism, counterintelligence, cyber, and transnational criminal activity.**

- **Joint Operations.** The FBI's counterterrorism and intelligence activities already rely extensively on joint operations, domestically with other federal, state, and local law enforcement entities, as well as abroad with both foreign law enforcement entities and U.S. intelligence agencies. Law enforcement officers from other federal, state, and local agencies manage their own cases and sometimes run squads that include FBI agents, and detailees from intelligence agencies actively participate in building cases. As the FBI becomes more specialized in national security matters, its reliance on law enforcement and intelligence partners will increase. Jointness is likely to extend to the vast majority of intelligence and law enforcement operations. The FBI will increasingly become a supporting partner to other law enforcement in the investigation of more traditional criminal activities. Joint operations, whether managed by the FBI or other federal, state, and local authorities, are becoming the norm, and this trend is likely to continue. **The Panel recommends that the concept of joint operations, whether through joint task forces or other similar approaches, be applied more broadly to other critical law enforcement activities.**

- **Information Sharing.** Agreement on the need for expanded information sharing is even stronger than that for increased domestic intelligence capabilities. The historic balkanization within intelligence and law enforcement, and between them, is fundamentally incompatible with effective joint intelligence and law enforcement operations. Although 9/11 has served as a powerful and at least temporary antidote to excessive information controls, information sharing remains largely ad hoc and is not recognized in law or regularized in process. Modern, readily available information technologies are underutilized. Strong executive branch leadership, and possibly statutory guidance, may be required to institutionalize information sharing. **The Panel endorses the 9/11 Commission's recommendation that "the President should lead a government-wide effort to bring the major national security institutions into the**

information revolution and coordinate the resolution of legal, policy, and technical issues across agencies to create a 'trusted information network'." The Panel further recommends that the FBI component of this trusted network should be implemented as soon as possible and be extended to state and local law enforcement agencies with respect to counterterrorism information.

- **Technological Investments.** Additional resources and technical staff clearly are needed in the information technology area. Yet resources by themselves are not sufficient; their development and deployment require top-notch technical talent, performed by employees or contractors. In addition, such capabilities can be applied effectively only in combination with the policy and institutional adjustments outlined above. A web-based trusted information network supporting counterterrorism is technologically feasible, but cultural and institutional changes are needed to maximize its application and utilization. **The Panel recommends that the FBI's enterprise architecture and information technology systems under development be broadened to ensure state and local connectivity.**

- **Human Resources.** Additional personnel, specifically agents, analysts, linguists, and technologists, are critically needed. Recruiting, training, and advancement improvements are being developed or under consideration, and career structures are being designed for new skills sets, such as analysts, security specialists, and linguists. Additional efforts in career and succession planning appear necessary given the rapid turnover among higher level personnel. Congress also is to provide the FBI, at its request, the authority to develop a reserve cadre of retired personnel, though planning for this new capability is rudimentary. There is increased interest in creating a multi-skilled intelligence career structure; this entails extremely careful planning to avoid damaging the esprit and professionalism of the FBI workforce. **The Panel recommends that the FBI devote increased emphasis to these human resource planning needs. More specifically, the FBI should develop intelligence career alternatives for analysts, agents, and support personnel. But given the integration of intelligence, operations, and support activities and the extent of proposed cross-training of agent recruits and supervisor agents, the FBI needs to consider alternatives that enable highly flexible and mobile career paths within a single personnel system.**

- **Strategic Management.** Executive leadership must increasingly focus on planning and strategic management, and devote less time to incremental decision-making. Planning should include longer-term resource and personnel considerations with incremental personnel and resource increases addressed in a multi-year context. This is particularly important when planning multi-year acquisitions or technological refreshment given the necessary integration of development, contract management, deployment, and training. At the same time, it is important when planning major personnel increments where recruitment, training, placement, promotion, and career development are required. FBI personnel must be trained in goals and performance-driven system management. **The Panel recommends, at a minimum, that the FBI move to, and Congress support, a multi-year resource planning system for critical technical systems and key personnel skills. In addition, it recommends that the FBI actively seek to broaden the training**

and experience of personnel, including agents, by encouraging enrollment in external management and technical training programs, and by promoting assignments to other agencies.

- **Performance Measurement:** The Panel has repeatedly urged the FBI to develop performance measures addressing its key operational and support functions and activities. It also recommended that such measures should be extended to some of the key strategic management activities of the Bureau, including its re-engineering projects. Specific output, or preferably outcome, measures with specific targets are critically needed in areas such as counterterrorism, intelligence, and security. **The Panel strongly recommends that performance measurement be increasingly incorporated as a fundamental management tool within the FBI.**

This common ground extends beyond the specific tasks assigned to the Panel as part of its current review. It incorporates the Panel's work conducted during the past three years, as well as broader findings of other studies of 9/11, counterterrorism, and the FBI. The following chapters are devoted to counterterrorism, intelligence, and security, reflecting the Panel's specific tasks for this year.

CHAPTER TWO
COUNTERTERRORISM

The World Trade Center bombing in 1993, the Oklahoma City bombing in 1995, and the East Africa embassy bombings in 1998 moved domestic and international terrorism to the forefront of the FBI's investigative priorities. Then-Director Louis Freeh made it a top priority, reassigning agents and analysts to support terrorism investigations. However, no structure existed for managing the counterterrorism program at the national level. Individual field offices conducted terrorism investigations, and responsibility and accountability were diffused among counterterrorism officials there and at headquarters. This arrangement allowed for field offices to assign varying priorities and levels of resources to terrorist groups or threats. It also limited oversight and complicated case coordination by leadership at FBI headquarters.

During this period, the number of joint terrorism task forces in field offices increased to more than thirty, but most focused on domestic terrorism. Resources devoted to counterterrorism investigations surged when crises occurred, but they remained primarily committed to traditional criminal investigation priorities. When resources increased, they were assigned to several priorities, including counterintelligence, critical infrastructure protection, Internet crimes, and political corruption.

Following 9/11, Director Mueller designated counterterrorism as the FBI's number one priority and temporarily reassigned more than 60 percent of its agents to this area immediately following the attacks. He replaced his predecessor's flexible, tiered system with a rank-ordered list of eight program priorities and shifted the organization away from a reactive focus on crime solving and toward a proactive, preventive posture appropriate to counterterrorism.

Director Mueller emphasized national management of the FBI's counterterrorism program. To this end, he reorganized and expanded the Counterterrorism Division, and directed headquarters to assume responsibility for oversight and coordination of counterterrorism field investigations for which he provided increased support and built specialized headquarters capabilities.

To draw upon federal, state, local, and foreign government resources, Director Mueller established a national task force to improve information sharing at the federal level and greatly increased the use of local joint terrorism task forces; at least one was established in each of the FBI's 56 field offices. Headquarters provided support for them, as well as others at satellite offices. Director Mueller increased the number of legal attaché offices to facilitate the FBI's access to information abroad.

THE CURRENT PANEL REVIEW

This chapter details the Panel's review of the FBI's progress in building its counterterrorism program. The review focused on selected elements of the counterterrorism program:

- **Counterterrorism Division.** Structural and process changes were reviewed, with particular emphasis on the new, more active role played by headquarters in the oversight and coordination of counterterrorism cases.

  - **Operations.** Headquarters' counterterrorism operations and staffing were examined. The Panel previously recommended that the FBI's expanded office investigating terrorism financing operations develop a close, coordinated relationship with Treasury's Financial Crimes Enforcement Network. This relationship was specifically addressed.

  - **Analysis.** The Analytical branch of the Counterterrorism Division was reviewed as well, with particular focus on the working relationship between the analytical and operational units. In addition, the adequacy of analyst staffing was examined.

  - **Support Activities.** Activities in two broad functional categories—administrative and logistical support and specialized information support—were examined.

- **Field Structure and Operations.** The structure and operations of counterterrorism programs in the field were reviewed, including the interaction between headquarters and the field. Given the FBI's strategy of working closely with its partners, special attention was given to the joint terrorism task forces and their connection to the organization and management of field counterterrorism programs. The FBI's interaction with emerging networks of federal, state, and local organizations was also reviewed. Field staffing issues included the current demands of counterterrorism work, the impact of temporary duty assignments, and the progress made in building the analyst workforce.

- **Information Sharing.** In its earlier work, the Panel recommended that the FBI adopt an explicit strategy to address information sharing. This year's review focused on several specific areas, such as headquarters' role in sharing information with the field; the role of Field Intelligence Groups; working relationships among analysts, operational units and FBI partners; and the communication of threat information to state and local officials.

THE COUNTERTERRORISM STRATEGY

In its Five Year Strategic Plan, the FBI identifies five goals of the counterterrorism program: (1) prevent terrorist attacks against the United States and U.S. interests; (2) deny terrorists and their supporters the capacity to plan, organize, and carry out logistical, operational, and support activities; (3) pursue appropriate sanctions against terrorists and their supporters; (4) provide incident response and investigative capacity; and (5) identify and respond to WMD threats and fully coordinate the investigative response of the U.S. government to a WMD threat or attack.

In an FBI presentation to the Panel, several measures designed to evaluate its performance of these goals were discussed. With regard to preventing terrorist attacks, the FBI focuses on indicators of its intelligence capability, such as the quality of its informants or "human assets." As for disrupting terrorist organizations, its indicators include identification of known or suspected terrorists and the disruption or elimination of terrorist operations and terrorism-financing operations. The FBI counts terrorism-related arrests and convictions toward the performance of its third goal, appropriate sanctions against terrorists. Performance measures for the last two goals were identified.

In its report to the 9/11 Commission, the FBI outlined the fundamental elements it believes are needed to meet the demands of these five counterterrorism goals. The elements include centralization of leadership (discussed in the introduction); integration of intelligence and law enforcement operations; coordination with other federal, state, and local law enforcement, the intelligence community, foreign governments, and the private sector; information technology; and workforce realignment.

The FBI is working to integrate its intelligence and law enforcement operations on two levels. First, it has established a policy and process for ensuring that its law enforcement capabilities are used to support intelligence-based efforts to identify and disrupt terrorist organizations. As a matter of policy, all counterterrorism cases are opened as intelligence cases. This policy is supported by a new case classification system that eliminates the "criminal" case classification for counterterrorism cases in favor of the intelligence-oriented "international terrorism" classification. The intent of the new policy is to obtain as much current intelligence as possible from a subject, consider the merits and feasibility of recruiting the subject as a long-term source, and consider criminal prosecution only as a last resort. Rather than being the primary goal, prosecution or the threat of it is used as an inducement to solicit cooperation for intelligence purposes or as a means to disrupt terrorist activity. Second, the FBI is building an enterprise-wide intelligence capability intended to drive counterterrorism investigations. Eventually, this capability will enable a more proactive approach to counterterrorism operations. The current approach is necessarily defined by the directive to "leave no lead uncovered."

Coordination with federal, state, and local partners has two components: joint operations through national and local task forces and information sharing to enable joint action. By providing state and local law enforcement with real time database checks to identify known or suspected terrorists, the FBI helps to guide action. It also gives officers access to electronic communication networks and information bulletins, as well as clearances when necessary to obtain classified information. The FBI also shares information with the intelligence community through daily joint briefings to the President and regular briefings to each other. Also, it is working to create secure networks and develop compatible information technology systems to facilitate timely information sharing with intelligence agencies.

Improvements in the FBI's information technology systems support its counterterrorism program because they enable effective and efficient information sharing and analysis. Workforce realignment is another critical element in building the counterterrorism program. The FBI is working to recruit and train personnel with a different mix of skills and experience to meet the demands of the program's goals

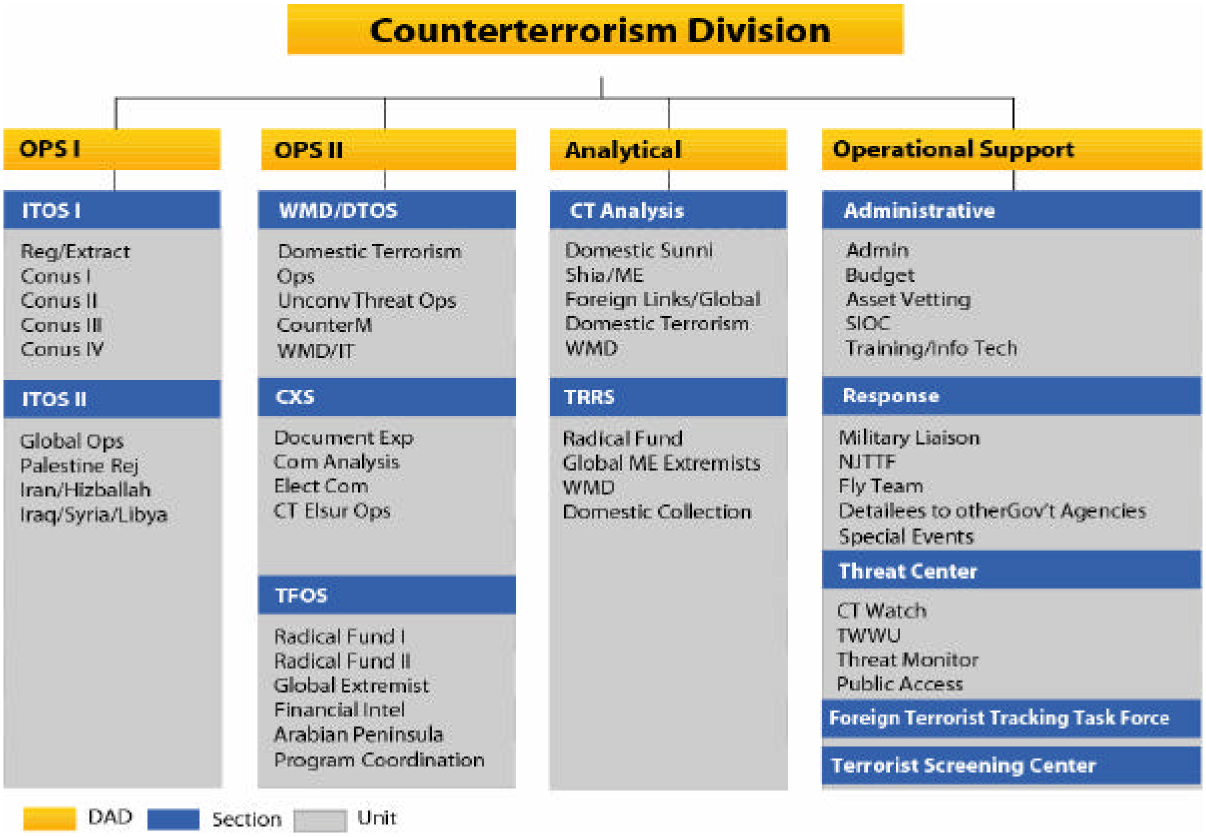
THE COUNTERTERRORISM DIVISION

As depicted in Figure 2-1 below, the Counterterrorism Division has four branches:

- Operations I (OPS I);
- Operations II (OPS II);
- Analytical; and
- Operational Support.

In the past year, a single Operations branch was split into two branches as the number of counterterrorism matters grew. In addition, the analysis function was moved into its own branch to strengthen its organizational identity, notwithstanding the fact that most analysts are distributed in the Operations branches.

Figure 2-1
Organization of the Counterterrorism Division



Operations I and II

The Counterterrorism Division's two operational branches are:

- Operations I is composed of two sections: International Terrorism Operations Section I (ITOS I) and ITOS II. The former covers al Qaeda terrorist activity on a regional basis in the United States and abroad. The latter focuses on four non-al Qaeda groups: Palestinian rejectionist groups, Iran and Hezbollah, Iraq/Syria/Libya, and other global terrorist groups.

- Operations II includes three more disparate sections: Weapons of Mass Destruction and Domestic Terrorism (WMD/DT), Communications Exploitation Section (CXS), and Terrorist Financing Operations Section (TFOS). Operational oversight for WMD is housed with domestic terrorism, despite its international scope.

With the exception of large, complex cases spanning multiple field office jurisdictions, Operations I and II do not manage counterterrorism cases directly. They oversee and coordinate counterterrorism cases run by the field offices, which are required to report major developments in all significant counterterrorism cases. The objective is for the division to support individual case efforts and make sure the "dots are connected" across field offices.

The Division also is developing sophisticated investigative technologies for use in the field. The cost and sensitivity of these technologies were presented as factors for supporting a special headquarters role in counterterrorism. The Division is taking a phased approach to offering these capabilities to ensure that higher priority investigations receive immediate support. It wants to avoid inducing demand that cannot be met until new personnel are trained.

The Terrorism Financing Operations Section, housed in Operations II, is an operational and coordinating entity. It directs terrorism financing investigations and works jointly with partners to block and freeze assets. However, its primary role is to coordinate and support the financial components of terrorism investigations conducted by ITOS I and II. This section establishes overall initiatives and policies on terrorist financing matters and coordinates with a National Security Council committee on terrorist financing, DOJ, and the financial services sector. Its staff coordinates with the joint terrorism task forces. Like the Analytical branch discussed below, the section assigns its analysts to headquarters' operational sections while retaining management control.

The Treasury Department's Financial Crimes Enforcement Network (FinCEN) is an important source of information for the Terrorism Financing Operations Section. FinCEN collects data on a range of financial transactions reported by financial institutions in compliance with the Bank Secrecy Act. It also receives financial transaction data from financial intelligence units maintained by other governments, which have agreements with the United States. FinCEN makes these data sets available to the FBI and other federal law enforcement agencies for analysis. The FBI is the largest customer and has briefed financial intelligence unit representatives on its goals and needs. FinCEN also does limited data analysis to improve its collection process and to identify trends and patterns in financial transactions, though this analysis is not focused on terrorist financing. Further, it provides analytic support to law enforcement agencies for large, complex cases. The FBI has developed a close working relationship with FinCEN, having assigned an agent to it full time. The FBI plans to place three analysts there, as well. FinCEN staff report that the FBI is far more open and willing to engage FinCEN in its efforts since 9/11.

Analytical

The Counterterrorism Division's Analytical branch includes two sections:

- Counterterrorism Analysis, which supports Operations I and II; and

- the Terrorism Reports and Requirements Section (TRRS).

The Division has pursued a conscious policy of integrating analysts with their operational counterparts in order to facilitate information flow and increase the resonance between the two. At the same time, the management of analysts is retained within the Analytical branch to cultivate an independent cadre that supports operations but does not become dominated by its demands. Some tension between analysis and operations is evident, but embedding the analysts with special agents in operations is judged to be effective.

The Terrorism Reports and Requirements Section is responsible for terrorism intelligence requirements and reporting. It is trying to build field capacity for reporting terrorism-related information, specifically training analysts to identify and report terrorism-related information in a standard format, called intelligence information reports. Currently, its staff prepares most of these reports on behalf of the field. After field analysts are hired and trained in reporting, they will prepare most of them.

Operational Support

This branch's activities fall into two broad categories:

- administrative and logistical support activities performed by the National Joint Terrorism Task Force and the Fly Team

- specialized information support activities performed by the Division's counterterrorism watch center (CT Watch), the Terrorist Screening Center, and the Foreign Terrorist Tracking Task Force

Formed as an ad hoc group following 9/11, the National Joint Terrorism Task Force was formally created in July 2002. Composed primarily of federal agencies but also including representatives of the New York Police Department and the Washington Metropolitan Police Department, it provides a forum for agencies to coordinate and share information at the national level. It also coordinates counterterrorism projects ranging from intelligence sharing on terrorist recruiting in prisons to aggregating information on ports and railroads. For example, Project Tripwire seeks to establish information gathering and reporting mechanisms ("tripwires") to indicate terrorist activity in various sectors. These projects are coordinated with or executed by local joint terrorism task forces, which receive administrative and financial support from the national task force. The National Joint Terrorism Task Force also provides limited funding support for state and local participants, sets criteria for establishing new joint terrorism task forces, and is beginning to evaluate their performance.

Originally conceived as "flying squads," the Fly Team has evolved from discrete, standing teams to a dedicated pool of personnel with an array of expertise, from which groups may be assembled to respond rapidly to crisis needs, special events, and high priority investigations. As of September of 2004, Fly Team personnel have been sent on 53 deployments: 16 domestic and 37 overseas. This team is independent of the field to ensure its continual availability and to facilitate information flow to headquarters. Groups of varying size and composition may be assembled for specific assignments in the United States and abroad, involving as many or as few agents as needed. The current Fly Team has 20 personnel in place, with forty as the long-term goal. In most cases, the Fly Team does not run investigations, but helps to set them up. It ascertains the expertise and equipment needed for specific situations, often conducts initial forensic work and interviews, and may develop the infrastructure, such as a command post or file structure to manage a case. For example, a Fly Team deployed to a legal attaché office abroad may do an initial assessment that provides background knowledge about activities of concern.

The Fly Team has alleviated, but not fully eliminated, the need for investigative support from the FBI's largest field offices, which traditionally provide support investigative, polygraph and technical—to the legal attaché offices. Some of these offices also maintain similar rapid response teams. Groups assembled by headquarters draw on these field teams. For example, members may be drawn from the New York field office if investigations relate to al Qaeda, the area of New York's traditional purview and expertise. Members are drawn from the Washington field office if other terrorist groups are involved.

Specialized information support is provided by three key components: the Terrorist Screening Center, CT Watch, and the Foreign Terrorist Tracking Task Force. They provide timely information on known and suspected terrorists to federal, state, and local officers to guide and coordinate operational responses to field encounters.

- The Terrorist Screening Center was created by Presidential directive in September 2003 to consolidate information on known and suspected terrorists from the multiple watch lists maintained by federal agencies to create a single terrorist watch list[3] and to provide 24/7 operational support for law enforcement, consular officers, and other federal screeners. The FBI was directed to lead this effort in December 2003. The center performs three functions:

    - It reviews the nomination of potential terrorists (name and identifying information) to the watch lists from different government agencies.

    - It maintains a terrorism screening database of known or suspected terrorists. This database draws on information developed by the Terrorist Threat Integration Center, which receives and merges information on known and suspected foreign terrorists, and the FBI's Terrorist Watch and Warning Unit, which develops and maintains the list of domestic terrorists.

[3] The goal of the Presidential directive was to create a single *terrorist* watch list to be used by all federal screeners, not to replace existing federal agency watch lists. Federal agencies maintained and continue to maintain separate watch lists to meet the distinctive goals and objectives of their respective missions.

- It assists police, border, and consular officials in matching identities with a known or suspected terrorist.

For example, when an official encounters a suspicious individual and runs the subject's name and other identity information through the National Crime Information Center system, the information is automatically checked against the Terrorist Screening Center's own database. If the check results in a match, the official automatically receives prepared instructions, such as "arrest," "detain," or "question the individual." The official is also instructed to call the center's 24/7 call center for assistance in identifying the individual. The official then is connected to CT Watch, which coordinates action through local joint terrorism task forces.

The Terrorist Screening Center has succeeded in developing a consolidated database of known or suspected terrorists. This database has the names of known or suspected terrorists from ten of the twelve federal watch list databases described in the April 2003 GAO report, "Information Technology: Watch Lists Should Be Consolidated to Promote Better Integration and Sharing." However, the quality of this list is an issue. The database includes over one hundred thousand names, and although the Terrorist Screening Center applies a relatively rigorous standard to the inclusion of names in the database, requiring at least two identifiers in addition to the name, the accuracy and completeness of the list is a continuing challenge. Another problem is the use of the list by other federal agencies and the private sector, particularly the airlines. For instance, the Transportation Security Administration uses its own lists, a No-Fly list and a Selectee list, although names from these lists are included in the FBI database when they meet the FBI's standard. These lists are checked by the airlines to screen passengers.

- CT Watch is a command center that refers action items to the local joint terrorism task forces to provide a coordinated response to information on suspects identified by the Terrorist Screening Center.

- The Foreign Terrorist Tracking Task Force assists the Terrorist Screening Center in identifying and tracking known and suspected terrorists through searches on a range of government and commercial databases. It searches these databases for information needed to confirm the identity of persons, whose records may contain inaccurate or incomplete information. This task force also assists the joint terrorism task forces in tracking known and suspected terrorists based on government interactions and/or commercial transactions.

Staffing

The number of positions funded and the number of personnel actually on board at headquarters are summarized below.

Table 2-1: Staffing of the Counterterrorism Division
(as of June 2004)

Funded	On-board
507 Special Agents	301 Special Agents
523 Analysts	304 Analysts
316 Support	180 Support

In addition to this permanent staffing at the Counterterrorism Division, the field is supplying personnel on temporary duty assignments, including 149 special agents and 37 analysts. Also, approximately 40 detailees from other agencies were assigned to the National Joint Terrorism Task Force. The Division attributes its reliance on temporary duty assignments to the promotions freeze that lasted for much of Fiscal Year 2004, which made it impossible to promote field agents and induce them to take positions at headquarters.

With regard to filling analyst positions, FBI staff attributed delays to the shift from old hiring processes to new ones and the pitfalls of the former. They also spoke to the major steps in the new process and how it is working. Upon receiving an employment package, an applicant has 10 days to return it on-line to the Administrative Support Division. The application then goes to the Background Investigation Contract Service, which assigns investigators to do the requisite background check. The Counterterrorism Division estimated that it considers 10 to 15 applicants for every applicant hired. It cited polygraph problems and competition from other agencies as the primary reasons for this. The Administrative Services Division reported that counterterrorism applicants receive priority attention, and that it is completing its work on applications for most counterterrorism positions in fewer than 90 days.

FIELD STRUCTURE AND OPERATIONS

FBI field offices vary greatly in size, structure, and organization. Project staff visited offices ranging from fewer than 70 to more than 700 agents. The geographic distribution of agents within field office jurisdictions and between the main field office and satellite offices, referred to as resident agencies, also varied substantially. Some field offices assign most of their agents to resident agencies, while others assign most of theirs to the headquarters office. In the Springfield, Illinois office, less than 10 percent of its agents are assigned to the main field office; the rest are assigned to nine resident agencies spread across the state. In fact, one resident agency is larger than the headquarters office. In the Chicago field office, a very large office in a relatively small geographic area, agents are concentrated in Chicago area locations; only a small number are located in one distant resident agency.

Counterterrorism field operations are organized into squads, the number of which varies according to the amount and diversity of activity in a field office's jurisdiction. Larger field offices, such as Los Angeles, maintain counterterrorism squads for each major terrorist group, as well as for domestic terrorism and terrorist financing, while smaller field offices combined such responsibilities across two to three squads. Larger offices often maintain a separate squad to follow up immediately on counterterrorism leads, allowing other squads to focus on longer term efforts, free from demands for immediate action. At the smaller offices, immediate follow up usually is part of the overall workload of counterterrorism squads working international terrorism. The resulting distribution across squads helps to limit the burn out of agents devoted solely to this task in "reactive squads."

The Field Intelligence Group is intended to coordinate intelligence in the field, linking operational field units and FBI partners in an integrated intelligence system. However, these groups still are in the formative stages; their organization and management and working relationships with field offices and organizations are being worked out. FBI headquarters has allowed field offices considerable latitude in how they choose to organize their Field Intelligence Groups, extending to how to integrate the work of analysts and operations. Some offices are withdrawing analysts from operational units to help create an independent intelligence group. This approach reflects the demands of creating an identity for a new function and the still small number of analysts, which limits the groups' capacity to deploy analysts to operational units and maintain a dedicated group.

Within this wide range of field structures, five elements of FBI counterterrorism operations were examined:

- headquarters' role in counterterrorism case management and its effect on field operations
- the role of the Joint Terrorism Task Forces and their relationship to the organization and management of field counterterrorism operations
- state and local organizations involved in counterterrorism operations and their interaction with the FBI field units
- the U.S. Attorneys' offices and their role in coordinating among the FBI and other federal, state, and local law enforcement agencies
- staffing of field counterterrorism investigations

Impact of Headquarters' Directives on Field Operations

Field office staff appreciated the need for headquarters to take a more active role in its operations and expressed a generally positive view of this involvement. Smaller offices, which lack the experience and expertise to conduct complex counterterrorism cases, related especially positive experiences given that headquarters often can provide needed legal, technical, and analytical assistance, as well as expertise in case management provided by Fly Teams. Staff at the larger offices, which have more specialized resources at their disposal, considered headquarters support to be less relevant.

On the other hand, several field offices expressed concern about the frequency and breadth of special headquarters requests to follow up on broad leads, such as suspicious customer inquiries, purchases or rentals of trucks, scuba equipment, and the like. Depending on the specific request and the size and other characteristics of the office, these requests can be quite time consuming. Consequently, these requests can divert considerable manpower from ongoing counterterrorism operations.

Counterterrorism Field Operations and the Joint Terrorism Task Forces

The field counterterrorism operations are organized within the FBI's Joint Terrorism Task Forces. These task forces encompass all FBI agents assigned to the counterterrorism program in the field; no counterterrorism cases are opened outside them. Each field office was directed to establish a Joint Terrorism Task Force. Many field offices have received support for additional "annex" task forces at their resident agencies. A list of Joint Terrorism Task Forces as of September 2004 is provided in Table 2-2 below.

Table 2-2. Joint Terrorism Task Force Locations*

- **Albany**
- **Albuquerque**
- **Anchorage**
- **Atlanta**
- **Baltimore**
- **Birmingham**
- **Boston**
  - Portland (ME)
  - Providence (RI)
  - Springfield
- **Buffalo**
  - Rochester
- **Charlotte**
- **Chicago**
- **Cincinnati**
- **Cleveland**
  - Toledo
- **Columbia**
  - Greenville
- **Dallas**
  - Lubbock
  - Plano
- **Denver**
  - Colorado Springs
- **Detroit**
  - Grand Rapids
- **El Paso**
  - Midland
- **Honolulu**
- **Houston**
  - Beaumont
  - Conroe/Bryan
  - Corpus Christi
  - Texas City
- **Indianapolis**
  - Bloomington
- **Jackson**
- **Jacksonville**
  - Pensacola
- **Kansas City**
  - Wichita City
- **Knoxville**
- **Las Vegas**
- **Little Rock**
  - Fayetteville
- **Los Angeles**
  - Long Beach
  - Santa Ana
  - Riverside
- **Louisville**
  - Covington
  - Lexington
- **Memphis**
  - Nashville
- **Miami**
  - West Palm Beach
- **Milwaukee**
  - Madison
- **Minneapolis**
- **Mobile**
  - Montgomery
- **New Haven**
- **New Orleans**
- **New York**
- **Newark**
- **Norfolk**
- **Oklahoma City**
  - Tulsa
- **Omaha**
  - Des Moines
- **Philadelphia**
- **Phoenix**
- **Pittsburgh**
  - Charleston (WV)
  - Clarksburg (WV)
  - Erie
- **Portland**
- **Richmond**
  - Charlottesville
- **Sacramento**
  - Fresno
- **Salt Lake City**
  - Helena (MT)
- **San Antonio**
  - Austin
  - Brownsville
  - Laredo
  - McAllen
- **San Diego**
- **San Francisco**
- **San Juan**
  - Virgin Islands
- **Seattle**
  - Everett
  - Inland NW
- **Springfield**
- **St. Louis**
- **Tampa**
  - Orlando
- **Washington DC**

* One Joint Terrorism Task Force is located at each of the FBI's 56 field offices. The location of these field offices is presented in **bold**. Additional Joint Terrorism Task Forces are located at satellite offices of some of the 56 field offices. These satellite offices, what the FBI calls "resident agencies," are presented in plain type, indented below. Many field offices have geographic jurisdictions that cover more than one state. Where satellite offices are located in a state different than the field office location, the state is presented in parentheses.

In the field, no distinction is made between task forces located at the main field office and those at resident agencies. For instance, the Los Angeles field office refers to its four task forces, each of which has its own supervisor or coordinator.

Task forces vary in membership and size, though they appear to be highly correlated with field office size. Non-FBI task force members largely are sworn officers drawn from law enforcement organizations. The specific mix depends on the interest, relevance, and resources of federal, state, and local law enforcement organizations operating in the service area. Other federal agencies offer complementary legal authorities and expertise. State and local agencies bring complementary legal authorities as well as local knowledge and contacts. The participation of smaller sheriff offices and police departments often is limited by available resources and qualified personnel.

Task force participants usually run cases, some independently and others jointly with FBI agents. Non-FBI participants sometimes manage squads that include FBI agents, but all are federally deputized. Local police and sheriff's offices often, though not solely, follow up leads and work cases centered in their home jurisdictions.

Immigration agents' participation in the Joint Terrorism Task Forces predates the creation of DHS and its Bureau of Immigration and Customs Enforcement (ICE). Almost immediately following 9/11, the Immigration and Naturalization Service assigned 1,000 agents to assist the FBI, and staff interviewed consistently emphasized the importance of these legacy agents now assigned by ICE. Many counterterrorism cases depend on the legal authority of ICE and the expertise of the agents who bring practical knowledge of immigration databases and legal authorities. Rather than special training for agents in this area, the FBI relies on close working relationships with ICE field representatives. Over time, it is expected that FBI agents will learn the basics of immigration law, but continue to rely on ICE personnel for guidance on complex matters.

Every field office visited practiced an inclusive approach toward FBI partners participating on Joint Terrorism Task Forces. Partners received access to FBI intelligence and analytical tools, such as case files and the Investigative Data Warehouse. Overall, the task forces have effectively integrated FBI partners into a joint operation. Yet one possible exception concerns ICE. FBI headquarters staff reported instances where ICE headquarters directed agents to act independently of FBI leadership on cases it deemed to be within its jurisdiction. The FBI is concerned that overly zealous immigration and customs enforcement will undercut its collection operations, which are driven increasingly by prevention, not enforcement. These operational leadership conflicts were not mentioned by field office staff though they were not asked directly about it. They spoke well of ICE task force members, most of whom were legacy immigration agents. Very few legacy customs agents served on the Joint Terrorism Task Forces visited; one frequently cited reason was insufficient staffing of customs enforcement staff at ICE offices.

One concern about the management of counterterrorism programs in the field relates to the evaluation of agent performance. In an effort to institutionalize the priority on intelligence gathering in the field, the FBI has proposed criteria—developing sources and the quality of information they provide—for evaluating the performance of counterterrorism agents. However, new intelligence-related performance criteria are not yet recognized in the field. Field staff was generally unable to articulate any specific criteria to be used to evaluate the performance of agents working counterterrorism.

A potential morale problem among field personnel in counterterrorism and other programs stems from the repeated delays in the implementation of Virtual Case File (VCF), the new automated case file system. Agents at every field office visited, though enthusiastic about the potential of VCF, expressed disappointment in the repeated delays in its implementation. Agents have been sent to training only to find that they will likely need to attend yet more training as the skills they learned will have been lost by the time VCF finally arrives.

State and Local Operations

FBI field offices often operate on a crowded field of organizations that may complement or conflict with FBI counterterrorism efforts. Field visits found state, local, inter-agency, and intergovernmental entities that conduct these operations, including the Maryland Coordination and Analysis Center, Illinois' State Terrorism Information Center, the California Terrorism Intelligence Center, and the California State Terrorist Warning Center.

These state organizations vary in mission, activities, and capabilities, and working relationships with FBI field offices. Maryland's center, run by the Maryland State Police, is coupled electronically and coordinated virtually instantaneously with the FBI's Baltimore field office. Illinois' center, also run by the state police, is not as tightly coupled with the FBI field offices. California presents a more complicated picture. At the time of our interviews, two state organizations were present on the field. The California Terrorism Intelligence Center was created by the California Department of Justice, which provides criminal investigators and analysts from its agencies to pursue counterterrorism operations. The center, which established its own task forces operating separately from the Joint Terrorism Task Forces, soon will be absorbed into the California State Terrorist Warning Center, which the state's Highway Patrol recently created.

With the exception of the California Terrorism Intelligence Center, these organizations play an intermediary role, connecting state and local law enforcement officers to the FBI's Terrorist Screening Center, CT Watch, and local Joint Terrorism Task Forces. Many police officers cannot conduct National Crime Information Center checks from their cars; nor can their dispatchers. The Maryland, Illinois, and California entities maintain call centers that provide this access, as well as to other databases against which officers can do checks. If a match appears, the officers receive relay instructions, the matter is referred to the Terrorist Screening Center, with the response coordinated through CT Watch.

Efforts are also underway to develop analytic capabilities to complement these organizations' watch and warning role. In Maryland's case, these capabilities are being developed in conjunction with the FBI Baltimore office's Field Intelligence Group, and Maryland State troopers staff the group's strategic analysis unit. Similarly, Illinois plans to develop its own analysis unit; the FBI's field offices there are working together to place an analyst at the center, whose efforts are closely tied to homeland security planning. The Illinois center participates in the Illinois Terrorist Task Force, which coordinates the expenditure of DHS grants to the state. In California, the Highway Patrol has created the State Terrorism Threat Analysis Center to provide a central, state-level analysis capability that ties in with the FBI's Field Intelligence Groups and regional threat analysis centers being proposed.

Also in California, sheriffs have sponsored the creation of terrorism early warning groups. There are four working groups in various stages of development, one for each FBI field office jurisdiction: Los Angeles, San Diego, San Francisco, and Sacramento. The most developed one is located in Los Angeles; its participants include the Los Angeles Sheriff's Office, Police Department, County and City Fire Departments, County Health Department, the FBI, DHS, as well as associations representing Los Angeles County's municipal police chiefs and fire chiefs. The core of the terrorism early warning group is conceived as an intelligence unit that will support planning for incident response and management. It is staffed by detailees from participating agencies, through whom it draws on expertise and intelligence. The terrorism early warning group, funded partially by DHS funds, participates on the county's grants task force, which helps to coordinate grant monies. Steps are being taken to create a regional intelligence center using a partnership that includes the terrorism early warning group in LA, the FBI, the Joint Drug Intelligence Group, a long-standing regional interagency intelligence group sponsored by the FBI, and LA Clear, a group formed to manage jurisdictional conflicts among agencies working drug cases in the area. This center, the Joint Regional Intelligence Center, will cover the five counties in the FBI Los Angeles field office's jurisdiction.

Our field visits suggest that cooperation and coordination between state and local operations and the FBI are accepted as necessary and useful. However, interviews with officials at FBI headquarters identified state and local counterterrorism operations that have actively resisted coordination with the FBI, most notably, the New York Police Department's Intelligence Division and the New Jersey Governor's Office of Counterterrorism. Both organizations have sought to run their own independent counterterrorism operations and have resisted sharing information with the FBI. The Panel believes that this lack of coordination could undermine a concerted counterterrorism effort.

Anti-Terrorism Advisory Councils

Immediately following the 9/11 attacks, U.S. Attorney General John Ashcroft directed each U.S. Attorney's office to create anti-terrorism task forces, to pursue counterterrorism efforts involving appropriate federal agencies, as well as state and local law enforcement and prosecutors. Due to confusion over the respective roles of the U.S. Attorneys' task forces and the FBI Joint Terrorism Task Forces, the Attorney General later directed the US Attorneys' task forces to avoid involvement in operations and changed the name of these bodies to Anti-terrorism Advisory Councils.

Although little guidance has been provided on the specific mission of these councils, they can wield considerable influence and appear to play various roles. Some perform a coordinating role by managing jurisdictional conflicts among agencies and levels of government involved in counterterrorism operations. Others serve an educational and training role. Also, most appear to play a useful role in information exchange among participating agencies.

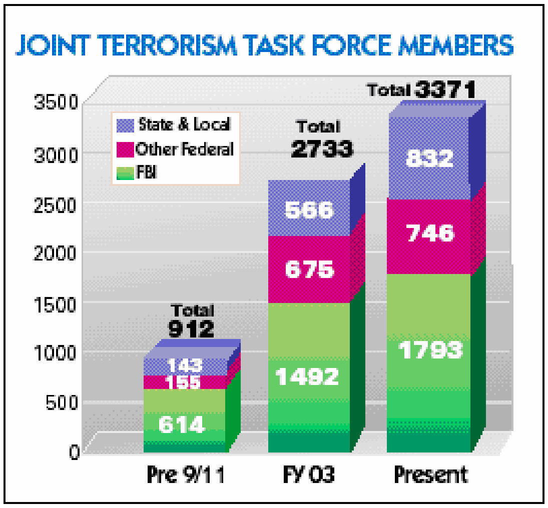
The effectiveness of the Anti-terrorism Advisory Councils in the areas visited varied considerably. In several FBI jurisdictions, they served as a forum for the various players in counterterrorism operations to come together, share information, and resolve disputes; the chairs were considered active and influential. In other jurisdictions, they were considered just one of many organizations in the mix, not necessarily a vital player. In some cases, Joint Terrorism Task Force's executive committee, not the council, appeared to play the coordinating role.

The U.S. Attorney's offices, however, are uniquely positioned to act as relatively neutral brokers to coordinate and manage disputes among the various federal, state, and local agencies involved in counterterrorism operations. However, there is little formal authority or organization behind the council's chair, and the success of individual councils depends largely on the individual Assistant U.S. Attorneys chairing them. Of course, local circumstances will shape their influence and effectiveness. Where there are multiple U.S. Attorneys within the jurisdiction of a FBI field office, the council's role may be less significant.

Staffing

As shown in Figure 2-2, the number of FBI field agents assigned to counterterrorism has almost tripled since 9/11, from 614 agents prior to the 9/11 attacks to 1,793 agents by April of 2004. These agents are complemented by 1,578 non-FBI law enforcement officers participating full time in Joint Terrorism Task Forces, 746 from other federal agencies and 832 from state and local agencies. Federal participation has increased almost five-fold since 9/11 and state and local participation has increased by even more. These numbers indicate that the FBI has been successful in drawing on other federal, state, and local organizations to assist its counterterrorism program.

Figure 2-2
Participation in Joint Terrorism Task Forces



Source: FBI, Report to the 9/11 Commission, April 2004

Nonetheless, field staff reported substantial deployment rates of between 10 and 20 percent above the FBI's funded staff levels, and suggested that these rates will continue as more investigations uncover still more work. In some cases, rates exceeding funded staff levels coincide with temporary duty assignments to headquarters and abroad. Such assignments generally were reported to be a significant burden on field staff. These assignments often take the most experienced agents in management positions. This has resulted in shortages of supervisors to manage counterterrorism squads. At least one office is considering "informal splits," in which half of a large squad is placed under an FBI agent supervisor with the other half under a non-FBI task force officer. Until counterterrorism work levels stabilize and workload demands are better understood, increased use of experienced task force officers may prove to be a useful approach.

INFORMATION SHARING

The FBI is developing processes for sharing information internally and with other federal agency, state, local, and international partners, to extend its workforce and capabilities. The Panel reviewed information sharing processes between headquarters and the field, the roles of the Joint Terrorism Task Forces and Field Intelligence Groups, the evolution of state watch and warning systems, the roles of FBI and DHS in communicating threat information to state and local officials, and the FBI's information technology infrastructure.

Headquarters' Role

The FBI has instituted procedures for field offices to routinely report to headquarters on terrorism cases, specifically major developments in all significant cases. Major developments include undercover operations employing sophisticated investigative technologies, and case significance is determined with reference to such indicators as the number of surveillances allowed by the Foreign Intelligence Surveillance Court, the use of sophisticated investigative techniques, and the magnitude of the threat.

Regular case reporting from the field to headquarters has become a critical component of the centralized management of terrorism matters. It supports daily briefings to the Director and the President, and is designed to reinforce regular sharing with headquarters and sharing among field offices through headquarters. In addition to this reporting, the Terrorism Reports and Requirements Section (TRRS) is developing the FBI's field capacity to report terrorism-related information. Pending the hiring and training of field analysts, section staff at FBI headquarters is writing most of the intelligence information reports on behalf of field offices and legal attaché offices. Currently, the field does not disseminate reports directly until section staff review them, which reflects the need for quality control until reports officers are deployed and trained.

The section also disseminates these reports based on standard distribution lists and special distributions tailored to internal and external requests. The dissemination preferences of external agencies are honored. For example, CIA does not want the reports disseminated directly to its field stations; it handles its own internal dissemination. However, all reports currently are distributed to all FBI field offices, even if the subject of the reports bears little or no relationship to the circumstances of a specific office. As might be expected, field staff describes many reports as having limited practical value; they are too general to inform action.

Information Sharing in the Field

Although Field Intelligence Groups will be the primary vehicle for sharing information with FBI field offices and partners, they are just now taking shape. In the meantime, the Joint Terrorism Task Forces have been the principal channel for sharing terrorism intelligence with partners in support of joint operations. Moreover, other federal, state, and local investigators are detailed to the task forces in no small measure to provide their leadership with information on terrorist activities and counterterrorism operations in their home agency's jurisdiction. This fact, which FBI staff recognizes, reinforces the task force's de facto role in information sharing.

Field Intelligence Groups focus on sharing terrorism intelligence with task force members. As they mature and information sharing becomes more automated, they will handle terrorism intelligence sharing not only with task force members, but with a wide range of tribal, state and local law enforcement agencies in a field office's jurisdiction, many of which do not participate in the task forces. One Field Intelligence Group represented a forward-looking approach to information sharing, having already opened channels to state and local law enforcement beyond the task force by having agents introduce analysts to relevant players in the field.

The state counterterrorism organizations, discussed earlier, have the potential to extend the reach and effectiveness of FBI operations and intelligence. However, their capabilities, policies and procedures vary in three areas: receiving information, tracking incidents to resolution, and state and local law enforcement reporting practices. First, some organizations maintain call-in lines only for law enforcement officers, while others do so for the general public as well. In the case of the former, calls from the public likely would come in through 911 and then be routed to state and local law enforcement dispatchers. This approach relies on state and local law enforcement to respond initially to tips, which lessens the demands on the Joint Terrorism Task Forces as state and local law enforcement act as a filter. This is the explicit strategy in some cases. The challenge is to ensure that real leads do not get filtered out.

Second, jurisdictions vary in the completeness of tracking systems. The FBI has developed and implemented a database system, called Guardian, to track incidents and leads to final resolution. However, some state intermediaries may not have tracking systems or may have databases that are not synchronized with the FBI field office database. In short, data points may be missed, undermining intelligence efforts and policing. For instance, if a police officer interviews a subject taking pictures of a water tower, he or she will not necessarily know whether the subject has been encountered previously for similar reasons. The FBI seeks to facilitate and encourage reporting when implementing Guardian's next phase, which will make database access available to state and local law enforcement in a web-based format.

Third, incidents are not consistently reported even when tracking systems are in place. In some jurisdictions, state and local law enforcement officers may not report incidents if they are resolved in the field. Again, data points may be lost.

The Maryland Coordination and Analysis Center offers a good example of a state watch and warning system. It has moved aggressively to market itself as the place to call with terrorism leads and tips, maintaining a call-in line for police officers and a separate hot line for the general public. It has worked to educate state troopers and local law enforcement to call in possible terrorism-related incidents. As discussed earlier, the center closely coordinates with the FBI's Baltimore field office. Incidents reported through it are tracked using FBI's Guardian database system.

The FBI shares responsibility with DHS for communicating threat information to state and local officials. DHS communicates threat information to state and local officials, except law enforcement, and the FBI communicates threat information only to law enforcement officials.[4] This approach has been a source of confusion and consternation at the state and local level, especially for law enforcement which receives threat information both from the FBI directly and DHS indirectly through government leaders. Conflicting information, or even the same information communicated by different sources at different times, can lead to confusion over the nature of the threat or the response. Efforts to develop consistent tracking systems also may suffer. DHS currently is promoting its own independent tip line for the public and its own database of threat information to state and local governments.

FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

The FBI has greatly strengthened its counterterrorism program through major efforts in several key areas. These include centralization of leadership; integration of the FBI's intelligence and law enforcement operations; coordination with other federal, state, and local law enforcement, the intelligence community, foreign governments, and the private sector; information technology systems; and workforce realignment. The FBI's achievements in these areas, as well as remaining challenges and recommendations are discussed below.

The FBI has centralized its leadership and built headquarters management capabilities to enable an enterprise-wide approach to the counterterrorism program. It has made substantial progress in this effort. A key element has been the new and more active role played by headquarters in overseeing and coordinating counterterrorism cases in the field. Field staff was generally positive about headquarters' performance, often noting that headquarters facilitated their efforts.

The integration of analysts with operations in the Counterterrorism Division at FBI headquarters is a key element supporting the success of the new role of headquarters in the oversight and coordination of counterterrorism operations in the field. The collocation of analysts with operational units at headquarters has enabled more effective exchange of information among analysts and operations management. Operations management has ready access to vital information and analysis and analysts are closely aligned to the circumstances and needs of operations, allowing them to provide useful information and insights. At the same time, Division management has recognized the importance of cultivating an independent analyst cadre that will support operations but not be dominated by operational demands. To this end, the analysis function was given its own branch and management.

The FBI's counterterrorism program is defined by the objective to "leave no lead uncovered." The FBI has clearly spared no effort to realize this objective. However, there is reason to believe that the FBI's efforts to achieve this objective could be improved with respect to how the Counterterrorism Division handles requests to the field. Field offices receive frequent requests from headquarters to follow up on broad leads, such as suspicious customer inquiries, purchases,

[4] This division of responsibilities was established in the March 4, 2003 Memorandum of Understanding on Information Sharing between the FBI and DHS.

or rentals. Depending on the lead and the size of the jurisdiction, these requests can be quite time consuming and divert considerable manpower from ongoing counterterrorism operations. Although the scope and timeframe for responding to these requests often are negotiated, requests and responses should not be left to chance. **The Panel recommends that the process by which FBI headquarters levies special requests on the field be reviewed to determine whether it might be managed so as to minimize disruption to ongoing counterterrorism cases.**

The FBI has improved and expanded headquarters capabilities to direct and support terrorist financing investigations. Before 9/11, terrorism financing operations was just one among several priorities competing for the time and attention of staff in a unit that handled financial investigations generally. Following 9/11, a separate section was created to handle only terrorist financing operations and it was funded in accordance with it new priority. The Terrorist Financing Operations Section has enjoyed considerable success. Much of the FBI's success in moving against terrorist organizations has followed from investigations of financing.

An important part of the FBI's strategy for dealing with terrorist financing has been to build a strong relationship between the Terrorist Financing Operations Section and Treasury's FinCEN. Through this section, the FBI has sought to communicate its goals and data needs, and has worked with FinCEN to evaluate financial data sets and to pursue large terrorist financing cases. In keeping with this Panel's earlier suggestion, the Terrorist Financing Operations Section has clearly developed a close working relationship with FinCEN, that appears to be working well.

In addition to operations and analysis capabilities, the Counterterrorism Division at FBI headquarters has built important operational support capabilities. These activities include logistical and administrative support and special information support. With regard to the former, the creation of a Fly Team has allowed headquarters to provide timely and expert support to field offices in the U.S. and to partners abroad. With regard to the latter, the FBI, through its Terrorist Screening Center and Counterterrorism Watch, is able to provide state and local law enforcement and federal screeners with real time database checks to identify known or suspected terrorists, to guide actions and to coordinate timely responses by local Joint Terrorism Task Forces. However, there are some shortcomings in this system; the quality of the Terrorist Screening Center database is a continuing challenge and the database is not being used by all federal and private screeners. **The Panel recommends the rapid development of a single watch list of known or suspected terrorists and its use by all counterterrorism screening operations.**

The FBI has taken important steps to integrate its law enforcement and intelligence operations. It has adopted policy and process changes that help ensure that its law enforcement priorities are used to support intelligence-based efforts to identify and disrupt terrorist organizations. As a matter of policy, all counterterrorism cases are opened as intelligence cases. This policy is supported by a new case classification system that eliminates the "criminal" case classification in favor of the intelligence-oriented "international terrorism" classification.

In an effort to institutionalize the priority on intelligence gathering in the field, the FBI has proposed criteria—developing sources and the quality of information they provide—for evaluating the performance of counterterrorism agents. These criteria are just a beginning. Further development of a new scheme for evaluating the performance of counterterrorism agents, including criteria and weighting, needs to be developed. Moreover, new intelligence-related performance criteria are not yet recognized in the field. Field staff was generally unable to articulate any specific criteria to be used to evaluate the performance of agents working counterterrorism. **The Panel recommends that immediate steps be taken to develop an initial scheme for evaluating the performance of counterterrorism agents in the field, that it be incorporated into agent training, and updated as needed.**

In addition to instituting polices and processes to support intelligence-oriented practices, the FBI has worked to develop an analyst workforce that eventually will provide the intelligence capability that underpins this approach. However, the FBI faces a significant challenge in recruiting and training analysts to staff headquarters and the field. This issue is addressed in Chapter Three.

The FBI has made striking advances in its willingness and ability to work jointly with other federal, state, and local law enforcement agencies. Through its use of the Joint Terrorism Task Forces, it has been able to increase greatly its capability to address counterterrorism goals. The number of personnel devoted to counterterrorism has grown due partly to increased participation of FBI partners in the task forces. Further, the FBI has been able to capitalize on the complementary legal authorities of its federal partners and the local knowledge of police forces, as well as their own complementary legal authorities. State and local task force participants testified to dramatic, positive changes in their working relationship with the FBI. The FBI's work with ICE immigration officials, in particular, has been markedly successful.

While our field visits suggest that cooperation and coordination between state and local operations and the FBI are accepted as necessary and useful, interviews with officials at FBI headquarters identified state and local counterterrorism operations that have actively resisted coordination with the FBI, most notably, the New York Police Department's Intelligence Division and the New Jersey Governor's Office of Counterterrorism. Both organizations have sought to run their own independent counterterrorism operations and have resisted sharing information with the FBI. The Panel believes that this lack of coordination could undermine a concerted counterterrorism effort. **The Panel recommends that senior FBI officials meet with the appropriate state and local officials to resolve outstanding jurisdictional conflicts to ensure the coordination of counterterrorism operations in the field.**

The FBI's Joint Terrorism Task Forces operate in a diverse and growing population of law enforcement organizations involved with counterterrorism operations. The FBI faces a significant challenge in developing productive working relationships with this emerging network of state and local entities. This task is further complicated by the management of DHS grants that support state and local counterterrorism initiatives and sometimes appear to promote competition to perform similar counterterrorism activities. This could discourage joint operations, lead to duplication of effort, and even undermine a coordinated counterterrorism effort. The basis for awarding grants has not seemed to have a coordinated counterterrorism effort as the goal. **The Panel recommends that the FBI work with the Congress and the relevant DHS components to ensure that funding such activities is conditioned on the development of a coordinated effort with the FBI field offices.**

Anti-terrorism Advisory Councils perform numerous important roles, including coordination, education, and training. However, the U.S. Attorney's offices are uniquely positioned to act as relatively neutral brokers to coordinate and manage disputes among various law enforcement agencies involved with counterterrorism operations in their jurisdictions. **The Panel recommends that the U.S. Attorney General provide clear guidance that Anti-terrorism Advisory Councils focus on coordination and dispute management and that they dedicate at least one Assistant U.S. Attorney to the task.**

Headquarters has provided considerable latitude to field offices in how to organize their Field Intelligence Groups. It is generally recognized that close interaction between analysts and operations is crucial to their effectiveness; physical proximity promotes that interaction. This model has worked well for the Counterterrorism Division at FBI headquarters. However, the field offices experience numerous pressures that may undermine this integration, including staffing, space constraints (such as secure compartmented information facilities) and the demands of cooperation with FBI partners. **The Panel recommends that field offices be given policy and funding support to ensure that meaningful integration of analysts and operations is established, maintained, and nurtured.**

State watch and warning systems are a positive development that is emerging in the counterterrorism area as they play an important intermediary role between state and local law enforcement and the FBI. The Maryland Coordination and Analysis Center represents a good example in the design of this type of system. Although the FBI cannot mandate how these systems are designed or run, they can promote their use. **The Panel recommends that the FBI promote the sharing of information on best practices for state watch and warning systems among state and local law enforcement and that it work with the relevant DHS components to accomplish this.**

The FBI also faces the challenge of sorting out its shared responsibility with DHS for communicating threat information to state and local officials, reported to be a source of confusion. The Panel urges both parties to work together to provide uniform messages.

The FBI continues to make progress in recruiting and training agents and analysts. However, growing pains still are apparent. In recent years, the FBI has relied heavily on temporary duty assignments to meet staffing needs at headquarters and abroad. This approach may be necessary to meet urgent short-term needs, but it should not be used on a routine basis. Extensive and regular use adversely affects field operations. Recently, the FBI's heavy reliance on temporary duty assignments reflected in part the hiring freeze in effect during much of Fiscal Year 2004. **The Panel recommends that funded headquarters positions be fully staffed and reliance on temporary duty assignments of field personnel be significantly reduced.**

The FBI has just begun to develop performance measures to track progress in meeting its counterterrorism program goals. Individual measures have been proposed. Some are reasonable. Others are less relevant. Although this limited progress is understandable in the midst of the FBI's efforts to organize and staff the program, performance measures are an important next step in the transformation process. **The Panel recommends that the FBI improve its performance**

measures, making sure that they are clearly linked to the satisfaction of its strategic goals and objectives.

CHAPTER THREE
INTELLIGENCE

The FBI historically had limited intelligence collection and analysis capabilities, with fewer than 300 personnel devoted to intelligence as late as the mid-1990s. Prior to 1998, these personnel were concentrated in the National Security Division, a small headquarters office that primarily handled the FBI's liaison with the U.S. foreign intelligence community in such areas as counter-intelligence, international terrorism, and occasionally criminal matters. The office also performed administrative duties associated with intelligence activities, such as clearances, compartmented document handling, and secure facility requirements.

When CIA official Aldrich Ames was identified as a long-time Soviet intelligence operative in the 1990s, increased emphasis was paid to counter-intelligence, including analyses of possible compromises by foreign intelligence services. Following the two U.S. embassy bombings in 1998, then-Director Freeh created a Counterterrorism Division focused on intelligence analysis of domestic and international terrorism.

Nonetheless, the FBI's intelligence capabilities remained limited due in part to legal constraints on the FBI. By law, FBI agents were not permitted to share information between criminal and intelligence cases. This barrier was removed by the Patriot Act. Also, the FBI made no effort to develop dedicated intelligence collection and analytic capabilities were regarded as weak. Certain aspects of the FBI's longstanding criminal investigative process were—and still are—similar to the U.S. intelligence community's information collection and intelligence analysis functions, but there are significant differences in terms of objectives, approaches, analysis process, distribution, and ultimate use.

Since the events of 9/11, Director Mueller has taken major steps to integrate intelligence into the FBI's mission. In early 2002, he established a small, largely administrative office of intelligence under the Executive Assistant Director for Counterterrorism and Counter-intelligence, and strengthened and placed its analytic center in the Counterterrorism Division. CIA detailed 25 analysts to assist the FBI, which initiated an analyst training course modeled on CIA's approach.

In January 2003, Director Mueller formally established both a separate Office of Intelligence (OI) and an intelligence program that provided the opportunity to centrally manage the FBI's core intelligence functions. The program had responsibilities for:

- Establishing and managing a new FBI intelligence collection requirements process.
- Prioritizing requirements.
- Coordinating collection against requirements, internally or externally.
- Analyzing information and producing intelligence.
- Disseminating intelligence information within the intelligence community.

- Evaluating field office performance against requirements.

The FBI views its intelligence production mandate as part of a three-pronged set of related responsibilities. In addition to providing intelligence information and analyses involving terrorist threats and national security crimes against the United States, the intelligence program strives to ensure that citizens' constitutional rights are protected. As such, the FBI's intelligence work is threat based, but constitutionally bound. OI is also responsible for ensuring that the FBI manages its intelligence resources responsibly.

The FBI's rapidly burgeoning intelligence role reflects:

- heightened **priority assigned to countering terrorism and espionage** as part of the FBI's strategy. These threats are global, transcend the nation's geographic boundaries, and often emanate from transnational enterprises.

- increased **importance of before-the-fact prevention** of activities inimical to U.S. security in these areas. In this threat environment, having the right information at the right time is necessary to protect national security by preventing attacks, not accumulating volumes of information after-the-fact to definitively prove culpability.

- increased **delegation of after-the-fact reactive investigations** of many actual or alleged illegal activities to other federal, state, and local law enforcement authorities

The FBI seeks to imbed intelligence into its day-to-day work, from the initiation of cases to the development of organization-wide investigative strategies.

An Executive Assistant Director for Intelligence was appointed in April 2003, and tasked to develop a plan for structuring an intelligence office, defining its functions, and managing a career structure for analytic and other intelligence personnel. The initial plan, presented to Director Mueller in September 2003, proposed a long-term implementation of an intelligence office and included five phases:

1. Develop an initial strategy for an FBI program plan and intelligence office.

2. Plan and develop a more detailed concept of intelligence operations for the organization.

3. Develop and execute a detailed implementation plan or path.

4. Build the intelligence office organization and functions, and integrate other aspects of the FBI organization and functions.

5. Reach total operational capability in the office.

Director Mueller approved this initial strategy for the intelligence program and office in November 2003.

THE CURRENT PANEL REVIEW

In its current review, the Panel examined the FBI's progress in establishing the office and implementing its intelligence program. The Panel paid particular attention to the FBI's efforts to:

- Develop and implement the intelligence program plan of operations.

- Integrate the FBI's intelligence program into similar activities that the U.S. intelligence community conducts.

- Stand up and staff OI's organizational structure.

The Panel's work plan emphasized structure and process over substance given the early stages of OI's development. Thus, the Panel focused broadly on OI's operational planning in relation to the FBI's evolving headquarters and field structure and its interface and connectivity with the larger intelligence community and other federal, state, local, and international counterparts. As a result, this work necessarily overlapped with information sharing and other issues addressed in the Counterterrorism and Security chapters. Areas included for specific review and discussed in this chapter are the following:

- **OI's headquarters structure** was reviewed, including its stand-up, staffing, and structuring of assignments and processes in relation to the Director's approved plan.

- **Terrorist Threat Integration Center and National Joint Terrorism Task Force collocation and integration** were reviewed, including the former's structure, staffing, information integration, and interaction with the re-located National Joint Terrorism Task Force operations as a means to facilitate information sharing and develop joint information collection and response plans.

- **Analyst workforce formation, development, and career track** were examined to assess the pace at which an analytic workforce, including reports officers, is being developed for headquarters and the field. Workforce quality, training, and development utilization and opportunities, and establishment of career reward and advancement processes also were reviewed.

- **Intelligence requirements, collection, analysis, dissemination, and evaluation** were examined, especially OI's established or proposed processes for them as part of the intelligence cycle. The value of OI's collection and analytical efforts was evaluated with particular emphasis on its processes, as well as involvement with broader intelligence community mechanisms.

- **Field intelligence structure and operations** were reviewed in the context of typical structures for different-sized field offices and resident agencies supporting the intelligence function, as were the roles of collection agents, reports officers, and analysts.

The interaction of these field intelligence cells with other field components, relationships to OI and headquarters divisions, and intelligence cycle operations at the field level were explored.

- **FBI information sharing**, especially OI's processes to share field and legal attaché intelligence reports, intelligence analyses, and other information with other entities was evaluated. OI's role in acquiring, tasking, processing, disseminating, and evaluating information from these sources was examined, as well.

At the Panel's suggestion and with FBI consultation, a review was conducted of the long-term resource plans and programs for OI and the intelligence program. The sections below summarize the Panel's findings and recommendations.

As with the other chapters, the methodology included reviewing a mix of public and internal documents on 9/11, counterterrorism, and intelligence. In-depth interviews with FBI headquarters and field personnel involved in intelligence were conducted. Other federal, state, and local officials were interviewed to obtain their insights on the state of OI's development and the FBI's intelligence program and activities. The congressional intelligence committee inquiries and the 9/11 Commission provided rich sources of information and insights with regard to intelligence.

THE INTELLIGENCE STRATEGY

The mission of FBI's intelligence program is to meet current and emerging national security and other threats to the United States. OI's proposed strategy to carry out this mission is to aim core investigative work proactively against threats to U.S. interests; build and sustain enterprise-wide intelligence policies and capabilities; and provide useful, appropriate, and timely information and analysis to the national security, homeland security, and law enforcement communities.

To fulfill this strategy and support the FBI intelligence mission, the intelligence program is based on performing nine core functions:

1. Provide intelligence doctrine and policy.

2. Manage a collection and requirements process.

3. Maintain standards for production and analytic rigor.

4. Develop human talent.

5. Oversee the headquarters and field intelligence structure.

6. Disseminate timely information to customers.

7. Build strong partner and customer relations.

8. Forecast and plan for human talent and information infrastructure needs.

9. Manage intelligence program resources.

Identifying these core functions provided the basis for the second, or design, phase of OI's intelligence plan: the development of operational plans for each function.[5] Operational plans for all but one function, customer relations, have been completed.

OI's plan serves as a rich blueprint for the intelligence program's structure, but not a detailed specification. It provides a shared vision of how the FBI will corporately execute the major aspects of each intelligence function listed above, identifying guiding principles and policies, describing certain standards and procedures, allocating key intelligence responsibilities, and creating a shared intelligence vocabulary. However, it does not attempt to provide a comprehensive list of every action or process required to guide the program's formation. It identifies the needs for detailed policy statements, requirements documentation, field reporting and operating procedures, and career development and training documents, but these are still being drafted.

For the intelligence program, OI has created four initial strategic goals that focus the intelligence functions toward attainable, executable, and measurable objectives. Taken together, the goals, objectives, and their corresponding performance metrics are designed to hold the FBI, as an enterprise, accountable for supporting its shared intelligence mission.

> **Goal 1: Intelligence Policy.** Create a common approach to intelligence work through enterprise-wide doctrine, policy, and production standards. The FBI's metrics for success will be (1) production and dissemination of an intelligence policy manual, (2) elimination of redundant policy documents, (3) production and dissemination of standards for intelligence products, and (4) a higher percentage of intelligence products that meet intelligence standards.
>
> **Goal 2: Intelligence Processes.** Fill intelligence gaps with a uniformly managed intelligence process. The FBI's metrics for success will be (1) percentage of identified intelligence gaps filled, (2) establishment of a Field Intelligence Group in every office, (3) establishment of an intelligence-based targeting activity in every office, (4) development and maintenance of intelligence collection capability baseline survey, and (5) maintaining baseline analytic capabilities.
>
> **Goal 3: Threat-Based Management.** Align operations and capabilities with the threat environment. The FBI's metrics for success will be (1) production and maintenance of an FBI threat forecast, (2) percentage of intelligence-based investigations, (3) workforce experience, education and demographics, (4) capability maturity model level for human

[5] OI refers to this operational plan as its "concept of operations," a document that defines an approach to each core function and the organizational structure needed to put the approach into operation.

talent, (5) capability maturity model levels for technology,[6] and (6) budget impact model for assigning value to sources.[7]

Goal 4: Customer Service. Support internal and external intelligence customers and partners with corporate information sharing and related support strategies. The FBI's metrics for success of this goal will be (1) percentage of products disseminated at each classification level, (2) percentage of products disseminated for each FBI priority, (3) percentage of products disseminated for National Intelligence Priorities Framework topics, and (4) percentage of positive responses from product and customer support feedback.

Subsequent policies, plans, and processes, which will derive from OI's operational plan, will flesh out these goals and metrics.

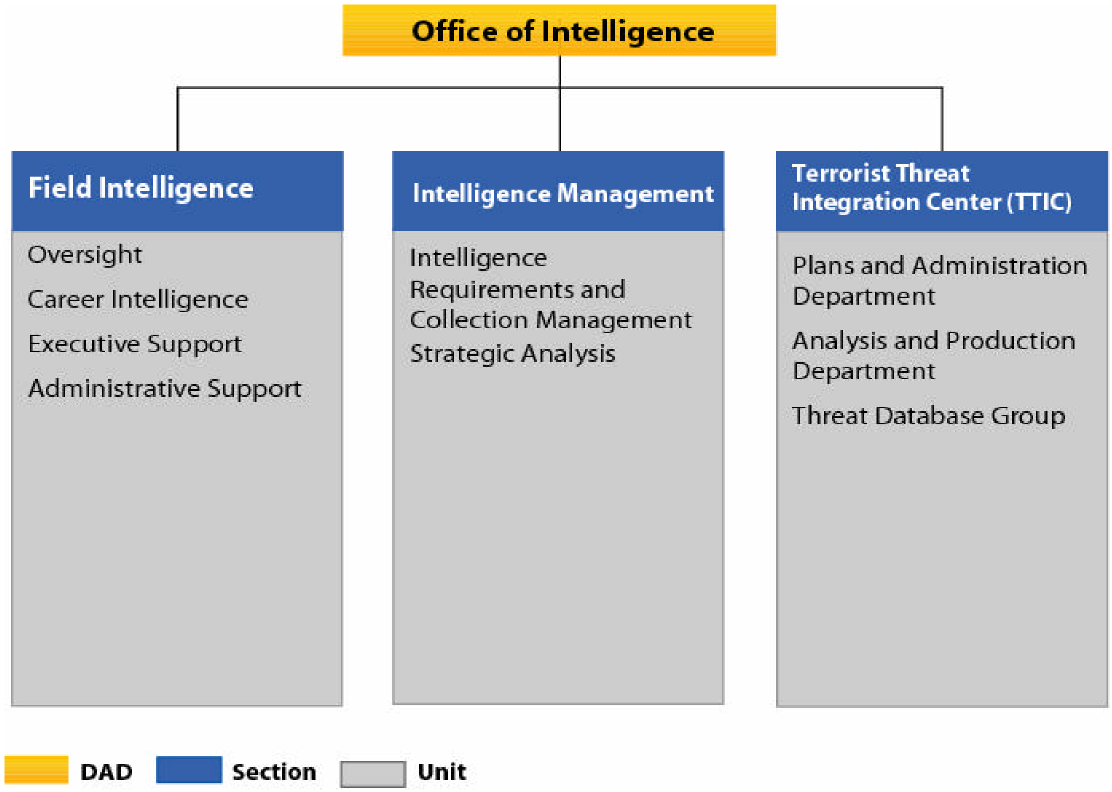
HEADQUARTERS' OFFICE OF INTELLIGENCE

The formation of OI's structure still is in the initial stages. As of August 2004, the organization has three major operating sections, as shown in Figure 3-1 below. In early May, OI operated three principal management units under a single section, but added a second one for Intelligence Management in June. It now treats the Terrorist Threat Integration Center as a third. These sections fall under the direct responsibility of a Deputy Assistant Director (DAD).

[6] The term, "capability maturity model," used in the statement of objective 4, refers to a phased plan for creating the organizational processes needed to develop, acquire, and maintain information management systems. As used in the statement of objective 5, the term refers to a phased plan for creating a set of organizational practices necessary to develop, motivate, and retain a highly trained and diverse workforce of the appropriate size.

[7] The "budget impact model" identified in Objective 6 provides an analytical basis for determining and justifying the financial resources required for developing sources.

Figure 3-1
Organization of the Office of Intelligence



The Field Intelligence section includes four units: the Oversight Unit, which oversees field activities, the Career Intelligence Unit, the Executive Support Unit, and the Administrative Support Unit. Also, the Field Intelligence Section is expected to incorporate Language Services, which is to be moved from the Office on International Operations. Language Services will continue to manage foreign language skills, including linguist recruitment, hiring, and training, within the FBI. The section's two principal units, Career Intelligence and Executive Support, are discussed below.

.

- **The Career Intelligence Unit** is responsible for managing the FBI's intelligence analyst personnel. It identifies the human talent needed for intelligence production and analysis and defines ways to recruit, develop, motivate, and retain the analytic workforce. Three types of intelligence positions have been designated: (1) all-source **intelligence analysts** responsible for discerning complex patterns of behavior necessary to understand present or future threats or understanding strategic areas through specific expertise; (2) **reports officers** responsible for identifying, extracting, and disseminating raw intelligence information from FBI investigations, sources, and contacts; and (3) **operations specialists** responsible for guiding investigative and intelligence activities and providing tactical support to these investigations. OI's operational plan addresses ways to recruit high quality candidates to its analytic workforce and provides a five step, "quick-hire" process for selection. This streamlined process includes an initial on-line application, cognitive ability testing followed by a full employment application, a structured interview and writing exercise, drug, polygraph, and interview screening, and final selection. The unit has conducted a highly successful recruitment drive with more than 25,000 applicants initially screened. It has successfully deployed training modules for career special agents at the FBI Academy and an initial intelligence analyst training curriculum at the Academy's newly formed College of Analytical Studies. Additionally, it is identifying career development opportunities through participating in intelligence community and Defense training programs, foreign area analyst programs, training exercises. Distance learning approaches are also being explored.

- **The Executive Support Unit** is documenting OI's authority to conduct intelligence activities and drafting basic policies governing the FBI's intelligence activities. These will incorporate such guiding principles as protection of sources and methods, widest possible information dissemination, rapid threat warning, and investigative results reporting. This unit has been supplemented with a senior intelligence community manager who works on developing intelligence policy.

The second OI section, Intelligence Management, handles the management of key aspects of the FBI's intelligence cycle. It includes two units discussed below.

- **The Intelligence Requirements and Collection Management Unit** is responsible for managing intelligence collection and production requirements, developing collection plans, collection management, and product dissemination. Its initial efforts involved defining standing information requirements for priority areas, such as international and domestic terrorism and public corruption, with standing requirements in other areas to follow. These are now available on-line to more than 17,000 law enforcement entities nationwide.

- **The Strategic Analysis Unit** is responsible for managing future threat forecasting, which will be key to updating the FBI's strategic plan, guiding the acquisition of human talent and technology to meet future needs, and understanding the impact of forecast trends on operations. Thus, these forecasts will serve not only long-term strategic planning needs, but also support the FBI's program/budget processes and near-term operational adjustments. A five-year threat forecast, produced quadrennially and updated annually, will identify the primary trends and drivers likely to affect the FBI's mission. They will be produced by OI's intelligence production board, which includes representatives from all operational components. Three additional forecasting documents will support the threat forecasts: operational impact assessments, led by the Office of Strategic Planning, that will translate the threat forecast into practical implications for FBI operations; intelligence human talent requirements forecasts**,** led by the career intelligence unit, that will identify the needs for the number and characteristics of intelligence personnel; and intelligence technology requirements forecasts, led by OI in conjunction with the Chief Information Officer, that will identify future information technology requirements through a prioritized list of functional requirements detailing capability characteristics, operational requirements, and timeframes. This unit is minimally staffed, relying heavily on contractor assistance to draft a threat forecast.

> The Strategic Analysis Unit also is responsible for other cross-divisional analytical products. It supports the production board in its efforts to coordinate short- and long-term production, link to Director of Central Intelligence and intelligence community processes, and review threats, developments, and issues affecting investigative priorities and production topics. The unit's chief serves as executive secretary of the Board, which has daily production and coordination responsibilities.

As demonstrated by the addition of these sections, the OI structure is evolving as decisions on policies, programs, and responsibilities are made. Staffing is the major current impediment to a faster evolution. Slightly more than one-third of OI's planned 150 personnel are on board, though plans are underway to acquire the remainder in Fiscal Year 2004. An additional 150 staff have been requested for Fiscal Year 2005, and this has been provided for in the House appropriations bill. In addition, a decision is pending on the proposal to transfer 100 foreign language program personnel to OI. All told, a permanent cadre of more than 400 staff is envisioned to perform the FBI's intelligence management functions, including the administration of 67 FBI personnel assigned to the Terrorist Threat Integration Center.

Over time, OI will assume a greater production role, particularly for analyses associated with strategic forecasts and cross-directorate products. Further, the FBI complement to the Terrorist Threat Integration Center may grow, particularly under the more expansive concept of a National Counterterrorism Center recommended in the 9/11 Commission report. Excluding that possibility, it appears reasonable that a staff size numbering 350 to 400 individuals can accomplish OI's program and personnel management role. A larger staff opens the door to greater OI involvement in operational and division-oriented production that has wisely been delegated to division and field elements.

Collocation and Integration of the Terrorist Threat Integration Center, National Joint Terrorism Task Force, and Counterterrorism Center

OI manages the administrative aspects of the FBI's staff contribution to the joint Terrorist Threat Integration Center. As President Bush directed in his 2003 State of the Union address, the center was established in May 2003 as a joint venture, reporting directly to the Director of Central Intelligence. It does not engage in intelligence collection or investigative operations, but provides for the integration of information, expertise, and analysis on international—not domestic—terrorism. Its partners include CIA, FBI, DHS, the Defense and State Departments, and other federal agencies. Its current staff consists of more than 125 assignees, including 90 analysts, and more than 200 contractors. The FBI component is sparsely staffed at less than 25 percent of its authorized strength due to the limited number of high quality analysts and, until recently, space limitations. The center recently relocated from CIA headquarters to a new facility that will house significant portions of the FBI's Counterterrorism Division, including the National Joint Terrorism Task Force, and the Director of Central Intelligence's Counterterrorism Center. It is envisioned that its full-time complement will grow to 300 assignees and 200 contractors.

The Terrorist Threat Integration Center produces a daily threat matrix based on all-source information supplied by intelligence community agencies and used in the day-to-day terrorism analysis provided to the President and twice-daily situation reports. Most of the center's production has concentrated on current intelligence on individual threats, real or potential. It has begun to produce terrorism analyses, though they are quite limited at this time.

Threat assessments are a notable weak point in the nation's domestic intelligence capability. Community-wide products addressing the nature, range, likelihood, and target of longer-term terrorist threats are very limited. Although the FBI updated its U.S. threat assessment approximately one year ago, the intelligence community's threat assessment is severely outdated. During our field interviews, state and local officials expressed considerable frustration about the availability and quality of threat assessments. They commented that the limited availability of threat assessments had led them to rely on alternative approaches, such as lists of key assets and infrastructure elements, equal sharing of grant funds, and vulnerability studies—rather than applying resources based on known or suspected threats. Moreover, there seems to be considerable confusion at the state and local level about the respective roles of the FBI, DHS, Terrorist Threat Integration Center, and state and local authorities in producing threat assessments. Confusion among state and local officials as to who is responsible for doing threat assessments seems to reflect confusion among federal agencies about the scope of their responsibilities. Although the Homeland Security Act of 2002 assigns a component of DHS, infrastructure information analysis and protection (IAIP), authority to do threat assessments, the FBI and CIA seem unsure of the scope of DHS' authority and responsibility for intelligence analysis. At the same time, the Homeland Security Act of 2002 also assigned the FBI specific responsibility to provide state, tribal and local law enforcement organizations with intelligence on terrorist threats.

The National Joint Terrorism Task Force is collocating with the Terrorist Threat Integration Center, but it is a component of the FBI's Counterterrorism Division. Composed of representatives from a large number of agencies, the task force serves as a primary means to facilitate the sharing of warning information, generate cooperation in addressing immediate threats, and task subordinate FBI offices, their local task forces, and other federal agencies to collect and resolve possible terrorist threats. It focuses on operational cooperation, in conjunction with other agencies and with the 100 Joint Terrorism Task Forces subordinate to the FBI's field offices and resident agencies.

Relocating these entities, as well as a significant portion of the Counterterrorism Division and the Counterterrorism Center, is occurring more rapidly than planned. The building contractor gave high priority to completing construction because the FBI was motivated to have its personnel in place and re-acclimated prior to the 2004 political campaigns and election. It believed a less timely relocation would have been disruptive to counterterrorism operations at a time when the threat is expected to peak.

THE ANALYST WORKFORCE

As noted above, the Career Intelligence Unit is responsible for the analyst workforce, and it has made significant progress in establishing the three work areas for intelligence analysts, interviewing and placing analysts in these areas, and developing career boards and qualification standards. In addition, it has made substantial headway in developing a training curriculum for intelligence analysts and preparing supplemental guidance to support the work areas.

The FBI has mounted an extremely successful recruitment effort of new analysts. However, hiring has not kept pace. Despite the priority given to intelligence analysts for counterterrorism in the hiring and personnel clearance processes, there are significant shortfalls in staffing at headquarters and in the field. As of June 2004, the Counterterrorism Division had filled less then 60 percent of its funded analyst positions (see data on staffing in Table 2-1, p.33). Shortfalls in analyst staffing were particularly apparent in the field offices. Moreover, many Field Intelligence Groups are composed solely of analysts consolidated from other field programs, such as Medicare fraud, white-collar financial crimes, and intelligence specialists providing operational support to counterterrorism squads.

Table 3-1 shows the number of intelligence analysts between 1999 and September 2004, both total and distributed between headquarters and the field. It shows a total increase of approximately 10 percent through 2003. Headquarters fared somewhat better in recent years with an increase of 240 analysts through 2003 since its low point in 2000. The field declined by 130 analysts over the same period.

Table 3-1
FBI Intelligence Analysts, FY 1999-2004

	1999	**2000**	**2001**	**2002**	**2003**	**2004**	
	Actual	Actual	Actual	Actual	Actual	Funded	On Board
Analysts - Total	1057	1070	1023	1012	1180	2053	1323
Headquarters	428	363	434	450	603	971	599
Field	629	707	589	562	577	1082	724

The table reflects the major increases planned for headquarters and field analysts in 2004, a projected 74 percent increase. The funded staffing level reflects current FBI plans, though some hiring may be delayed through the first quarter of 2005 due to processing delays and entrance-on-duty decisions. It is projected that headquarters will hire more than 370 new analysts, and the field offices more than five hundred. Nonetheless, a high percentage of qualified candidates have not been hired. Either candidates have been dropped from consideration due to security concerns or they have dropped out due to the length of time required by the FBI to select candidates and make them a firm employment offers. The FBI could not provide precise data on attrition due to these factors.

During the past year, the FBI has experimented with three different hiring processes for analysts and other non-agent support personnel. Perhaps out of confusion, field offices conducted their review and hiring approaches in differing ways. All used a career board to review applicants' forms, but some had no personnel interview while others conducted limited "meet-and-greet" sessions with applicants. Still others did full applicant interviews. Given the importance of these interviews in determining professional qualifications and analytical competence, an in-person interview is necessary. The FBI has indicated that "Quick Hire," an approach it has used to hire intelligence analysts since mid-2004, will be adopted for 2005. It will include in-person interviews of candidates by the hiring component. Looking longer term, the Administrative Services Division is considering a national hiring system that would bring qualified applicants to a central facility for interviews and security purposes.

The current understaffing of analyst positions is compounded by the loss of some senior analysts and best-qualified candidates to other intelligence agencies. This may be due to better pay and promotion opportunities elsewhere, as well as a wider range of assignments and opportunities. The FBI is seeking to remedy this shortcoming through improved pay grades for analysts, either through an OPM-approved demonstration project or enactment of statutory pay and personnel provisions similar to those of CIA and most other intelligence agencies involved in national security.

THE INTELLIGENCE CYCLE

Traditional FBI case management processes do not mirror those of the intelligence community or its major agencies. The intelligence cycle typically includes identifying and validating requirements, collection tasking and collecting information, processing collected information into raw information reports for dissemination, analyzing multiple inputs, producing and disseminating finished assessments, evaluating the status of requirement satisfaction, and reiterating refined needs through this cyclical process. The portions of OI's operational plan that address intelligence requirements, collection management, and intelligence assessments go a long way toward establishing a similar system for the FBI.

OI's Intelligence Requirements and Collection Management unit, which monitors this responsibility, has elaborated on its approach in a separate handbook that defines OI's procedures for establishing intelligence collection and production requirements, monitoring satisfaction, and disseminating products to customers. These functions are centralized within the unit for requirements that interface with external agencies or feature coordination across FBI divisional or field office components. It assigns requirement identifier, priority, time thresholds, reporting format, and internal FBI dissemination instructions. It also is responsible for developing collection and production plans associated with the approved internal requirements, including the identification of resource adjustments through reallocating current resources or acquiring additional ones. However, operational management of production and collection remains with headquarters' operational divisions and the field offices.

Self-generated requirements within a specific headquarters division, field office, or legal attaché office—as well as the collection, analysis, and dissemination related to satisfying them—are not directly integrated with interagency or intra-agency coordination requirements, though OI is surveying FBI field collection capabilities that may identify some. This handbook differentiates intelligence requirements and traditional FBI "operational leads." The latter usually involves case-specific, tactical leads more responsive to individual investigations, rather than more general and generic information needs responsive to national intelligence and FBI-defined requirements. Neither operational leads, nor requirements that can be satisfied with resources under a component's own control, are integrated into the intelligence collection, production, and dissemination process requirements.

OI's plan also defines a comprehensive approach and standard process for intelligence assessment, which generally includes a project proposal, terms of reference, detailed research, review of secondary sources, aggregation of data from all available sources, and evaluation of sources, analysis and integration, drafting, review and approval, dissemination, and evaluation. The plan calls for interaction between analysts and customers to develop a clear understanding of the information needed or to narrow the request to customer-critical elements; these are to be incorporated in the project proposal and the terms of reference. A product evaluation, such as a customer satisfaction survey, completes the process.

Here, too, there are several differences between the FBI's plan and standard intelligence community practice. First, the FBI has integrated operations and analysis in contrast to standard intelligence community practice which segregates analysts and collectors. This provides FBI with a much more direct and less cumbersome process for tasking collection in response to requirements. Second, FBI treats "raw intelligence" field reporting as product, which is at variance with CIA's treatment of human source reporting but more attuned to NSA's treatment of its more definitive products. With respect to field agent reporting of informant information, however, it is important to distinguish raw, unevaluated reporting from finished all-source intelligence, a distinction new to traditional law enforcement processes. Third, the FBI is treating its validated information needs as tasked requirements when levied on internal elements, but as requests for information when referred to external agencies as it does not have the authority to "task" them. The difference is more than semantics; it is at the heart of the 9/11 Commission recommendation that the National Counterterrorism Center do operational planning and that collection agencies focus on hiring, training, equipping, and fielding personnel and collection systems. Nonetheless, both approaches are equivalent to a levy for collection action or production. It will be important to manage these internal and external levies in balance, particularly when evaluating and comparing their efficacy.

As with the rest of the intelligence community, the FBI has a gap-oriented requirement process, emphasizing deficiencies but not providing confident assessments of what is known. As noted above, it appears to treat external capabilities and competencies as more remote and less reliable. Integration with the intelligence community's requirements process and Director of Central Intelligence tasking responsibilities appears to be an important ingredient requiring extensive knowledge of external capabilities, strengths, and weakness to be efficient and productive.

There is concern that the requirements process will not capture some very important field collection and reporting activities, although OI's ongoing intelligence collection capabilities survey may alleviate this concern. Examples include field collection and production activities that seem to have broad utility inside and outside the FBI, but are not captured by the requirements process because they remain within a single field office. These may be isolated circumstances, and relatively easy to overcome when field units adapt to a more pervasive intelligence culture. Field offices and legal attaché offices are not now required to report all significant field production activities to headquarters.

FIELD INTELLIGENCE STRUCTURE AND OPERATIONS

OI's plan for field office intelligence operations envisions field offices as being an integral part of the FBI's intelligence network, with each one having an Assistant Special Agent in Charge responsible for centralized intelligence functions in a Field Intelligence Group which manages and coordinates intelligence functions. The field intelligence units will be organized into one or more squads depending on the size of the field office. A smaller office may have a group organized within a traditional squad that has other responsibilities supervised by a Supervisory Special Agent who reports to an Assistant Special Agent in Charge for intelligence. The group also will include the positions and functions of an asset/informant coordinator and its personnel. Personnel will have routine access to top secret and sensitive compartmented information, and their workspace will require sensitive compartmented information facility-level protection for secure discussion, processing, and storage of information. Personnel also will be responsible for protecting and securely managing the dissemination of classified, sensitive, and unclassified information to state and local law enforcement officials.

OI's operational plan and the Field Intelligence Group concept provide a reasonable basis for structuring field office intelligence management, analysis, and reporting operations. The field offices received substantial latitude on how to structure their groups. Some consolidated most of their analysts, reports officers, and intelligence specialists into a centrally-managed pool. Most have opted for a consolidated analytic and reporting pool composed of virtually all analysts—including financial analysts generally associated with support for white-collar crime investigations—and reports officers. Still others have decentralized intelligence specialists supporting individual counterterrorism squads to provide more immediate involvement by intelligence personnel in collection operations. Most groups are collocated with or in close proximity to the field office's Joint Terrorism Task Force to promote close working relations between intelligence and operations. Overall, the Field Intelligence Group concept as implemented appears to provide a flexible structure and administrative mechanism easily adaptable to field offices of differing size, configuration, and workload. It provides a significant intelligence presence in each field office while retaining the Special Agent in Charge's unity of command over all field office activities.

The primary deficiency in the Field Intelligence Group is not structure, but personnel. Most have limited personnel or are awaiting additional hires. A substantial influx of additional analysts is promised. The work day of group analysts, as at headquarters, is driven by near-term threats and immediate information inquiries, not longer-term strategic analyses of potential threats and targets. The project team identified only one office that seemed to have consciously focused on strategic assessments, though most recognized the need, and even tried, to isolate one or two analysts for these tasks. Interestingly, most were not even aware of alternative approaches that had been taken to organize and manage intelligence, even by adjacent field offices. The team, in effect, became the communications medium for thinking about alternative approaches. The Special Agent in Charge's flexibility to organize his or her own resources need not be precluded, and a one-size-fits-all approach need not be imposed. Yet there are real opportunities for OI to assess best practices at field offices of varying sizes, geographical dimensions, and threat issues, and guide their managers on alternative approaches to organizing and allocating scarce resources. Although OI feels its oversight unit is becoming aware of organizational options and practices, there was little evidence that this information was being shared with the field.

INFORMATION SHARING

OI's information sharing plan provides a set of principles and basic guidance to encourage extensive operational information sharing between FBI headquarters and field personnel, including intelligence analysts and field agents. Indeed, headquarters analysts generate most intelligence information reports based on operational traffic from the field pending establishment of Field Intelligence Groups and training for field reports officers. The plan encourages converting intelligence information into reportable products and sharing these reports externally.

The guiding principles emphasize that information sharing shall be the rule, and filtering the exception only when sharing is legally or procedurally unattainable. OI has responsibility for sharing information with the intelligence community, law enforcement agencies, and other federal and international agencies. Its field extensions—the Field Intelligence Groups—are responsible for being the intelligence information sharing coordinators in the field. The principles endorse a write-for-release policy implemented through tear-line formats and electronic information sharing using technology that customers and partners find compatible. Standing requirements for international terrorism are web-based and available to more than 17,000 law enforcement agencies. Similarly, periodic publications and special assessments are being developed that include specific dissemination lists encompassing a wide range of customers. OI coordinates this process in conjunction with the National Joint Terrorism Task Force. The 100 local Joint Terrorism Task Forces serve as the primary mechanism that facilitates information sharing for time sensitive operational intelligence, which the Field Intelligence Groups will support as they develop.

The community support part of OI's plan addresses customers external to the FBI, as well as the roles that OI, operational divisions, and field offices respectively have in this process. In the final stages of production, this part will provide a framework of guiding principles, common terms, operational approaches, and appropriate means for information sharing externally. In the meantime, specific responsibilities for information sharing, particularly at the field office level, have not been designated. For finished product, the plan appears to favor a highly centralized process of dissemination from headquarters to external agencies. Somewhat in contrast, the Field Intelligence Groups currently provide staff to the Joint Terrorism Task Forces to facilitate direct information exchange with other federal, state, and local agencies represented. In addition, there are numerous examples where task force or group personnel have developed ad hoc mechanisms to share information; local e-mail and rolodexes seem to be proliferating in the absence of explicit headquarters guidance. As with military operations, local exigencies tend to establish real-life information sharing practices. The tension between localized sharing and directed centralized sharing is inherent in the increasingly centralized management of counterterrorism operations and consideration of fair play in the field.

In addition, the plan provides no specific guidance on information sharing within the Terrorist Threat Integration Center, or with the broader intelligence community, DHS, or international organizations, though it does identify state and local information sharing categories. Interviews conducted as part of the Panel's work indicate that information sharing with intelligence agencies has significantly improved. However, the Panel is concerned that the FBI may not be receiving all relevant information from its partners in the community, most notably the NSA. While FBI officials have expressed confidence that the NSA is making a good faith effort to share information, they were unable to explain the process by which the NSA determines what information to share. This situation suggests the need to establish formal information sharing processes so as to clarify what information is to be shared and why. Interviews also indicated that progress in information sharing relies heavily on personnel exchanges among organizations and the recognized imperatives associated with terrorism, while information sharing processes remain unclear. The Panel is concerned that information sharing could erode once the current emphasis on terrorism abates unless it is embedded in formal processes.

LONG-TERM RESOURCE PLANNING

Intelligence program/budget formulation is one key function that the OI plan addresses. OI has begun to develop longer-range resource planning for intelligence resources designed for a five-year resource plan, supplanting the one-year incremental budgeting process common in most non-national security agencies. Several major resource areas, such as personnel, communications, information technology, and training, have been tentatively identified.

OI, in conjunction with the Finance Division, will identify intelligence capabilities and gaps and develop strategies to fill them. Many of the deficiencies diagnosed in initial reviews clearly are not amenable to short-term solutions. Most, such as acquiring intelligence analysts and modernizing information technology, can only be addressed over a substantial period of time within the context of a longer-term plan, such as a multi-year strategy or enterprise-wide architecture. This approach is more important to institutions in transition than those with continuing and reasonably stable objectives and operations. It may not be necessary for every aspect of FBI operations, but a long-range plan certainly is appropriate, if not essential, for its intelligence, counterterrorism, information technology, and security operations.

OI, working with the Finance Division and garnering agreement with other divisions, has taken an initial cut at identifying FBI-wide resources that the FBI and Department of Justice must address through the budget process. This aggregation was included in the House bill appropriating funds for FBI for Fiscal Year 2005, and corresponds with a recommendation of the Academy-convened task force to reshape the FBI's budget decision units. It also will serve as a basis for future resource decisionmaking and review for 2006 and future years, and be included in the FBI's planning estimates to Justice. As budget formulation moves forward to Justice, the Office of Management and Budget, and congressional appropriators, OI will work with the

Finance Division to address questions, concerns, or differences in conjunction with the operating divisions.

In addition, OI has explored several resource areas in conjunction with the FBI's Fiscal Year 2006 budget that are clear candidates for resource augmentation. Examples include the following:

- **Secure Space.** In most FBI offices, including headquarters, there are extremely limited areas of secure space where classified material can be productively used and maintained. Although the Liberty Square[8] project will accommodate much of this need for some divisions and alleviate headquarters crowding, major SCIF space needs remain in field offices where most work with highly sensitive intelligence material is relegated to small communications and computer terminal rooms. Even recently constructed facilities, such as the Baltimore field office, have only a single conference-type room for highly sensitive work or meetings. The Fiscal Year 2005 budget includes only $11 million to address the need for secure space. The FBI believes that significant additional funding will be needed, and agreed that it could require $125 million to $250 million for SCIF space over the next five years. (A fuller discussion of SCIF space needs and costs, as well as a Panel recommendation, are provided in Chapter Four.)

- **Information Technology and Communications.** FBI's communications and data networks are not positioned to satisfy the 9/11 Commission's recommendation to develop a "trusted information network." The widely distributed Law Enforcement Online and National Law Enforcement Telecommunications System are limited to law enforcement sensitive material. Internally, the FBI's new Trilogy can handle classified material, and the FBI is expanding its secure communication network to handle compartmented information. Externally, however, highly classified materials are handled by alternative, sometimes less secure means, particularly with state and local agencies. A multi-security trusted information network linked to state and local law enforcement is beyond current plans, but it appears to be a reasonable requirement to facilitate information sharing and secure joint operations.

- **Training.** The FBI has limited training facilities that are primarily committed to agent training and supportive of improved state and local law enforcement training. These facilities were able to accommodate OI's demands associated with its new College of Analytical Studies, but the demands of expanding courses and development of a nationwide FBI lead in criminal analysis are being considered. The FBI has only begun to consider alternative solutions to the training facilities issue, but the need for some long-term augmentation appears obvious.

- **Personnel Acquisition:** The incremental personnel strategy that OI has pursued in recent years is not optimized to acquire the most talented analysts and specialists. Highly

[8] Liberty Square is the new complex housing TTIC, portions of the FBI's Counterterrorism Division and the CIA's Counterterrorism Center. This complex provides expanded SCIF space to accommodate the combined efforts of the FBI, CIA, and other federal agencies participating in TTIC.

decentralized recruitment and interview processes might be improved by more robust national recruitment efforts, mirroring the approach that most intelligence agencies use. This approach makes sense only if it is adopted as a multi-year commitment to elevate the FBI's recruitment and outreach efforts.

FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

The FBI is well on its way to establishing an intelligence structure, policies, processes, and a program to fill the gap in domestic intelligence on terrorism. The structure of the Office of Intelligence (OI) is evolving and will continue to do so as staff is acquired. It has made measurable progress in establishing an intelligence analyst cadre and initiating augmentation of a major staff addition both at headquarters in the field. The basics of the FBI's intelligence cycle have been defined and are being fleshed out. Field Intelligence Groups are in place in all field offices, though some are sparsely staffed.

OI's plan appropriately emphasizes management, rather than daily operational and most production responsibilities, which have largely been decentralized to operating divisions and field offices. **The Panel recommends that the Office of Intelligence continues to emphasize intelligence management and that it not become encumbered by detailed operational and production responsibilities**.

Threat assessments are a notable weak point in the nation's domestic intelligence capability. Community-wide products addressing the nature, range, likelihood, and target of longer-term terrorist threats are very limited. Although the FBI updated its U.S. threat assessment approximately one year ago, the intelligence community's threat assessment is severely outdated. During our field interviews, state and local officials expressed considerable frustration about the availability and quality of threat assessments. They commented that the limited availability of threat assessments had led them to rely on alternative approaches, such as lists of key assets and infrastructure elements, equal sharing of grant funds, and vulnerability studies—rather than applying resources based on known or suspected threats. Moreover, there seems to be considerable confusion at the state and local level about the respective roles of the FBI, DHS, Terrorist Threat Integration Center, and state and local authorities in producing threat assessments. Confusion among state and local officials as to who is responsible for doing threat assessments seems to reflect confusion among federal agencies about the scope of their responsibilities. Although the Homeland Security Act of 2002 assigns a component of DHS, infrastructure information analysis and protection (IAIP), authority to do threat assessments, the FBI and CIA seem unsure of the scope of DHS' authority and responsibility for intelligence analysis. At the same time, the Homeland Security Act of 2002 also assigned the FBI specific responsibility to provide state, tribal and local law enforcement organizations with intelligence on terrorist threats.

The 9/11 Commission concluded that hard choices must be made when allocating scarce resources and recommended that risk-based priorities be established and funding made available to implement protection measures. Yet, this is difficult to accomplish in the absence of generally agreed upon threat assessments.

While DHS is assigned authority to do threat assessments, the current administrative reality militates against DHS performing them. At this time, the IAIP has not developed the intelligence capacity to perform the threat assessment function. Moreover, the entire intelligence structure as currently set up, and as proposed by the 9/11 Commission is at odds with the statutory language providing authority to DHS to do domestic threat assessments. Given the current structure, the intelligence community, not DHS, is in the best position to determine the threat "from abroad" to US interests, and the FBI is specifically assigned responsibility to assess and communicate threats based in the United States and has the capability to do so now. Therefore, **the Panel recommends that the FBI perform domestic threat assessments and continue to develop its capability to do so.**

In this division of responsibility, DHS would still perform critical threat assessment roles both as a member of the intelligence community and in particularizing threats as they impact federal, state, private, and local sectors. For example, in the case of aviation, the intelligence community would identify threats emanating from abroad, and the FBI would identify threats based in the U.S, while DHS specified those threats in terms of the risk posed to civil, cargo, private aviation or air facilities.

Inadequate staffing of analytical positions is the major challenge to the FBI's intelligence program and deserves the highest management attention. While both OI and the Administrative Services Division appear focused on fulfilling staff needs and hiring additional analytical personnel, a longer-term view suggests that the FBI should consider reexamining its internal processes and policies to determine if they are impediments to staffing. Moreover, the FBI should consider whether more flexible hiring authorities would facilitate staffing. **The Panel recommends that the FBI consider reexamining its internal personnel processes and policies to determine possible impediments to staffing, as well as identifying more flexible hiring authorities that would facilitate staffing .**

The FBI experimented with at least three hiring processes in 2004: a traditional skills-based assessment, "Quick Hire," and a specialized intelligence analyst system. This variety has led to conditional offers of employment to analysts without conducting in-person interviews with candidates to verify paper qualifications or assessing personal qualities. **The Panel recommends that in-person interviews with candidates be mandated when hiring analysts.**

In-depth strategic collection and analyses efforts tend to be deferred at the FBI. This tendency reflects the realities of a still small analytical staff and the heavy demands for operational support. However, even after a larger analytical staff is built, the tendency will be for immediate operational demands to push out strategic analyses. These analyses must be emphasized and nurtured**. The Panel recommends that the FBI work with headquarters and field personnel to develop a production program focused on strategic analyses. Its work should be coordinated with the Terrorist Threat Integration Center and the intelligence community's National Intelligence Production Board.**

As noted earlier, the FBI treats requirements for collection and production internally as taskings requiring action by its operational and analytical components. It treats similar assignment to other intelligence agencies as requests for information. This approach, as in other intelligence community agencies, fosters over-reliance on capabilities directly under its control and tends to minimize friction with other collection or production agencies. Because of the increased linkage of foreign and domestic intelligence activities concerning terrorism, the treatment of internal and external taskings should be made more uniform to avoid duplicating existing capabilities external to the FBI and increased collection and production efficiencies. **The Panel recommends that the FBI rely on American intelligence agencies operating abroad to meet their covert foreign intelligence needs and that those agencies rely on the domestic intelligence capabilities of the FBI, rather than develop redundant capabilities.**

Sharing counterterrorism information at the federal, state, and local levels clearly has improved. Joint activities have played a critical role in this regard. Nonetheless, the norms for information sharing are largely ad hoc, and mechanisms are lacking to enforce or promote sharing, either through penalties or incentives. OI's operational plan for sharing information with the intelligence community provides no specific guidance on information sharing within the Terrorist Threat Integration Center, or with the broader intelligence community, DHS, or international organizations. If formal processes are not put in place, sharing could erode once the current emphasis on terrorism abates. **The Panel recommends that the FBI develop regular processes that promote sharing, such as tear-line products and information technologies. It specifically endorses the findings and recommendations of the 9/11 Commission concerning the need for improvements in information sharing and the potentially helpful role that incentives (and penalties) could play in the process.**

OI is pursuing a longer-term resource planning process to address needs, such as sensitive compartmented information facilities, information technology, and training, which require sustained investment over time. However, it must operate within the constraints of an annual appropriations process, in which resources must be distributed to meet competing demands in the near term. Although there may be an opportunity through a post-election supplemental to address some of the most pressing long-term needs of OI, such as building more sensitive compartmented information facilities, this would provide only short-term relief. **The Panel recommends that the Administration and Congress adopt at a multi-year appropriation process to address the need for sustained investment in some of these key areas.**

The 9/11 Commission report urges the FBI to establish an intelligence cadre composed of analysts, cross-trained agents, linguists, and technologists. Additional study is needed to understand its applicability to and impact on the special agent workforce. **The Panel recommends that the FBI develop intelligence career alternatives covering all intelligence analysts as soon as possible. Given the integration of intelligence, operations, and support activities and the extensive law enforcement and intelligence cross-training recommended by the 9/11 Commission for new recruits and supervisory agents, the Panel recommends that the FBI consider alternatives that enable highly flexible and mobile career paths within a single personnel system.**

CHAPTER FOUR
SECURITY

The FBI has undertaken an ambitious initiative to improve its security program, which includes creating a Security Division. This action has primarily resulted from the findings and recommendations of recent studies by the Commission for the Review of FBI Security Programs (Webster Commission) and RAND. The effective establishment and operation of the Security Division is critical to the FBI's counterterrorism and intelligence programs and its counter-intelligence responsibilities. It must ensure adequate security of its information, personnel, and facilities if other intelligence and law enforcement agencies are to share sensitive information.

The Webster Commission report, issued in March 2002 and conducted in response to the treason committed by Special Agent Robert Hanssen, outlined 29 recommendations for improving security. Significant deficiencies in FBI policy and practice were discovered, flowing from what the Commission characterized as pervasive inattention to security. It found that security often was viewed as an impediment to operations, and security responsibilities as a hindrance to career advancement. FBI culture emphasized the priorities and morale of its criminal components based on cooperation and the free flow of information internally. This work ethic contrasts with the compartmentalized characteristics of intelligence that often involve highly sensitive, classified national security information.

The RAND study, *Reinforcing Security at the FBI*, was completed in February 2003. RAND was charged with assessing how the task of security changed due to the events of 9/11 and FBI's revamped mission, as well as progress made in this regard. The study found that the FBI had made substantial progress in moving forward with the Webster Commission's agenda, most notably creating a Security Division with a cadre of security-minded professionals drawn mostly from outside agencies. However, RAND and FBI leadership noted that many important decisions remained, including the development of policies and procedures, commitment of resources, and determination of how information is to be shared inside and outside the FBI.

THE CURRENT PANEL REVIEW

This chapter addresses the FBI's progress in implementing the Webster Commission and RAND study recommendations, as well as the organization's overall security program. A list of the Webster Commission recommendations and the FBI's assessment of their implementation status as of September 2004 are provided at the end of this chapter.

The Panel's methodology included interviews with executive and staff officials at headquarters and eight field office locations, and a review of the 2004 strategic plan, numerous policy documents, and actions taken in response to the Webster Commission. The review concentrated on the following areas:

- **Security Structure.** The Webster Commission called for a separate security component that would assume certain personnel and information security functions, the acquisition and advancement of a career professional security workforce, and development of audit, analysis, and compliance units. The objective was to examine the status of the new Security Division, including the personnel, information system, technical, document, and physical security sections being developed.

- **Policies.** The Webster Commission called for the FBI to make major policy changes in its personnel security (financial disclosure, polygraph, and re-investigation); information security (information system certification, accreditation, and access auditing); document and access security (access to wiretap information and compartmented information); and active compliance/violation reporting and audit policies. The objective was to determine the degree of implementation and, to the extent possible, the effectiveness of these policies in addressing identified security deficiencies.

- **Personnel Security Investigations.** The Webster Commission recommended that the security component be responsible for security investigations and adjudications, improvements in the timeliness and thoroughness of the processes, and automation of the security process. The objective was to assess steps taken to implement these recommendations, their status to date, and the plan to achieve full implementation.

- **Security Incident Reporting and Discipline.** The Webster Commission called for an active program of identifying, reporting, and reviewing security compliance and violations, including active auditing of investigator file access, badge and access controls, and classified document handling controls. The objective was to assess how far the FBI has come in establishing a compliance reporting system and the degree to which the system identifies and corrects violations through disciplinary actions or other security approaches.

THE SECURITY STRATEGY

The FBI’s strategic goal for security is to establish an enterprise-wide security program that protects people, information, and capabilities. The goal’s objectives and related priority action items are the following:

- Protect the FBI from compromise of its employees.

    - Establish a security center of excellence to provide expert security guidance to the FBI and its customers.

    - Develop and implement a security division management information system that will document, track, and analyze data relevant to personnel security.

    - Establish and communicate well-defined security policies, providing guidance that is clear and well understood, and that facilitates compliance.

- Protect the FBI from compromise of its communications and information.

  - Bring the enterprise security operations center to full operating capacity in order to detect and prevent FBI network intrusions.

  - Establish an information system security manager program with program employees assigned to all operational and major support divisions.

- Protect the FBI from physical attack.

  - at FBI headquarters and in all field divisions.

To implement this strategy, the Security Division has a five-year strategic plan with its fiscal year 2004 portion included in the FBI's overall five-year plan. An evolving, unclassified document, the Division's strategic plan provides operational guidance developed through meetings with representatives of various operational components and field input. It reflects the FBI's transformation, including the underlying emphasis on intelligence and security needs associated with the intelligence function. Senior management agreed that most of the Webster Commission findings are valid, and found RAND's suggestions and recommendations helpful. Indeed, the plan is consistent with them.

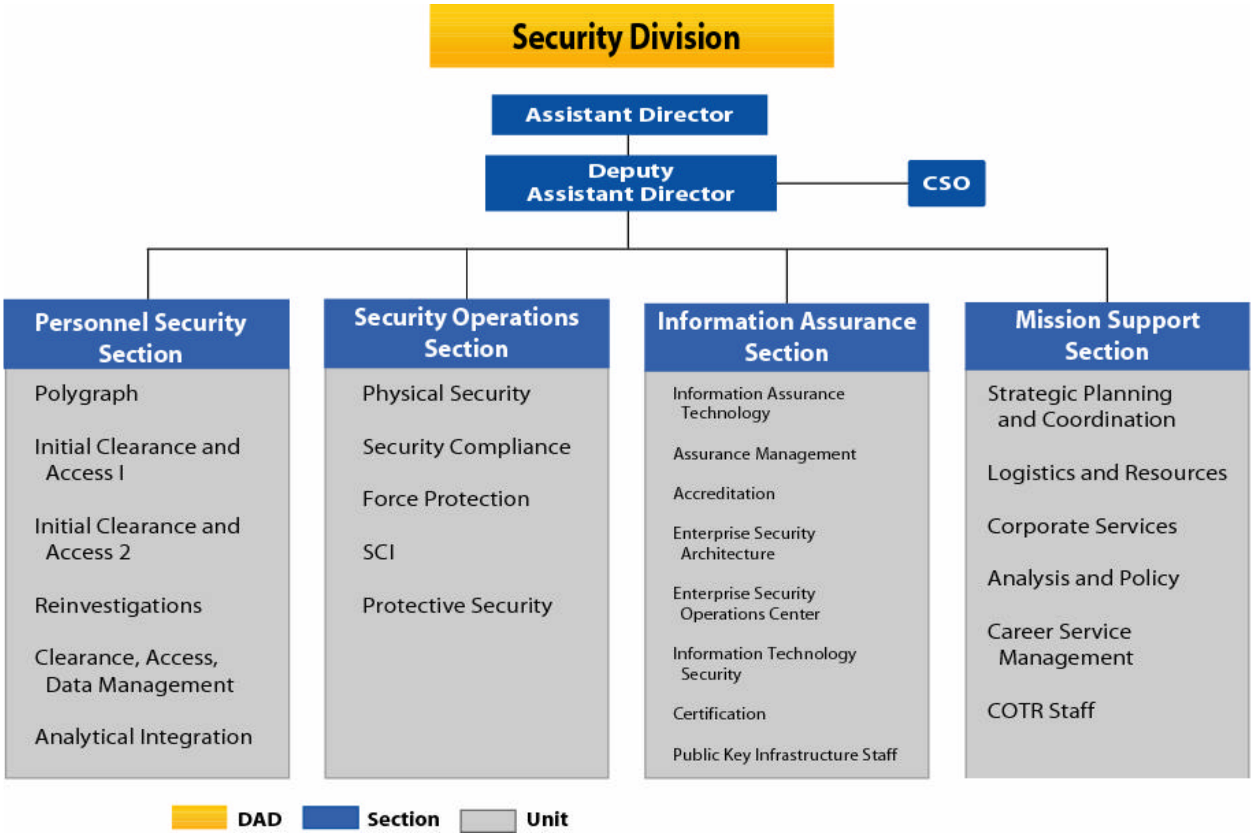
Goals and objectives contained in the Security Division's plan are to be measurable, attainable, and realistic; quarterly reviews are conducted for the units. Meanwhile, performance measures have been developed by headquarters section chiefs and through executive reviews conducted by the Assistant Director and his deputy. Due to limited automation, however, it is difficult to obtain accurate and timely data about accomplishments or clearances. The Webster Commission recommended an automated clearance process. The Division has not yet implemented an automated process. However, prototypes for tracking clearance cases and measuring individual performances are being tested.

Division leadership believes that an effective, functioning Security Division is years away given such challenges as budget requirements, staff, and organization. Competent security personnel must be recruited and trained, and budget requirements developed to support the other divisions. Adequate sensitive compartmented information facilities must be provided, but the funding strategy has not yet been finalized. Personnel are not "cleared" the same way as in other intelligence agencies, and employees work with different computer systems. Leadership believes a key issue is how fast the FBI can get to where it should be in the security area.

THE SECURITY DIVISION

The Security Division is being organized and managed as depicted in Figure 4-1 below.

Figure 4-1
Organization of Security Division


Security Division
Assistant Director
Deputy Assistant Director
CSO
Personnel Security Section
Polygraph
Initial Clearance and Access I
Initial Clearance and Access 2
Reinvestigations
Clearance, Access, Data Management
Analytical Integration
Security Operations Section
Physical Security
Security Compliance
Force Protection
SCI
Protective Security
Information Assurance Section
Information Assurance Technology
Assurance Management
Accreditation
Enterprise Security Architecture
Enterprise Security Operations Center
Information Technology Security
Certification
Public Key Infrastructure Staff
Mission Support Section
Strategic Planning and Coordination
Logistics and Resources
Corporate Services
Analysis and Policy
Career Service Management
COTR Staff
DAD
Section
Unit

The Division is managed by an Assistant Director and Deputy Assistant Director. The FBI's Chief Security Officer reports directly to the latter. The Division is comprised of four sections: Personnel Security, Security Operations, Information Assurance, and Mission Support.

- **The Personnel Security Section** protects FBI personnel, facilities, and information by ensuring the trustworthiness of FBI employees and others through initial security clearance investigations, periodic re-investigations, and counterintelligence measures. This section has established priority areas to support the Division's goals, specifically:

    - to improve the FBI's capability to make accurate and timely judgments regarding the trustworthiness of applicants, employees, contractors, and others who require access to FBI information or facilities

    - to develop an integrated, automated, security information collection and management system that facilitates case tracking, data exploitation, and mining, analysis, and risk mitigation and monitoring

    - to institute a formal program to identify and track the progress of action plans in personnel security cases when derogatory information exists but is insufficient in severity to revoke access

- **The Security Operations Section** provides security services and products that assist in the protection of FBI personnel, facilities, information, and operations through selective initiatives. These initiatives include physical and technical security assistance, security policy and training, sensitive compartmented information programs, police force management, security compliance, risk analysis, industrial security, continuity of operations, critical mission assurance, and field security support.

- **The Information Assurance Section** protects the FBI's digital information through practical and effective security techniques. To do this, it has established priority areas: ensure that those with access to classified and sensitive information processed by FBI information systems have proper security clearance and are adequately trained; ensure the availability of information processed within the information systems with the proper security safeguards; infuse the organization's enterprise system with necessary security technology; and establish a comprehensive, consistent, and centrally managed information assurance program that institutes lifecycle security.

- **The Mission Support Section,** the latest component added to the Division, provides comprehensive planning, communications, reporting, administrative, logistics, risk analysis, policy, training, and other support services to enable the Division to achieve its mission.

One key organizational issue remains to be resolved. The Webster Commission recommended consolidating personnel security activities, which includes the Background Investigation Contract Services (BICS) component currently located in the Administrative Services Division. There is a proposal to transfer BICS to the Security Division and interviews with personnel offered differing views concerning this approach. This issue is addressed in more detail later.

The Security Division is a work-in-progress. Its organizational structure recently increased from three to four sections, and it has filled only 145 of the 213 positions allocated for the Personnel Security section. Moreover, few security officer positions have been filled by non-special agent employees as directed by a policy that has been met with mixed feelings in the field. The Division is acquiring security experience from other federal agencies to address its mission goals, including detailees and permanent hires from CIA and DOD. Those interviewed expressed energy and commitment to the FBI's mission, attempts to professionalize the Division, and security requirements. Almost without exception, however, serious concern was expressed about FBI's hiring processes, which were characterized as bureaucratic, laborious, and risk averse. The FBI vetting process is both a suitability and security clearance process. One manager reported that the FBI clearance process is more cumbersome and bureaucratic than the security clearance processes that other agencies use.

Most of those interviewed at headquarters also expressed concern or alluded to an organizational culture that values input from special agents over other employees, and an insistence on doing it "the Bureau way." This has caused Security Division unit managers to operate with little or no staff for long periods, and to lose prospective employees to other agencies or companies because of the lengthy hiring process.

FIELD STRUCTURE AND SUPPORT

Risk management techniques permit the Security Division to analyze field needs, assess trends, identify security gaps, and define budget requirements. Different security structures exist in the field depending on the size and risk level for each office. The Division expects security officers, who are trained in analytic risk management, to use risk level analysis information when working with their Special Agents in Charge to make security decisions that impact their field offices. Analyzing risk assessment reports from headquarters and field security officers, headquarters staff produces a classified summary report that the Division uses to prioritize budget and strategic planning.

Most Special Agents in Charge and Assistant Special Agents in Charge in the field are directly involved with security issues, according to Security Division executives interviewed. The Inspection Division is provided with Security Division "check lists" to assist in its inspections and ensure that Security Division policies are adopted and followed. In addition, the Security Division has initiated a program in which special agents from one field office can participate in inspecting another office. The Inspection Division also provides reports to the Security Division on the number and type of issues identified during its field office reviews. Interviews with Special Agents in Charge and Assistant Special Agents in Charge revealed understanding and support for the security officer position, as well as for the skill sets required. At all the offices visited, security officers reported to the Special Agent in Charge and preferred this structure due to the importance and sensitivity of security issues.

From an operations standpoint, the FBI's strategic plan calls for transitioning to a professional security officer cadre responsible for field office security. This goal is consistent with the Webster Commission's recommendation to develop a professional security staff through enhanced selection, training, and retention. Field security officers are almost exclusively GS-13 special agents, but the Director is seeking to fill all of these positions with non-special agents within five years. A career development program for security officers is being developed to accomplish this objective, which will include a Security Careerist Advisory Committee to assist in determining the most effective program elements and structure. The committee, to be composed of support personnel and security officers from headquarters and field, also will review draft security policies, provide feedback, and facilitate policy implementation. Position descriptions for security officers have been developed for GS-13 through GS-15, demonstrating support for the career development program.

The security officer position is becoming more professional, as demonstrated by the following:

- All security officers are required to complete basic security officer training and attend such additional training and security conferences as intermediate, advanced, and modular courses.

- Security officers in field offices report to no one lower than the number two official in the offices.

- Security officers sit at the management table and serve as counselors to the Special Agents in Charge.

- The Security Division has input to Special Agent in Charge evaluations.

- Additional security support positions are being hired for field offices.

Interviews with field office security officers and management officials revealed that filling all security officer positions with non-special agents is a somewhat controversial goal. Although the positions are currently filled almost exclusively by special agents, a limited number of non-special agents with security-related backgrounds hold these positions. Several interviews with special agents serving as security officers revealed strong views that special agents should perform this role. They stated that security officers are required to conduct sensitive employee interviews, handle potential breaches of physical security, address policy issues that impact special agent investigations, and address potentially volatile incidents when employees are subjected to disciplinary actions. They contended that special agents are very experienced in handling such incidents, know how to blend their job requirements with security requirements, and are authorized to carry firearms, a necessity to ensure safety in volatile situations.

At the same time, special agents interviewed in the field expressed little interest in pursuing a long-term career as a security officer if the position was going to be non-law enforcement. This lack of interest is due primarily to special agents not wanting to transfer to a non-law enforcement job series position with less perceived professional status, no authority to carry a firearm or receive law enforcement availability pay, and a different retirement plan.

Most field managers understood the decision to utilize non-special agents who they acknowledged could perform effectively so long as they have a security background, learn the issues facing special agents, and approach the position in a professional and knowledgeable manner. Meanwhile, senior level managers in the Security Division believed that special agents would be good security officers due to their training and background as criminal investigators.

Security officer and management official interviews also revealed concerns about limited staffing. This was especially true in field offices with numerous resident agency offices, where security officers were involved with constructing new office sites, where offices handle a large volume of classified information, and where other physical security demands were present.

SECURITY POLICIES

The FBI's goal is to build an analytical capability into all security processes to assess risk, knowing that some degree of risk always will exist. Policy documents are reviewed to ensure that they are consistent with risk management issues and that policies are understandable, efficient, and enforceable. The Senior Security Policy Advisory Board has been formed to vet policy issues.

To help achieve this goal, the FBI is preparing a new web-based security manual and updating its security policies. In the meantime, there appears to be some confusion about what security policies are in effect. Several security officers interviewed were unaware of all security policies that emanate from FBI headquarters or impact field operations. For example, some offices were confused as to whom the security officer should report. One office, which recently underwent an Inspection Division review, was informed that the policy was for the security officer to report to the Special Agent in Charge, not the Assistant Special Agent in Charge as was the case at that location. It seems the Inspection Division was unaware of the electronic communication permitting the security officer to report to an Assistant Special Agent in Charge.

It was expected that the new policy manual, to be issued in November 2004, would be developed separate from the two existing FBI manuals, the Manual of Administrative Operations and Procedures and the Manual of Investigative and Policy Procedures. The Director has authorized removing security policies and procedures from the other manuals except for specialized policies related to legal attaché offices, foreign counterintelligence, and the Security Division itself.

A new financial disclosure program policy has been approved. In fiscal year 2003, the Attorney General determined that within the FBI, financial disclosure requirements would generally apply to all personnel – including contractors, detailees, etc. – with access to sensitive compartmented information (SCI). Implementation of the requirement is being phased in by the FBI. Currently, SES personnel with SCI access and employees stationed at Legal Attaché offices are required to submit financial disclosure filings. While, at present, there is no requirement to include all special agents in the financial disclosure program, there is a system that uses commercial databases to examine the finances of certain employees where possible vulnerabilities or problems are indicated.

The FBI is taking steps consistent with the Webster Commission's recommendation to develop a counterintelligence polygraph policy and program, and create an infrastructure to support it. The FBI is using a phased approach to administering polygraphs to its employees. In addition to all newly hired employees, employees in sensitive positions are to be examined first, followed by employees and contractors in counterintelligence, counterterrorism, and security. In 2002, 7,767 examinations were administered; in 2003, 8,277 examinations were administered; and, in 2004 (through December 5th), 10,773 have been administered.

Overall, the FBI has made considerable progress in implementing the polygraph program. Officials at field offices visited reported that special agents actually sought positions as polygraph examiners. Twenty-two polygraph examiner positions were added in fiscal year 2004, bringing the Security Division's complement to 51 examiners though not all of the positions have been filled. The program is augmented by 85 examiners in field offices. The Division recently initiated a regionalized approach to management of examiners, a development that has been well received by examiners and field security personnel.

At the same time, field visits found that not all special agents in sensitive positions had been examined. For example, a Senior Supervisory Agent, who manages a foreign counterintelligence squad and worked in one for several years, reported that he never received a polygraph examination. Policy consistency is crucial to the credibility and viability of the program. Field office officials and special agents understood the need for the examinations, and security officers believed it was necessary for the polygraphs to be administered by those outside the office being examined.

Security education is crucial if personnel are to understand and ultimately accept FBI policies related to security. This education has been a major undertaking, in part because not all managers are overly supportive of security issues. All headquarters personnel have attended a general security awareness training program, and all security officers interviewed engage in similar exercises at their field offices. New agent training includes courses on security, as well.

PERSONNEL SECURITY

All FBI employees must undergo a security background investigation and adjudication process in order to receive a top secret clearance. This is a condition of employment, with new hires, regardless of age or previously held clearances, required to provide information dating back to their sixteenth birthday. However, new employee vetting is both a suitability and security clearance process. For example, a prospective employee may qualify to have a security clearance despite minor drug use in the employee's teenage or college years, but he or she may not be eligible to be employed as a law enforcement agency employee since the employee would be involved in, and associated with drug enforcement matters. Some managers and other employees view this rigorous pre-employment process, which historically has taken six to nine months to complete, as inefficient, cumbersome, and a roadblock to the FBI's mission.

Once an individual receives clearance and starts work, he or she is re-investigated every five years. Depending on the employee's assignment, access to sensitive compartmented information also may be necessary, thus requiring a polygraph examination. Contract personnel must undergo similar background investigations.

Personnel security is an important risk management issue given the unpredictability of human behavior. The baseline clearance for FBI employees is top secret, though this context has been used in conjunction with "law enforcement sensitive" information. In other words, day-to-day application relates to a criminal investigation or law enforcement work perspective, not a national security point of view. This is a crucial distinction during the FBI's adjudication process, which traditionally has been performed with greater attention paid to the suitability criteria for employment and less on security. The FBI now is seeking a better balance between the two perspectives.

The FBI uses BICS to obtain background information on individuals. BICS has approximately 1,500 private contractors, many of whom also work for other companies and have former law enforcement experience. The Security Division uses the BICS information to make security adjudication decisions, while the Administrative Services Division uses it to make suitability decisions related to new applicants. Security Division executives and managers believe that BICS should be brought into its component and placed under the supervision of the Personnel Security Section to ensure the quality and integrity of the security clearance process. In contrast, Administrative Services Division leaders believe that background investigations should remain with them, and saw two different adjudicators reviewing the same data as a strength. Thus, the Administrative Services Division judges suitability and the Security Division judges security. The Webster Commission recommended that security investigations and adjudications be consolidated in a new Office of Security—now the Security Division—with responsibility for improvements in timeliness, thoroughness, and automation. This recommendation is awaiting decision.

The Personnel Security Section has a funded staffing level of 213 individuals, yet only 145 positions have been filled. There has been some thought that building a cadre of security managers is hindered by a fundamental conflict within the organization. Some division personnel believe they cannot hire or promote non-special agents into managerial positions. Yet the Security Division has more support employees at the GS-14 and GS-15 levels than it has special agents. Consideration is being given to a security career track similar to the CIA's, where security specialists can advance to higher levels and take management positions.

Controls have been significantly tightened with regard to interim clearances, though the need for such clearances has been recognized for exceptional circumstances. According to FBI guidelines, interim clearances last for 180 days, though an extension can be granted due to issues beyond the control of the individual being investigated. Background investigations are conducted simultaneous with the period that the interim clearance is in effect. Data were not available to generate statistics on interim clearances approved.

Processing clearances for state and local law enforcement personnel serving on the Joint Terrorism Task Forces has been timely; GAO gave the FBI a favorable rating. This is partly due to the decision to accept background investigations done by state and local law enforcement agencies so long as the FBI can subsequently fill any identified gaps. This policy was vetted and accepted by the Defense Intelligence Agency, CIA, and other intelligence agencies. Field office interviews revealed that there were lengthy delays in clearing Joint Terrorism Task Force officers prior to their working with the FBI during the immediate post 9/11 period. Although it still takes considerable time to clear new task force members, it does not approach the prior delays.

INCIDENT REPORTING AND DISCIPLINE

The Security Division has two units to address security violations: the Security Compliance Unit and the Analysis and Investigations Unit (formerly the Analytical Integration Unit as shown in Figure 4.1). The former investigates security violations from an incident standpoint, addressing damage assessments, the reasons for violations (training requirements, policy deficiencies, or lack of awareness), their severity, and their criminal or administrative nature. Its workload is composed overwhelmingly of security incident investigations with the remainder being specialized work associated with Foreign Intelligence Surveillance Act or other agency requirements. The Analysis and Investigations Unit handles investigations and potential adjudications for personnel involved with security-related incidents. The Security Division uses information developed by the Analysis and Investigations Unit to determine whether an employee's security clearance should be revoked.

Although the Security Division is responsible for deciding security consequences for an employee's actions related to a security violation—such as revoking a security clearance—the Office of Professional Responsibility investigates an employee's actions for possible discipline. The Security Division cooperates with that office during such inquiries.

Headquarters' senior management is very pleased with the progress made to date concerning security incident reporting and discipline. A unit chief and staff for the Security Compliance Unit are in place, and the Security Division has done some trend analysis regarding the types of violations that occur and assistance requested by staff. Training is provided on how to avoid similar security incidents and ways to handle incidents when they occur. Internal newsletters are distributed that report security disciplinary problems and corrective actions. A working group of agents and support staff assists in receiving feedback to enhance security policies.

Leadership does not believe there is an aversion within the FBI to disciplining employees for security violations. Violation self-reporting is encouraged without penalties that are so harsh or punitive as to be counter productive. Most violations are found to be mistakes. The Security Division views its challenge as identifying the cause of the mistakes and minimizing reoccurrence. Approximately 290 security incidents were reported in 2003, compared with 150 incidents reported for the prior 10 years, demonstrating that security is becoming a recognized priority. FBI management believes this process enhances security by identifying the reasons for mistakes, permitting refined and improved security polices, and identifying security gaps.

Field office inspections also identify security problems. Prior to 9/11, the inspection process did not give detailed attention to security issues. In early 2003, the Inspection Division began to do a more thorough review of security matters. As mentioned earlier, security officers from one office now participate in the inspection of other offices, significantly helping the quality of the inspections performed and the development of their colleagues' expertise. The approach is designed to improve the security program by identifying required corrective actions while not being perceived as a "gotcha." However, any egregious matters are identified and referred to the Office of Professional Responsibility for resolution. Security officers interviewed in the field have voiced an understanding of their inspection assignments and reported very positive experiences related to knowledge gained of approaches used.

Only one of the eight field offices visited acknowledged any serious security incidents by special agents. Many security officers said the incidents they encounter are self-reported, such as mistakes occurring while agents address investigative needs. They said that employees usually are accepting of the security rules once they are informed of the reasons for them. They further stated that additional training is necessary as the FBI evolves into an agency that handles considerable amounts of classified information related to national security matters.

INFORMATION TECHNOLOGY

When the Security Division was established, it took over information assurance responsibility from the Information Resources Division. The FBI's strategy for improving information technology security has been to hire outside expertise and have them work closely with the Chief Information Officer. This strategy is well underway at headquarters and appears to be working. A key element is to raise awareness of security concerns throughout the FBI; based on discussions at headquarters and in the field, staff are well aware of the need to provide adequate information security.

The Security Division initially has focused on assessing and improving security of existing systems. An accreditation process for information technology systems was created in which the Division identifies and certifies the systems, while the Chief Information Officer accredits them. As of late August 2004, this headquarters-led program had identified 224 systems, of which ninety-six had been certified and accredited, seventy-nine were in progress, and forty-nine were beginning the process. The majority of those systems are headquarters-based and the Division is actively identifying field office systems to move them through the certification and accreditation process. Re-accreditations will be required every three years.

As part of the Trilogy modernization, much of the FBI systems' administrative control was removed from field offices and placed in headquarters. The intent is to better control activity on the network and limit add-on software. The Enterprise Operations Center was created to centrally manage the network. According to information technology specialists interviewed, this centralized approach appears to be working. An important by-product has been the ability of headquarters to provide much greater security control over the systems.

Network access soon will be controlled by smart card and PIN technology, and badges will be required to access both facilities and systems. A new public key infrastructure based on this smart card and PIN technology has been tested, and is awaiting final issuance of badges.

The Security Division recognizes that insiders represent the greatest threat to the FBI's networks. Consequently, it has created the Enterprise Security Operations Center to monitor activity on the FBI's closed networks, as well as Internet usage. Its network monitoring tools detect anomalies in activity and help investigate them. Eventually, the center will work on all FBI networks, including those at headquarters, legal attaché offices, resident agencies, field offices, and Joint Terrorism Task Forces. In the interim, it is taking a risk management approach for monitoring work, focusing early efforts and resources where a loss would have the greatest cost. Thus, it is monitoring the classified information network and doing some rudimentary work on the Trilogy backbone. Once accreditation for Trilogy's software monitors is received, more extensive work will be performed. It is envisioned that the center eventually will perform vulnerability scanning and some penetration testing of high risk systems under controlled conditions.

A key facet of the Enterprise Security Operations Center's effectiveness is the deterrent effect it has on employees browsing information in restricted networks. For this to work, however, employees must believe that their activities are being monitored. During field office visits, system users were sampled; although none had heard of the center per se, all indicated their belief that their on-line activity in the FBI's systems was being or could be monitored.

Although the Security Division is responsible for managing information technology security, field office security is not organized in that fashion. Field security officers handle personnel and physical security, but they are responsible for information technology security in name only. While headquarters is developing policies regarding the use of such specific technologies as personal electronic devices, as well as the lock-down of external input/output devices on personal computers, centralized guidance for these areas is lacking. A wide variety of security measures are in place at different offices. For example, project staff visits showed that cell phones with photographic capability were allowed in some headquarters and field offices, but not in others. Equally important, however, is policy and rationale training so that the workforce accepts limits imposed on the use of technology to perform the job. Of those officers interviewed, all rely heavily on local office information technology expertise, which has been somewhat mitigated by the centralization of administrative control of the FBI's networks. The Division is looking to staff field offices with information system security managers and officers to ensure the security of key field systems. This is a useful long-term goal, but a more pressing challenge is to ensure that field security officers are properly selected and trained to manage their responsibilities.

CLASSIFIED INFORMATION

In the post 9/11 intelligence sharing environment, the FBI is handling significantly more classified information for national security purposes. Handling this information must be done in accordance with strict procedures which include sanctions for improper disclosure. Since these procedures can potentially impede information sharing, field offices were asked about their experiences with classified information. Of particular interest was how the Joint Terrorism Task Forces shared counterterrorism information. It was determined task force members were cleared to handle classified information. Although the clearance process was initially cumbersome, that challenge since has been largely overcome. The project staff found several instances where state and local task force members could not share classified information with their departments. In those cases, their chiefs received clearances so that the members could share the information, if necessary.

In some cases, the members worked around the problem by "dumbing down" the information or simply asking others to do things based on their trust, which some agents said resembled working on political corruption cases. Only one individual tried to go back to the originating agency to get information declassified. That process took several weeks, essentially making the information useless. Every individual with whom this issue was discussed reported that if it came down to sharing critical information for public safety purposes or following security rules, they would choose the former. In effect, the time-critical need to share information provides the need to know.

The secure and effective handling of classified information will require a substantial increase in the space devoted to sensitive compartmented information facilities (SCIF) at FBI headquarters and in the field. Although the Liberty Square project will accommodate much of this need for Counterterrorism Division and alleviate some headquarters crowding, major SCIF space needs remain in field offices where most work with highly sensitive intelligence material is relegated to small communications and computer terminal rooms. Even recently constructed facilities, such as the Baltimore field office, have limited room for highly sensitive work or meetings. The FBI is revising SCIF requirements to ensure sufficient specialized space is provided for in field offices. The FBI is attempting to get away from the use of small rooms, instead building or retrofitting entire floors as SCIFs to allow intelligence, counterterrorism, counter-intelligence, cyber and some criminal personnel to work together and handle classified information readily.

The provision of this space, though necessary, will be very costly. Providing adequate SCIF space for a single field office is estimated to cost between $2-5 million, depending on the size of the field office and whether SCIF space is built as part of new facilities or existing facilities must be retrofitted. SCIF space requirements have been discussed with Office of Intelligence executives, who are well aware of these needs and are attempting to address budget requirements. Only $11 million are available in the 2005 budget for SCIF construction, which clearly is insufficient considering the number of buildings without adequate space. Most, if not all, of the approximate 800 intelligence analysts being hired will require SCIF space to effectively perform their duties. The FBI believes that significant additional funding will be needed, and agree it could require as much as $125-250 million for such space over the next five years.

An internal FBI study is forthcoming on the management of classified information; it will include a review of how classified information is transported, handled internally, stored, processed, and destroyed. In the meantime, the FBI is strengthening the process for properly destroying classified or sensitive documents.

FINDINGS AND RECOMMENDATIONS

The FBI has made significant progress in developing a viable security organization with an evolving structure that meets the demands of establishing a new division. The Webster Commission identified 29 recommendations, twenty-one of which have been addressed and are considered implemented. A significant number of new personnel have been hired, and a security officer cadre is being professionalized to meet the demands of an intelligence-driven agency. Security policies are being developed that implement a risk management approach to security. And, a significant number of technology system certifications and accreditations have been made. At the same time, a fully mature Security Division remains several years away. To assist in its development, the Panel makes the following recommendations:

The FBI's strategic goal for security is to establish an enterprise-wide program that includes protection of the FBI from compromise of its employees, its communications and information, and physical attack. To implement this strategy, the Security Division has a five-year plan, covering 2001 to 2006, with its fiscal year 2004 portion included in the FBI's current overall five-year strategic plan. **The Panel recommends that the FBI develop performance measures for all essential elements of security operations.**

During interviews with personnel security investigation staff, reliable quantitative management data could not be provided to make judgments regarding management's accomplishments and needs. This problem stems in part from inadequate information technology systems. **The Panel recommends that the Security Division complete a management information system that provides accurate and adequate statistical information on security.**

Numerous security policies have been developed and issued via executive communications. However, headquarters and field personnel interviewed often were not aware of these policies. This is due in part to the lack of a complete up-to-date listing of policies in one place, where the policies may be referenced systematically. A new web-based security manual is due to be completed in November. **The Panel recommends that the new security policy manual be completed and issued as soon as possible.**

Educating FBI staff about their security responsibilities has been a major undertaking. However, not all employees are aware of the various policies and not all managers are overtly supportive of security issues. **The Panel recommends that each manager's performance appraisal include a critical element that relates to the manager's understanding of security rules and procedures and the security awareness of his or her subordinates.**

The FBI's new security structure and policy requirements are being addressed by existing staff at headquarters and in the field offices. In all of the interviews conducted, a lack of personnel to carry out these new duties was indicated. **The Panel recommends increased support staff and physical and technical security resources for the field offices to implement the FBI's strategic plan relating to security.**

The FBI uses the Background Investigation Contract Service to obtain required background information on individuals. The Webster Commission recommended consolidating security investigations and adjudications in a new Office of Security. A decision about which division – Administrative Services or Security—has managerial responsibility for BICS is needed. **The Panel recommends that security investigation and adjudication responsibility (for security, as well as suitability) be placed within one division, regardless of which division is selected.**

The Webster Commission recommended that the FBI's personnel security process be automated. Yet the FBI's system for processing security background investigations, re-investigations, and adjudications continues to be paper intensive. Lack of automation creates inefficiencies that are partially responsible for the length of time taken to complete the security clearance process. Likewise, the BICS process should be automated and integrated with the application/background investigation programs. **The Panel recommends that whichever division is given responsibility for security investigations and adjudication, that division give high priority to accelerating automation of the personnel security process.**

The large number of new special agents and support staff being hired has placed considerable pressure on the FBI to complete applicant and security background investigations in a timely way. BICS has not been able to complete all interviews in the time period required. To achieve its agent and support hiring goals for fiscal year 2004, the FBI supplemented its contract services' workforce with special agent resources. This is a less than ideal use of these resources. The current peak in new hires and the reinvestigation demand outstrip BICS' capacity, which has remained level over the past five years. The hiring process' background investigation period cannot be shortened until there are additional investigators to perform the function, accounting for the largest percentage of the time required for hiring applicants. **The Panel recommends that the FBI supplement BICS by utilizing additional private contractors who specialize in federal background investigations when attempting to clear large numbers of applicants or contractor personnel.**

The FBI's process enables the Director of Security to certify the security of an information technology system, and the Chief Information Officer to accredit it. The system's user or owner is not formally involved in this process. Last year, the Academy Panel recommended that the user or owner be responsible for accreditation and agree to accept any security risks. Although the Chief Information Officer's involvement is necessary, the current process does not recognize the responsibility of risk that should be borne by the user or owner. **The Panel recommends that system users or owners be formally involved in the accreditation process with the Chief Information Officer and the Security Division.**

Sensitive compartmented information facilities (SCIF) are essential if an intelligence organization is to adequately protect classified information and work effectively with other intelligence agencies. Currently, the FBI does not have adequate SCIF space to address the operating requirements of counterterrorism, counterintelligence, and intelligence personnel. It is estimated that the FBI will require $125 to $250 million for SCIF space over the next five years. In addition, most, if not all, of the approximately 800 intelligence analysts being hired will require such space to effectively perform their duties. The lack of secure space may cause a serious morale problem and risk underutilizing highly sought-after analytic resources. **The Panel recommends that the FBI request additional funding to adequately address SCIF deficiencies over the next five years.**

The FBI is receiving more classified national security information than ever before. Based on field interviews, it appears that information will be shared in emergency situations, regardless of its classification. In practice, the time-critical need to share classified information provides the need to know. **The Panel recommends that the FBI adopt explicit procedures to monitor classified national security information sharing to ensure that necessary sharing occurs and that the discretion demanded by the practical need to share is not abused.**

The Security Division is looking to staff field offices with information system security managers and officers to ensure the security of key field systems. This is a useful long-term goal, but field office visits indicate that a more pressing problem is to ensure that security officers are properly selected and trained to manage these responsibilities. **The Panel recommends that when selecting new security officers, the Security Division specifically address their qualifications and credentials for managing security of information technology systems, as well as provide information system security training for current security officers.**

WEBSTER COMMISSION RECOMMENDATIONS
AND STATUS OF FBI IMPLEMENTATION

GENERAL RECOMMENDATIONS:

1. A system should be established so that significant security lapses in an entity within the intelligence community lead to improved security measures across the community.

Status: Recommendation closed (Approved 6/17/2003)

2. The Bureau should within six months submit to Congressional intelligence oversight committees, through the Attorney General, a plan addressing weaknesses in its security programs, and it should submit annual reports on its efforts to implement that plan.

Status: Recommendation closed (Approved 6/17/2003)

INFORMATION SECURITY

3. Comprehensive, consistent, and centrally coordinated information security policies should be adopted.

Status: Recommendation closed (Approved 10/28/2003)

4. Information security education and training must be implemented.

Status: Open; the development of an information system security manager and information system security officer training courses will be completed during the first quarter fiscal year 2005, and an advanced security officers' course will be piloted in fiscal year 2005.

5. Key information security positions must be filled and supported.

Status: Recommendation closed (Approved 5/09/2003)

6. The FBI must institutionalize a formal, tailored process to certify and accredit computer systems.

Status: Recommendation closed (Approved 10/28/2003)

7. The FBI should develop a comprehensive, prioritized plan to address security shortcomings.

Status: Open; a certification accreditation and reporting application process will be implemented in the fourth quarter of fiscal year 2005.

PERSONNEL SECURITY

8. Security investigations and adjudications should be consolidated in a new Office of Security.

> **Status: Open; the Security Division has prepared and delivered to the Executive Assistant Director for Administration a white paper recommending the transfer of responsibility for the Background Investigative Contract Services program (BICS) to the Security Division. This will be closed upon a decision by FBI executive management.**

9. The personnel security process should be automated.

> **Status: Open; a complete formulation of the information automation and management program team is scheduled for completion in fiscal year 2006; scattered castles will be implemented within the FBI in fiscal year 2005 to include development of an on-line visitor request form; and a security management information system will be developed in modular form between fiscal year 2005 through fiscal year 2011**

10. BICS investigations should be thorough.

> **Status: Open; the Security Division, in conjunction with Administrative Services Division, will improve quality of BICS investigations by the third quarter fiscal year 2005, through more advanced training.**

11. Adjudicator training should be improved.

> **Status: Recommendation closed (Draft)**

12. Stricter controls should be placed on interim clearances.

> **Status: Recommendation closed**

13. The FBI should adopt a financial disclosure program and develop a technical structure to support financial monitoring.

> **Status: Recommendation closed (Approved 10/02/2003)**

14. The FBI should implement a counterintelligence polygraph program and create an infrastructure to support the program.

> **Status: Recommendation closed (Approved 08/07/2003)**

DOCUMENT and PHYSICAL SECURITY

15. Classified national security documents should be handled and stored in SCIFs and secure areas and available only to those with a need to know.

> **Status: Open; FBI will complete by the fourth quarter fiscal year 2005, via a commercial institution, a study focusing on document security procedures, including the use of technologies for document tracking and recording.**

16: The security access control badge system and the FBI Police Program should be strengthened.

> **Status: Recommendation closed (Draft)**

17. The Bureau should enhance protections on the handling, copying, and disposing of classified material.

> **Status: Recommendation closed (Draft)**

18. Written guidance on top secret and sensitive compartmented information should be current, clear, and in compliance with Director of Central Intelligence directives and Executive Orders.

> **Status: FBI is continuing to review and develop implementation processes for new security policy and procedures manual; scheduled for delivery in Novermber of 2004.**

19. The operations of the Special File Room should be improved by eliminating unnecessary classified material and enhancing staffing, training, and equipment.

> **Status: Recommendation closed (Approved 8/28/2003)**

20. SCIF operations must be improved by promulgating clear, enforceable rules and providing training for SCIF tenants.

> **Status: Recommendation closed (Approved 7/15/2003)**

21. The FBI should consider adopting the Human Intelligence Control System (HCS).

> **Status: Open; based on a recommendation of a working group with the CIA and the HCS Secretariat, the FBI will complete by fourth quarter FY 2005, a feasibility study on adoption of an HCS.**

22. The Foreign Intelligence Surveillance Act (FISA) process should be simplified, and access to FISA information in Automated Case File System should be restricted.

Status: The Security Division has completed those actions for which it is responsible. The Criminal Division is responsible for all other related FISA issues.

23. A central security authority must coordinate and oversee all document and physical security violations and compliance activity.

Status: Recommendation closed (Approved 7/15/2003)

24. FBI policy manuals should require security coordination.

Status: Recommendation closed (Approved 10/08/2003)

SECURITY STRUCTURE

25. FBI security programs should be integrated in an Office of Security that reports to the Director.

Status: Recommendation closed (Draft)

26. The Office of Security should develop a professional security staff through enhanced selection, retention, and training programs.

Status: Open; the FBI plans to hire a security support coordinator to assist security officers at FBI headquarters and field offices, and establish a career track for professional security officers. A business plan to accomplish these actions will be formulated by second quarter fiscal year 2005.

27. The Office of Security should implement comprehensive employee security education and awareness programs.

Status: Recommendation closed (Approved 10/28/2003); the Security Policy Operating Manual is scheduled for delivery 11/2004.

28. The Office of Security should develop a centralized security violation reporting program.

Status: Recommendation closed (Approved 10/08/2003)

29. The Office of Security should audit security programs.

Status: Recommendation closed (Draft)

PANEL AND STAFF

PANEL

Dick Thornburgh,[*] *Chair*—Counsel, Kirkpatrick & Lockhart. Former Under Secretary General, Department of Administration and Management, United Nations; Attorney General of the United States; Governor, State of Pennsylvania; U.S. Attorney for Western Pennsylvania; Assistant Attorney General of the United States, Criminal Division.

Robert M. Alloway*—Director, National Leadership Task Force on Y2K. Former Professional Staff Member, Subcommittee on Government Management, Information and Technology, U.S. House of Representatives; President, Alloway Incorporated; Assistant Professor, Sloan Graduate Business School, and Research Faculty, Center for Information Systems Research, Massachusetts Institute of Technology; Director, Management Information Systems, First National Stores.

Frank J. Chellino—Criminal Justice Consultant; Former Special Agent in Charge, Miami Field Division, U.S. Drug Enforcement Administration (DEA); Vice Chairman, Executive Committee, Washington/Baltimore High Intensity Drug Trafficking Area. Prior Headquarters positions with DEA: Deputy Assistant Administrator, Office of Inspections; Unit Chief, Office of Security Programs. Prior positions with DEA: Special Agent in Charge, Washington Division Office; Supervisory Senior Inspector, Public Information Officer, Special Agent, Miami Division Office; Special Agent, New York Division Office.

Martin C. Faga*—President and Chief Executive Officer, The MITRE Corporation. Former positions with The MITRE Corporation: Executive Vice President and Director, Department of Defense Federally Funded Research and Development Center; Senior Vice President and General Manager, Center for Integrated Intelligence Systems; Member, Technical Staff. Former Assistant Secretary of the Air Force for Space; Director, National Reconnaissance Office, U.S. Air Force; Professional Staff Member, House Permanent Select Committee on Intelligence.

Kristine M. Marcy*—Consultant, McConnell International. Former Chief Operating Officer, Small Business Administration; Senior Counsel, Detention and Deportation, Immigration and Naturalization Service; Assistant Director for Prisoner Services, U.S. Marshals Service, U.S. Department of Justice; Associate Deputy Attorney General, Office of the Deputy Attorney General, U.S. Department of Justice; Acting Director/Deputy Director, Office of Construction Management and Deputy Budget Director, U.S. Department of the Interior; Deputy Assistant Secretary, Office of Civil Rights, U.S. Department of Education; Assistant Director, Human Resources, Veterans and Labor Group, U.S. Office of Personnel Management.

Robert J. O'Neill, Jr.*—Executive Director, International City/County Management Association. Former President, National Academy of Public Administration; County Executive, Fairfax County, Virginia. Former positions with the City of Hampton, Virginia: City Manager;

[*] *Academy Fellow.*

Assistant City Manager for Administrative Services; Management Systems Coordinator; Management Intern; Director, the Public Employment Program. Former Director of Management Consulting Services, Coopers and Lybrand; Regional Manager, Management Improvement Corporation of America.

PROJECT STAFF

J. William Gadsby—*Vice President*, *Academy Studies*. National Academy of Public Administration; Responsible Academy Officer on all Academy management studies. Former Senior Executive Service; Director, Government Business Operations Issues, Federal Management Issues and Intergovernmental Issues, General Accounting Office.

Arnold E. Donahue—*Project Director*. Consultant on defense, intelligence and information technology; project director on recent Academy studies on military sex crime investigations, geographic information, and the Global Positioning System. Former Senior Executive Service; Chief, Intelligence and Command, Control, and Communications, U.S. Office of Management and Budget; Intelligence Officer, Central Intelligence Agency.

Edward L. Federico, Jr.—*Senior Project Advisor and Interim Project Director*. Law enforcement consultant, National Academy of Public Administration. Former Senior Executive Service for the Internal Revenue Service; IRS positions include Deputy Assistant Commissioner (Criminal Investigation Division), Director of National Operations, and Chief, Criminal Investigation Division, St. Louis Office. Former Director of Operations for an international investigative firm.

Edward C. Springer—*Senior Project Advisor*. Management consultant, National Academy of Public Administration. Former position as senior policy analyst, Office of Information and Regulatory Affairs, Office of Management and Budget.

Jonathan C. Tucker—*Senior Research Analyst*. Ph.D., Public Policy, former analyst, Technology Partnership Practice, Battelle Memorial Institute, former intern, Committee on Science, Engineering and Public Policy, National Academies, former program analyst, Advanced Technology Program, National Institute of Standards and Technology, former analyst, Office of Policy and Research, New York State Department of Economic Development (now part of Empire State Development).

Martha S. Ditmeyer—*Senior Program Associate*. Staff for a wide range of Academy Studies. Former staff positions at the Massachusetts Institute of Technology and the Communications Satellite Corporation.

INTERVIEWS

FBI HEADQUARTERS

Counterterrorism Division

- Executive Assistant Director for Counterterrorism and Counterintelligence
- Assistant Director for Counterterrorism
- Deputy Assistant Director for Operations I branch
- Section Chief, International Terrorism
- Section Chief, Terrorism Financing Operations (Operations II branch)
- Financial analyst
- Deputy Assistant Director of the Analytical Branch
- Section Chief, Terrorism Requirements and Reports
- Section Chief (acting), Counterterrorism Analysis
- Deputy Assistant Director, Operational Support Branch
- Section Chief, Threat Center
- Section Chief, Terrorism Screening Center
- Section Chief, Foreign Terrorist Tracking Task Force
- Supervisory Special Agents, National Joint Terrorism Task Force
- Unit Chief, CT Watch

Office of Intelligence

- Executive Assistant Director for Intelligence
- Special Advisor, FBI Intelligence Program Implementation
- Assistant Director for Intelligence
- Section Chief, Intelligence Operations (now two sections: Field Intelligence and Intelligence Management)
- Unit Chief, Career Intelligence (now part of Field Intelligence)
- Unit Chief, Intelligence Requirements and Collection Management (now part of Intelligence Management)
- Section Chief, Terrorism Threat Integration Center
- Section Chief (acting), Intelligence Management

Security Division

- Assistant Director, Security Division
- Deputy Assistant Director, Security Division
- Unit Chief, Strategic Planning and Services
- Section Chief, Information Assurance Section
- Unit Chief, Assurance Management
- Unit Chief, Enterprise Security Operations Center

- Section Chief, Personnel Security
- Unit Chief, Initial Clearance and Access I (now the Contractor Clearance Unit)
- Unit Chief, Initial Clearance and Access II (now the Clearance Passage, and Access Unit)
- Unit Chief, Reinvestigations (now the Employee Clearance Unit)
- Section Chief (acting), Security Operations
- Unit Chief (acting), Security Compliance
- Unit Chief, Clearance, Access, and Data Management (now the Law Enforcement Clearance Unit)
- Unit Chief, Security Policy, Education & Training

Other Headquarters Staff

- Director of the Inspection Division
- Executive Assistant Director(s) for Administration
- Chief Information Officer
- Director of the Office of Law Enforcement Coordination
- Assistant Director of the Administrative Services Division

FIELD OFFICES[9]

Baltimore Field Office

- Special Agent in Charge
- Assistant Special Agent in Charge for counterterrorism and counterintelligence (and intelligence before the recent creation of a separate ASAC position)
- security officer
- Supervisory Special Agents, JTTF
- Supervisory Special Agents, counterterrorism squads
- Supervisors (Maryland State Police), counterterrorism squads
- Supervisory Special Agent, Field Intelligence Group
- Supervisory Special Agent, Annapolis resident agency/SWAT coordinator
- Supervisory Special Agent, Wilmington (DE) resident agency
- Special agents, Joint Terrorism Task Force
- Non-FBI task force members:
    - immigrations agent detailed by ICE
    - Sergeant, Delaware State Police
- Administrative Officer
- IT specialist

[9] Interviews were also conducted at the New York and Washington field offices last year as part of the Academy's review of the FBI's reorganization.

Interviews with other FBI partners:

- Assistant US Attorney, Maryland District, coordinator, antiterrorism advisory council
- Director of Homeland Security, Office of the Governor (Maryland)

Philadelphia Field Office

- Special Agent in Charge (acting)
- Assistant Special Agent in Charge (counterterrorism, counterintelligence, intelligence, security)
- Chief Security Officer
- Supervisory Special Agents, counterterrorism squads
- Supervisory Special Agent, Field Intelligence Group
- Non-FBI task force members:
    - Detective, Philadelphia Police Department
    - Trooper, Pennsylvania State Police
    - Investigator, Defense Criminal Investigative Service,

Interviews with other FBI partners:

- Chief Public Safety Officer, Delaware River Port Authority
- Lieutenant, Delaware River Port Authority Police

St. Louis Field Office

- Special Agent in Charge
- Assistant Special Agent in Charge (only one ASAC for the office)
- Security officer/program coordinator, counterintelligence
- Supervisory Special Agent, Joint Terrorism Task Force
- Non-FBI task force member:
    - detective, St. Louis Metropolitan Police Department
- Intelligence analysts, Field Intelligence Group
- Information Technology specialist

Interviews with other FBI partners:

- Sergeant, St. Louis Police Metropolitan Department, detailed to Gateway information sharing project

Springfield Field Office

- Special Agent in Charge (acting)
- Assistant Special Agent in Charge (only one, acting)
- Security officer/polygrapher
- Supervisory Special Agent, Field Intelligence Group (formerly also coordinator for counterterrorism and counterintelligence)
- Supervisory Special Agent, JTTF/coordinator, counterterrorism
- Supervisory Special Agent, Fairview Heights (E. St. Louis) resident agency
- Special agent, Joint Terrorism Task Force
- Administrative Officer
- IT specialist

Interviews with other FBI partners:

- Supervisor, State Terrorism Information Center (Illinois State Police)
- Senior Terrorism Advisor, Illinois State Police
- Senior officer, Illinois State Police

Chicago Field Office

- Special Agent in Charge
- Assistant Special Agent in Charge (counterterrorism)
- Assistant Special Agent in Charge (administrative)
- Security officer
- Supervisory Special Agent, Joint Terrorism Task Force
- Supervisory Special Agent, Field Intelligence Group
- Non-FBI task force members:
    - Cook County Sheriff
    - Special Agent, Immigration and Customs Enforcement
    - Master Sergeant, Illinois State Police
    - Special Agent, Federal Air Marshall Service (ICE)
    - Special Agent, Criminal Investigation Division, U.S. Army
    - Special Agent, U.S. Coast Guard Investigative Service
    - Detective, Chicago Police Department

Los Angeles Field Office

- Assistant Director in Charge
- Special Agent in Charge (Counterterrorism)
- Special Agent in Charge (Counterintelligence, Intelligence)
- Special Agent in Charge (Cyber, Criminal)
- Supervisory Special Agent , Security
- Supervisory Special Agent, JTTF

- Program Manager-Intelligence Branch
- Intelligence Analyst
- Supervisory Special Agent, LAX resident agency
- Special agent, LAX resident agency
- Non-FBI task force members:

    - Chief Intelligence Analyst, Antiterrorism Division, LAPD
    - Special Agent, Immigration and Customs Enforcement
    - Special Agent, Coast Guard Investigative Service
    - Police Officer, Torrance, CA Police Department
    - Police Officer, Los Angeles Police Department, JTTF member

- Acting Supervisory Special Agent, Long Beach Resident Agency/Joint Terrorism Task Force
- Senior Supervisory Special Agent, Long Beach Resident Agency/Criminal Investigation matters

Interviews with other FBI partners:

- Chief, Antiterrorism Division, LAPD
- Captain, LA Sheriff's Department
- Deputy Federal Security Director for Los Angeles International Airport, Transportation Security Administration
- Captain, Los Angeles International Airport Police Department

Sacramento Field Office

- Special Agent in Charge
- Assistant Special Agent in Charge (counterterrorism, counterintelligence, cyber)
- Security officer/Supervisor, Field Intelligence Group
- Coordinator, Joint Terrorism Task Force
- Program coordinator, domestic terrorism/Supervisor, domestic terrorism squad
- Supervisory Special Agent, Modesto/Stockton resident agency
- Information technology specialist

Interviews with other FBI partners:

- Lieutenant, California Highway Patrol, State Warning Center
- Captain, California Highway Patrol, State Terrorism Threat Assessment Center
- Deputy Chief of Administrative Services, Governor's Office of Emergency Services, Law Enforcement Branch
- Deputy Director, California Office of Homeland Security,
- Analyst, California Office of Homeland Security

San Diego Field Office

- Special Agent in Charge
- Assistant Special Agent in Charge (criminal, administrative matters)
- Security officer
- Supervisory Special Agent, Field Intelligence Group
- Intelligence Analyst
- Supervisory Special Agent, information technology coordinator
- Supervisory Special Agent, Joint Terrorism Task Force
- Non-FBI task force members

    - Special Agent, Defense Criminal Investigative Service
    - Special Agent, US Immigration and Customs Enforcement
    - Special Agent, Naval Criminal Investigative Service
    - Officer, San Diego Police Department

- Supervisory Special Agent, North County resident agency
- Director, FBI Regional Computer Forensics Laboratory
- Supervisor, information technology
- Information technology specialist

Interviews with other FBI partners:

- Commander, US Coast Guard
- Resident Agent-in-Charge, US Coast Guard Investigative Service

OTHER INTERVIEWS

- Chairman, FBI Science and Technology Advisory Board
- Deputy Director of the Financial Crimes Enforcement Network, Treasury Department
- Secretary and two members, National Association of Assistant United States Attorneys
- Former Deputy Director of the FBI

APPENDIX C

SELECTED BIBLIOGRAPHY

Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. *Forging America's New Normalcy: Securing Our Homeland, Protecting Our Liberty*. (Fifth and final report). RAND: Arlington, VA, December 2003.

Arthur Anderson. *Management Study of the FBI*. December 2001.

Commission for Review of FBI Security Programs. *A Review of FBI Security Programs*. U.S. Department of Justice: Washington, D.C.: March 2002.

Cumming, Alfred and Todd Masse. *FBI Intelligence Reform Since September 11, 2001: Issues and Options for Congress*. Washington, D.C.: Congressional Research Service, April 6, 2004.

Eldridge, Thomas R. et al. *9/11 and Terrorist Travel*. Staff Report the National Commission on Terrorist Attacks upon the United States. August 2004.

Federal Bureau of Investigation. *2004-2009 Strategic Plan*. Undated.

Federal Bureau of Investigation. *Report to the National Commission on Terrorist Attacks upon the United States: The FBI's Counterterrorism Program Since September 2001*. Washington, D.C.: April 2004.

Franklin, Daniel. "Freeh's Reign". *The American Prospect*. January 1, 2002. Vol. 13, pp. 20-23.

Global Intelligence Working Group. *National Criminal Intelligence Sharing Plan*. Washington, D.C.: October 2003.

Hill, Eleanor. *Counterterrorism Information Sharing with Other Federal Agencies and with State and Local Governments and the Private Sector*. Report to the House Permanent Select Committee on Intelligence and Senate Select Committee on Intelligence (Joint Inquiry). Washington, D.C.: October 2002.

House Permanent Select Committee on Intelligence and Senate Select Committee on Intelligence. *Report on the Joint Inquiry on Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001*. 107th Congress, 2nd Session, 2002. Senate Report No. 107-351, House Report No. 107-792.

Independent Task Force on Terrorist Financing. *Update on the Global Campaign Against Terrorist Financing*. New York, NY: Council on Foreign Relations, June 2004.

Independent Task Force (Hart/Rudman). *America Still Unprepared – America Still in Danger*. Council on Foreign Relations: New York: NY, October 2002.

International Association of Chiefs of Police. *Criminal Intelligence Sharing: A National Plan for Intelligence-led Policing at the Local, State, and Federal Levels.* International Association of Chiefs of Police: Alexandria, VA, August 2002.

Kinghorn, C. Morgan. Testimony before the Subcommittee on Commerce, State, Justice, the Judiciary, and Related Agencies, Committee on Appropriations, U.S. House of Representatives. June 3, 2004.

Kinghorn, C. Morgan. *The FBI's Budget Authority and Personnel and Pay Authorities*. Report to the Subcommittee for Commerce, Justice, State, and the Judiciary, Committee on Appropriations, U.S. House. May 26, 2004.

Markle Foundation. *Creating a Trusted Information Network for Homeland Security*. Washington, D.C.: Markle Foundation, December 2003.

Markle Foundation. *Protecting America's Freedom in the Information Age*. Washington, D.C.: Markle Foundation, October 2002.

National Commission on Terrorism (Bremer Commission). *Countering the Changing Threat of International Terrorism*. June 2000.

National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report*. July 22, 2004.

National Governors' Association. *State Homeland Security Organizational Structures*. January 2004.

National Research Council. *A Review of the FBI's Trilogy Information Technology Modernization Program*. National Research Council: Washington, D.C., 2004.

Office of Homeland Security. *National Strategy for Homeland Security*. Washington, D.C.: July 2002.

Office of Management and Budget. *2003 Report to Congress on Combating Terrorism*. Washington, D.C.: September 2003.

Roth, John et al. *Monograph on Terrorist Financing. Staff Report the National Commission on Terrorist Attacks upon the United States*. Undated.

Thornburgh, Dick. Testimony before the Subcommittee on Commerce, State, Justice, the Judiciary, and Related Agencies, Committee on Appropriations, U.S. House of Representatives. June 18, 2003.

Treverton, Gregory F. et al. *Reinforcing Security at the FBI*. RAND: Washington, D.C., February 2003.

U.S Department of State. *Patterns of Global Terrorism 2003*. Washington, D.C.: April 2004.

U.S. Commission on National Security in the 21st Century (Hart/Rudman Commission). *Seeking A National Strategy: A Concert for Preserving Security and Promoting Freedom*. September 1999.

U.S. Department of Justice, Office of the Inspector General. *The Internal Effects of the Federal Bureau of Investigation's Reprioritization* (Redacted and Unclassified). Report No. 04-39. Washington, D.C.: September 2004.

U.S. Department of Justice, Office of the Inspector General. *Federal Bureau of Investigation Legal Attaché Program*. Report No. 04-18. Washington, D.C.: March 2004.

U.S. Department of Justice, Office of the Inspector General. *The Federal Bureau of Investigation's Efforts to Improve the Sharing of Intelligence and Other Information*. Report Number 04-10. Washington, D.C.: December 2003.

U.S. Department of Justice, Office of the Inspector General. *The Federal Bureau of Investigation's Implementation of Information Technology Recommendations*. Report No. 03-36. Washington, D.C.: September 2003.

U.S. Department of Justice, Office of the Inspector General. *An Investigation of the Belated Production of Documents in the Oklahoma City Bombing Case*. Washington, D.C.: March 2002.

U.S. Department of Justice. *Information Technology Strategic Plan*. Washington, D.C.: July 2002.

U.S. Department of Treasury. *National Money Laundering Strategy*. Washington, D.C.: July 2002.

U.S. Government Accountability Office. *Information Technology: Foundational Steps Being Taken to Make Needed FBI Systems Modernization Management Improvements.* GAO-04-842. Washington, D.C.: September 2004.

U.S. Government Accountability Office. "9/11 Commission Report: Reorganization, Transformation, and Information Sharing." Testimony Before the Committee on Government Reform, U.S. House of Representatives. GAO-04-1033T. Washington, D.C.: August 2004.

U.S. Government Accountability Office. FBI Transformation: Data Inconclusive on Effects of Shift to Counterterrorism-Related Priorities on Traditional Crime Enforcement. GAO-04-1036. Washington, D.C.: August 2004.

U.S. Government Accountability Office. "FBI Transformation: Human Capital Strategies May Assist the FBI in Its Commitment to Address Its Top Priorities." Testimony Before the Subcommittee on Commerce, Justice, State, the Judiciary, and Related Agencies, Committee on Appropriations, U.S. House of Representatives. GAO-04-817T. Washington, DC: June 2004.

U.S. Government Accountability Office. "FBI Transformation: FBI Continues to Make Progress in Its Efforts to Transform and Address Priorities." Testimony Before the Subcommittee on Commerce, Justice, and the Judiciary, Committee on Appropriations, U.S. Senate. GAO-04578T. Washington, D.C.: March 2004.

U.S. Government Accountability Office. *Terrorist Financing: U.S. Agencies Should Systematically Assess Terrorists' Use of Alternative Financing Mechanisms.* GAO-04-163. Washington, D.C.: November 2003.

U.S. Government Accountability Office. Information Technology: *FBI Needs an Enterprise Architecture to Guide Its Modernization Activities.* GAO-03-959. Washington, D.C.: September 2003.

U.S. Government Accountability Office. "FBI Reorganization: Progress Made in Efforts to Transform, but Major Challenges Continue." Testimony Before the Subcommittee on Commerce, Justice, State, the Judiciary, and Related Agencies, Committee on Appropriations, U.S. House of Representatives. GAO-03-759T. Washington, D.C.: June 18, 2003

U.S. Government Accountability Office. *Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing*. GAO-03-322. Washington, D.C.: April 2003.