FEDERAL BUREAU OF INVESTIGATION

STRATEGIC PLAN

2004 2009

A Message from the Director

The events of September 11th have forever changed our nation and the FBI. Since that terrible day, the FBI's overriding priority has been protecting America by preventing further attacks. The FBI has made and will continue to make many significant changes in order to protect America. We have refocused our priorities to enable us to better accomplish our mission and we are making comprehensive changes in the overall structure, organization, and business practices of the FBI to ensure that we excel at everything we do.

Changes are occurring from top to bottom — from reassigning personnel to counterterrorism, to examining our hiring practices, to rethinking the scope and form of internal and external information sharing. FBI Headquarters has been restructured to make it more effective and efficient. We have centralized case management; realigned the workforce to address our priorities; and developed a central body of knowledge available to all field offices and to our partners in the Law Enforcement and Intelligence Communities.

These changes have allowed us to make significant contributions to the war on terrorism. Working with our partners over the past 28 months, we conducted numerous counterterrorism investigations, resulting in more than one thousand arrests and hundreds of convictions or pre-trial diversions. We broke up the Lackawanna Six, dismantled the Portland Seven, and put would-be shoe bomber Richard Reid behind bars. We investigated thousands of cyber intrusions, with one case involving a global criminal network reaching as far as the South Pole. We strengthened counterintelligence operations, placed counterintelligence squads in almost every field office, and created a counterespionage section at FBI Headquarters.

Even as our efforts evolve, the FBI continues to meet its traditional responsibilities to uphold and enforce federal criminal laws of the United States. We pursued major corporate fraud schemes that accounted for billions of dollars in losses; the "collar bomb" incident in Pennsylvania; and sniper shootings in Maryland, Washington D.C., Virginia, West Virginia, and Ohio. The FBI has had successes against public corruption and continues to aggressively protect civil rights. In one hate crime investigation, a man was sentenced to death for killing a Sikh male in a parking lot.

We continue to improve our technology and are finding better ways to communicate with our federal, state, local, and international partners. To keep us focused on our principles, the FBI amended its core values to place new emphasis on accountability for our actions and leadership through example.

Looking forward, the FBI's greatest challenges will be to further improve its intelligence capabilities and strengthen its information technology infrastructure. The FBI will continue to develop its talents through ongoing training, and through the recruitment and hiring of analysts, technology experts, and individuals with language skills. The FBI's international presence will continue to grow, and we will continue our tradition of excellence in carrying out all of our responsibilities overseas and at home.

The FBI's 2004–2009 strategic plan serves as a high-level road map for the FBI to achieve its mission. While the strategic plan provides clear goals and objectives, it also includes the flexibility necessary to adjust quickly to evolving threats. Since the FBI's inception, the nation has turned to it to address the most significant threats, and the FBI has always responded. The strength of the FBI has been, and will always be, its people. The skill, determination, and sacrifice of the men and women of the FBI are outstanding, and I am extremely proud to serve as the Director of this extraordinary organization.

2004 2009

STRATEGIC PLAN

Table of Contents

INTRODUCTION

The FBI Strategic Plan 2004-2009 serves as a high-level road map for the next five years, with strategic goals and objectives that address the mission of the FBI and fulfill the imperatives of the President, the Attorney General, and the Director of Central Intelligence (DCI). This document updates our earlier strategic plan (FBI Strategic Plan 1998-2003) and reflects profound and far-reaching changes to our investigative priorities and business practices since 9/11. The FBI's efforts to remake and reengineer itself continue and this plan serves as a primary guide to the new realities of the war on terrorism.

The plan reflects these external and internal changes by laying out a new set of priorities and an altered structure for the organization's goals and objectives. Our reinvigorated strategic planning process, outlined on facing page, translates these goals and objectives into actionable and measurable activities in order to track their progress. Annual implementation plans provide priority actions and measures to incrementally achieve our strategic goals, and completion dates are assigned and tracked to ensure that deadlines are met. Comprehensive program evaluations are conducted to measure whether we have met our goals and objectives. Although this plan improves on its predecessor, we recognize that improvements can still be made and we anticipate annual updates, as the FBI continues to make fundamental changes to its organizational culture and administrative processes.

The plan is divided into four sections. Section I provides an FBI forecast. Section II provides strategic goals, objectives, and priority actions for achieving the mission of the FBI over the next five years. Section III addresses the most important asset of the FBI — its people. Section IV is devoted to the tools we must have to perform our mission effectively and efficiently. Appendices A, B, and C provide information about the external and internal factors, or "drivers," that affect FBI planning, the stakeholders who provide input into that process, and the program evaluations that address whether programs are operating effectively.

FBI THREAT-BASED PLANNING CYCLE

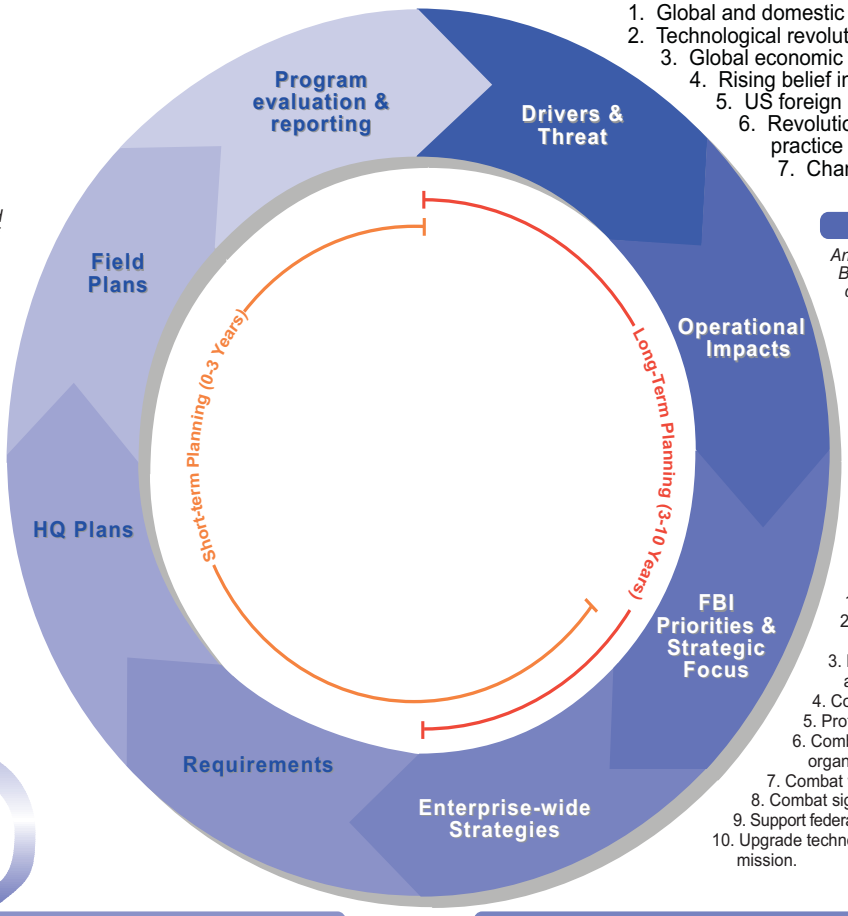
PROGRAM EVALUATION & REPORTING

Program evaluation and reporting ensures FBI programmatic flexibility to address both emerging and forecasted threats. Evaluations also report progress in achievement of goals and objectives.

DRIVERS/THREATS

Drivers are broad factors that can directly or indirectly cause changes in the future threat environment that are developed by Office of Intelligence. Current threat is assessed annually and also considered in this stage; 10 year time frame

1. Global and domestic demographic changes
2. Technological revolution
3. Global economic changes
4. Rising belief in non-material values
5. US foreign policy
6. Revolutions in security technology and practice
7. Changing role of state and law



FIELD PLANS

Each field office will establish goals and objectives based on local application of national priorities, communicated by operational divisions; 1 year time frame

OPERATIONAL IMPACTS

An assessment of the operational impact on the Bureau is developed based on the drivers and current threat.

1. Enterprise strategy and Culture
2. External relationships
3. Recruiting, training and development
4. Resources
5. Priorities

HQ PLANS

Each HQ division will draft an operating plan that is consistent with FBI priorities, supports enterprise-wide strategies, and meets requirements defined by operational divisions; 1 year time frame

CJIS | TD | ASD | IRD | CD | CID | LAB | OGC | INSD | SEC | FIN | CTD | OIO | CyD | RMD | ITD | OI

As HQ Plans are being developed, changes to the requirements may arise. There is a need for continual collaboration and review.

FBI PRIORITIES

After the operational impacts are weighed, the Director's Office will determine the strategic priorities of the Bureau.

1. Protect the US from terrorist attack
2. Protect the US against foreign intelligence operations and espionage.
3. Protect the US 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 white collar crime
8. Combat significant violent crime
9. Support federal, state, local, and international partners
10. Upgrade technology to successfully perform the FBI's mission.

REQUIREMENTS

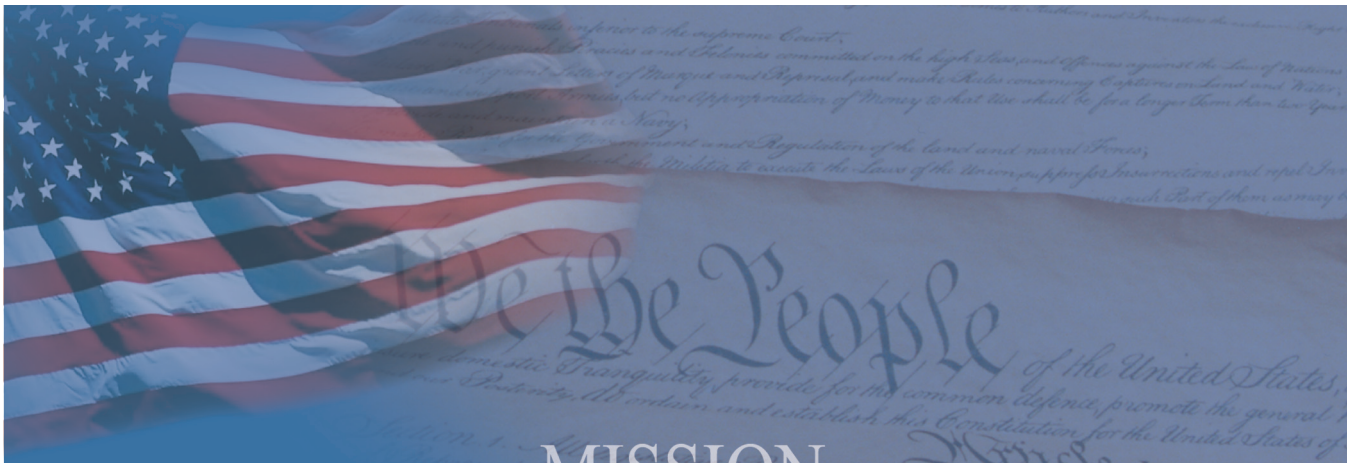
Requirements will be established and communicated to the divisions that execute and support the national operational strategies.

Human Capital | **Intelligence** | **Information Technology**

ENTERPRISE-WIDE STRATEGIES

With clear strategic priorities, the FBI will develop strategies against the threat, which include operations and infrastructure, and will set national goals and objectives. The operations drive the infrastructure; 5 year time frame

Operational → **Infrastructure**



MISSION

The mission of the FBI is to protect and defend the United States against terrorism and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners.

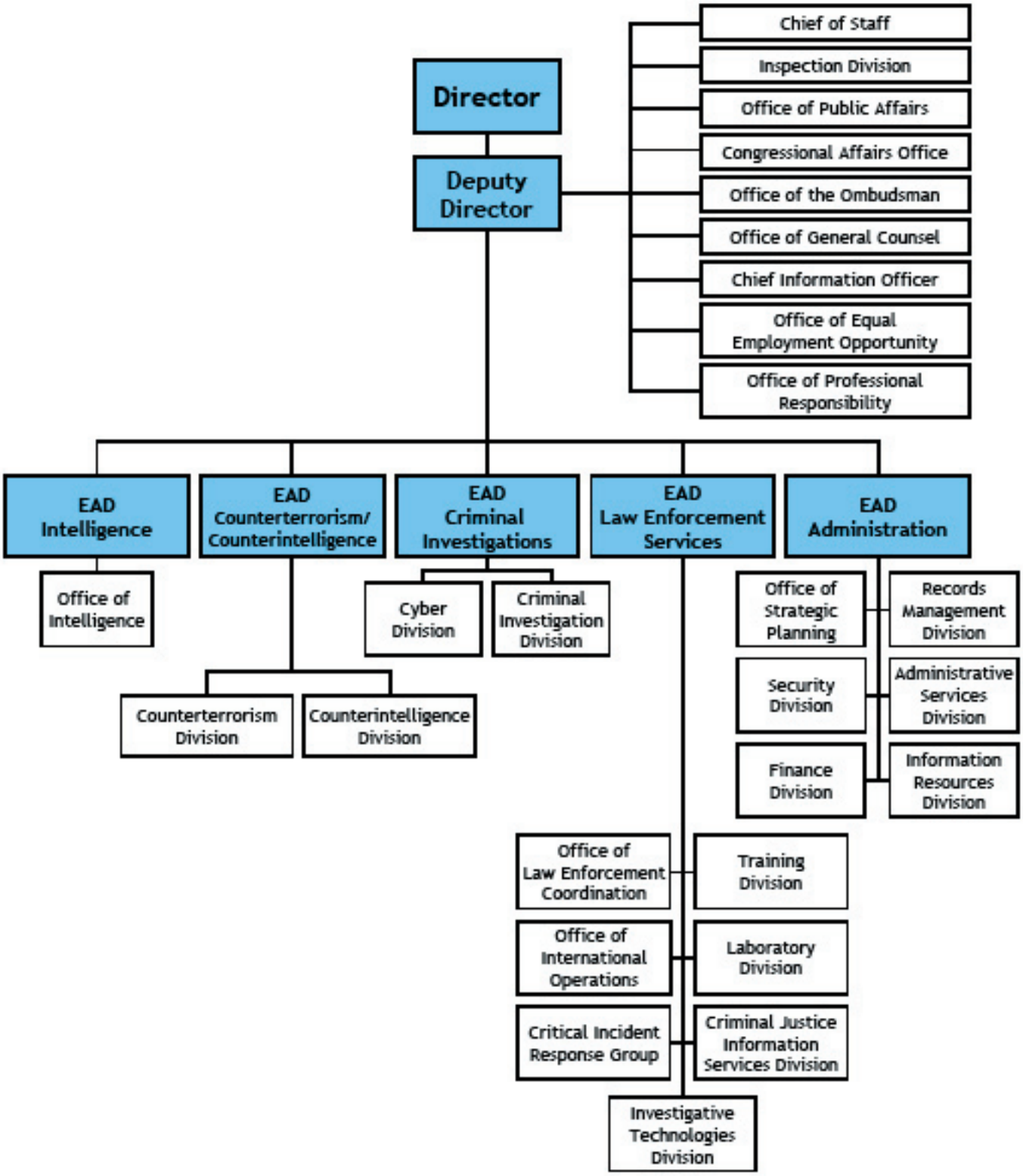
CORE VALUES

The FBI will strive for excellence in all aspects of its mission. In pursuing its mission, the FBI and its employees will be true to, and exemplify, the following core values:

ADHERENCE	to the rule of law and the rights conferred to all under the United States Constitution;
INTEGRITY	through everyday ethical behavior;
ACCOUNTABILITY	by accepting responsibility for our actions and decisions, and consequences of our actions and decisions;
FAIRNESS	in dealing with people; and
LEADERSHIP	through example, both at work and in our communities.

Organization Chart

Federal Bureau of Investigation



FBI Legat Offices

FBI Headquarters centrally manages and directs worldwide FBI operations and investigations. FBI Headquarters is comprised of four operational divisions (Counterterrorism, Counterintelligence, Cyber, and Criminal Investigative) plus 10 divisions and 10 offices that support operational and administrative functions. The intelligence and investigative work of the FBI is conducted out of 56 field offices and 400 satellite offices (referred to as resident agencies) that report to the field offices. The FBI also has 45 offices located outside the United States — referred to as Legal Attaché offices or Legats — that support investigations and operations around the world.

FBI PRIORITIES

The FBI's principal mission is to defend the security of the United States and within that mission there are priority focus areas. On May 29, 2002, Director Mueller announced the priorities of the FBI to clearly articulate to the American public, our Law Enforcement and Intelligence Community partners, and the employees of the FBI, the manner in which the FBI will address its wide range of responsibilities.

The order of the listed priorities is determined by the interaction of three factors: (1) the significance of the threat to the security of the United States as expressed by the President in National Security Presidential Decision Directive 26; (2) the priority the American public places on various threats; and (3) the degree to which addressing the threat falls most exclusively within the FBI's jurisdiction.

The FBI has a broad mission with varied and competing challenges. By weighing and evaluating the above factors, the top priorities of the FBI become clear.

Director Mueller has established ten priorities. The first eight are listed in order of priority. The final points (collaborative partnerships and technology improvement) are key enabling functions that are of such importance they merit inclusion. The priorities are:

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, local, and international partners;***
10. ***Upgrade technology to successfully perform the FBI's mission.***

By stating our priorities, we discipline our actions. We now staff and work high priority matters before lower ones. Support processes, including hiring and technological competence, serve our highest priorities first.

TRANSFORMING THE FBI

The current and foreseeable threat environment requires the FBI to evolve constantly. The FBI has a proud history of adapting to changing threat environments. After the terrorist attacks on September 11, 2001, the FBI once again faced the need to adapt. Since then, new leadership, organizational structure, priorities, technologies, resources, and enabling legislation have better positioned the FBI to fulfill its vital mission in a changing world. Those who wish to sow terror, however, are determined and adaptable and should never be underestimated. Hence, the FBI must continue to evolve to address tomorrow's threats. Implementing an enterprise-wide intelligence capability second to none and modernizing our information technology systems are critical to the FBI's transformation.

To achieve dramatic improvements, the FBI adopted the "reengineering" method which has been a successful business practice in the private sector for decades. In 1994, this method gained momentum in the federal government as a result of a General Accounting Office (GAO) Symposium which concluded that "reengineering" can enable government agencies to reduce costs and improve business processes. As shown in the chart below, GAO's analysis identified nine key practices that resulted in the transformation of businesses into high performing organization.

Key Practices That Resulted in the Transformation of Business into High Performing Organization

Current State
- Process-oriented
- Stove-pipe
- Hierarchical
- Inwardly focused
- Micro-managing
- Reactive behavior
- Avoiding technology
- Hoarding technology
- Avoiding risk
- Protecting turf

9 Key Practices
- Leadership
- Integrated mission and goals
- Clear principles and priorities
- Goals and timeline
- Implementation team
- Line of sight
- Communication strategy
- Employee involvement
- World class organization

High Performing Organizations (HPO)
- Results-oriented
- Matrixes
- Flatter and more horizontal
- Externally focused
- Employee empowerment
- Proactive approaches
- Leveraging technology
- Sharing knowledge
- Managing risk
- Forming partnerships

Source: GAO analysis.

TRANSFORMING the FBI

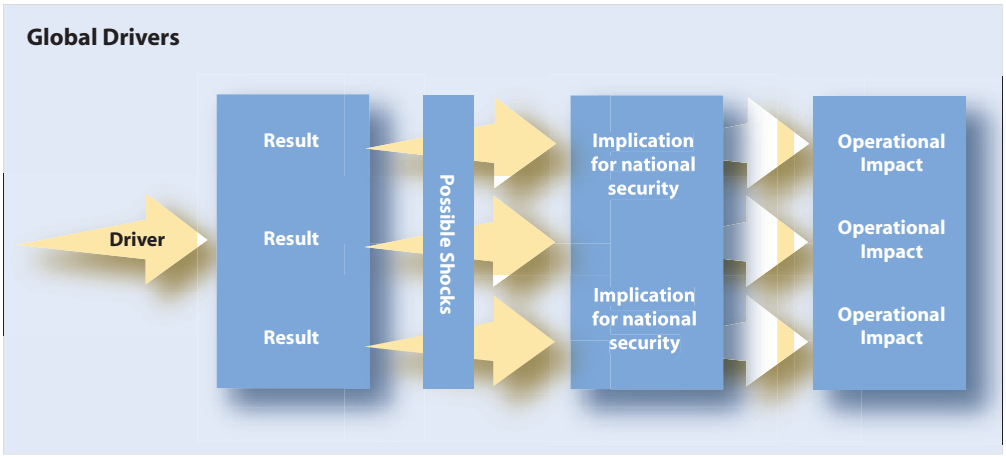
Adopting a reengineering approach to change enabled the FBI to make immediate improvements in key areas. The approach was then expanded to address six core processes essential to the transformation of the FBI: (1) Intelligence; (2) Information Management; (3) Investigative Programs; (4) Human Capital; (5) Strategic Planning & Execution; and (6) Security Management.

As noted in the GAO symposium, transformation of any large organization cannot occur overnight. Essential ingredients to long-term success include: (1) top management support in identifying and analyzing core business processes in an effort to improve overall effectiveness in accomplishing the mission; (2) the ability to set time frames for full implementation of transformation efforts; (3) requirements-based project management software to assist in the tracking of key milestones and assessment points; and (4) the ability to hold managers accountable. Taking these ingredients into account, the FBI has taken the actions necessary to make systemic organizational and operational improvements in its continuing effort to excel in all that it does.

SECTION I

FBI FORECAST

The foundation of strategic planning is long-term forecasting. The FBI's enterprise-wide Intelligence Program provides robust forecasting capability, which integrates external and internal data to forecast global drivers and their operational impacts. Those impacts, in turn, are translated into organizational goals and objectives. The FBI identifies global "drivers" — broad factors that can directly or indirectly cause changes in the future threat environment. These "drivers" correlate in many ways to categories or "dimensions" used in a variety of U.S. and foreign forecasts. The FBI forecast process focuses on seven global drivers, outlined below and discussed in more detail in Appendix A. From those drivers, we identify probable results, as well as less probable results caused by "shocks" — high-impact, low probability events. The results are then assessed for their implications on the FBI mission and its strategic planning process. From those implications, a list of operational impacts, as well as organizational and recruiting consequences, is produced.



The most notable operational impacts and organizational consequences related to each "driver" identified by the FBI are:

(1) Global and domestic demographic changes

- global — more operations abroad; need increased intelligence from within immigrant communities; wider variety of linguists required
- domestic/internal — rapid FBI staff turnover presents opportunity for culture change, but loss of corporate memory

(2) Communications revolution

- intelligence — encryption constrains Foreign Intelligence Surveillance Act (FISA) operations, will need to get closer to end-nodes
- investigations — identity theft will make perpetrator identification more difficult
- internal — easier FBI peer-to-peer communications; greater need for technically savvy staff; need for alternate communications in event of catastrophic outage

(3) Global economic changes

- external — terrorism and organized crime converge; greater need for coordinating countermeasures with foreign countries and financial organizations
- internal — difficulty recruiting highly paid technical talent

(4) Rising belief in non-material values abroad

- external — increasing danger to agents working abroad as anti-Americanism increases and actors disperse, FBI may become target
- internal — greater difficulty recruiting ethnic Arabs and Muslims, as well as any newly identified ethnic groups associated with threats

(5) Technological revolutions

- external — reduced ability for threat groups or governments to hide undercover identity of agents; increase in espionage and cyber crime against U.S. corporations
- internal — need for increased technical recruiting; need for enhanced civil liberties training as technology outpaces policy

(6) Revolutions in security technology and practice

- international — more "policing" actions abroad; more espionage against U.S. defense and contractors
- internal — need for continuity of operations following attack on FBI; mounting political pressure for technical solutions faster than they can be produced and implemented

(7) Changing role of state and law

- external — need to cooperate with more entities; need more methods of cooperation beyond task forces and cases
- internal — need to reassess security procedures as number of non-FBI partners and participants grows

The FBI forecasts that sub-national and non-governmental entities will play an increasing role in world affairs for years to come, presenting new "asymmetric" threats to the United States. Although the United States will continue to occupy a position of economic and political leadership — and although other governments will also continue to be important actors on the world stage — terrorist groups, criminal enterprises, and other non-state actors will assume an increasing role in international affairs. Nation states and their governments will exercise decreasing control over the flow of information, resources, technology, services, and people.

Globalization and the trend of an increasingly networked world economy will become more pronounced within the next five years. The global economy will stabilize some regions, but widening economic divides are likely to make areas, groups, and nations that are left behind breeding grounds for unrest, violence, and terrorism. As corporate, financial, and nationality definitions and structures become more complex and global, the distinction between foreign and domestic entities will increasingly blur. This will lead to further globalization and networking of criminal elements, directly threatening the security of the United States.

Most experts believe that technological innovation will have the most profound impact on the collective ability of the federal, state, and local governments to protect the United States. Advances in information technology, as well as other scientific and technical areas, have created the most significant global transformation since the Industrial Revolution. These advances allow terrorists, disaffected states, weapons proliferators, criminal enterprises, drug traffickers, and other threat enterprises easier and cheaper access to weapons technology. Technological advances will also provide terrorists and others with the potential to stay ahead of law enforcement countermeasures. For example, it will be easier and cheaper for small groups or individuals to acquire designer chemical or biological warfare agents, and correspondingly more difficult for forensic experts to trace an agent to a specific country, company, or group.

In the 21st Century, with the ready availability of international travel and telecommunications, neither crime nor terrorism confines itself territorially. Nor do criminals or terrorists restrict themselves, in conformance with the structure of our laws, wholly to one bad act or the other. Instead, they enter into alliances of opportunity as they arise; terrorists commit crimes and, for the right price or reason, criminals assist terrorists. Today's threats cross geographic and political boundaries with impunity; and do not fall solely into a single category of our law. To meet these threats, we need an even more tightly integrated intelligence cycle. We must have extraordinary receptors for changes in threats and the ability to make immediate corrections in our priorities and focus to address those changes. And, we must recognize that alliances with others in law enforcement, at home and abroad, are absolutely essential.

Counterterrorism Forecast: Terrorism is the most significant threat to our national security. In the international terrorism arena, over the next five years, we believe the number of state-sponsored terrorist organizations will continue to decline, but privately-sponsored terrorist groups will increase in number. However, the terrorist groups will increasingly cooperate with one another to achieve desired ends against common enemies. These alliances will be of limited duration, but such "loose associations" will challenge our ability to identify specific threats. Al-Qaeda and its affiliates will remain the most significant threat over the next five years.

The global Weapons of Mass Destruction (WMD) threat to the United States and its interests is expected to increase significantly in the near term. We expect terrorists to exploit criminal organizations to develop and procure WMD capabilities. Globalization will make it easier to transfer both WMD materiel and expertise throughout the world. The basic science and technologies necessary to produce WMD will be increasingly well understood. Similarly, raw materials will be more available and easier to obtain.

Violence by domestic terrorists will continue to present a threat to the United States over the next five years. The number of traditional left wing terrorist groups, typically advocating the overthrow of the U.S. Government because of the perceived growth of capitalism and imperialism, have diminished in recent years. However, new groups have emerged that may pose an increasing threat. Right wing extremists, espousing anti-government or racist sentiment, will pose a threat because of their continuing collection of weapons and explosives coupled with their propensity for violence. The most significant domestic terrorism threat over the next five years will be the lone actor, or "lone wolf" terrorist. They typically draw ideological inspiration from formal terrorist organizations, but operate on the fringes of those movements. Despite their ad hoc nature and generally limited resources,

they can mount high-profile, extremely destructive attacks, and their operational planning is often difficult to detect.

Counterintelligence Forecast: The threat from countries which consider the United States their primary intelligence target, adversary or threat either will continue at present levels or likely increase. The most desirable U.S. targets will be political and military plans and intentions; technology; and economic institutions, both governmental and non-governmental. Foreign intelligence services increasingly will target and recruit U.S. travelers abroad and will use non-official collection platforms, including increasing numbers of students, visitors, delegations, and emigres within the United States. Foreign intelligence activities are likely to be increasingly characterized by the use of sophisticated and secure communication technology to handle recruited agents and to be more likely than in the past to occur almost anywhere in the United States.

Cyber Forecast: Cyber threats confronting the United States emerge from two distinct areas: (1) traditional criminal activity that has migrated to the Internet, such as fraud, identity theft, child pornography, and trade secret theft; and (2) Internet-facilitated activity, such as terrorist attacks, foreign intelligence threats, and criminal intrusions into public and private networks for disruption or theft. The vulnerability of the United States to such activity is rapidly escalating as its economy and critical infrastructures become increasingly reliant on interdependent computer networks and the World Wide Web. The cyber threat to our national security stems from two groups: (1) non-state actors such as terrorist groups and hackers; and (2) foreign governments that have developed cyber espionage or information warfare programs to target U.S. networks. The number of foreign governments and non-state actors exploiting computer networks and developing their cyber capabilities is on the rise.

Public Corruption Forecast: The corruption of local, state, and federally elected, appointed, or contracted officials undermines our democratic institutions and sometimes threatens public safety and national security. The root of corruption is greed, and over the next five years there will be increased government spending and increased opportunities for government officials to violate the public trust. As our nation tightens security at our land borders and our air and sea ports to prevent terrorism — terrorists, international drug enterprises, and alien smuggling rings will increasingly seek to recruit U.S. law enforcement officials to further their operations, thereby undermining our security at the borders. Likewise, as additional controls are established to minimize identity fraud, there will be an increase in demand by criminal enterprises to corrupt government officials who issue identification documents.

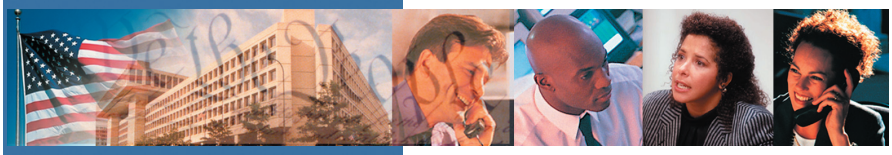
Civil Rights Forecast: Most hate crimes statistics have remained relatively constant, but there have been specific areas of increased activity. From 1996 to 1998, there was a spike in arson against religious properties. Since 9/11, there has been an unprecedented number of hate crimes directed against Muslim, Sikh, and Arab-American individuals and institutions. In the event of another terrorist attack on U.S. soil or against U.S. interests abroad, we anticipate similar spikes of activity directed against persons who share actual or perceived ethnicity, religion, or national origin with the terrorists. In addition, the number of crimes under "Color of Law" statutes is expected to increase in direct proportion to the increase in the number of law enforcement and correctional officers over the next decade.

Transnational/National Crime Forecast: Drug trafficking poses a continuing threat, responsible for an estimated 50,000 drug-related deaths and $110 billion in social costs per year. In producer countries, the trade funnels both money and power to criminal elements and illegally armed groups, and provides a breeding ground for corruption, violence, environmental degradation, and political and economic instability. Gang-related violence will continue as long as the demand for illicit drugs remains or increases, and drives gangs to battle for retail drug distribution markets, especially in large user-based metropolitan areas. Human trafficking organizations have increased dramatically in recent years, and will likely continue to do so over the next five years. Worldwide human smuggling is estimated to be a $7 billion industry, bringing hundreds of thousands of illegal immigrants to the United States each year. Increasingly, terrorists and their supporters will use alien smuggling networks to circumvent increased border security measures implemented since 9/11. International criminal groups will grow and form new partnerships and alliances due largely to globalization. It is likely that criminal groups will expand their intelligence capabilities to thwart law enforcement investigations.

White Collar Crime Forecast: Major white collar crime will impact the U.S. economy over the next five years. Corporate fraud has undermined the public's confidence in American business institutions, and the aggressive investigation and prosecution of major corporate fraud will be a key factor in restoring long-term confidence in our business leaders. Money laundering poses a growing threat to national security. Advances in technology and the globalization of financial institutions will allow terrorist and criminal organizations to more easily influence economic, social, and political institutions. Money launderers and those engaging in financial institution fraud will increasingly use sophisticated computer technology, offshore banking, and complex financial mechanisms to facilitate their criminal activity and hide illicit proceeds. An increase in government procurement from industry over the next five years will create opportunities for major fraud. Health care fraud is expected to increase dramatically over the next decade as the aging of the U.S. population drives increases in private health care and Medicare spending.

Violent Crimes Forecast: General violent crime rates have significantly decreased over the last five years (1997-2002); however, murders have increased over the last three years (1999-2002). Additionally, within the first six months of 2003, murder rates in the northeast United States continued to rise. New York, Newark, Philadelphia, and Baltimore all had significantly more murders compared to the same period in 2002. Major violent incident crimes, such as sniper murders and child abductions will continue. These crimes paralyze whole communities and stretch local law enforcement resources often for long periods of time. The widespread publicity associated with sniper murders may produce imitators. The problem of organized child prostitution will continue to increase as criminal enterprises victimize juveniles to meet increasing demands.

SECTION II



ACHIEVING the MISSION

To achieve its mission, the FBI must strengthen three inextricably linked core functions: intelligence, investigations, and partnerships. A robust national Intelligence Program ensures that all critical information is identified, collected, evaluated, analyzed, and disseminated to the widest extent possible. Investigations are the means by which the FBI proactively collects intelligence and evidence in a manner that protects civil liberties. Partnerships are essential if the FBI is to effectively address evolving threats that are too complex or multi-jurisdictional for one agency to handle alone. To achieve its vital mission, the FBI is dependent upon the goodwill, cooperation, and expertise of our local, state, federal, and international partners.

A. Intelligence

Strategic Goal
Establish an enterprise-wide intelligence capability that optimally positions the FBI to meet current and emerging national security and criminal threats.

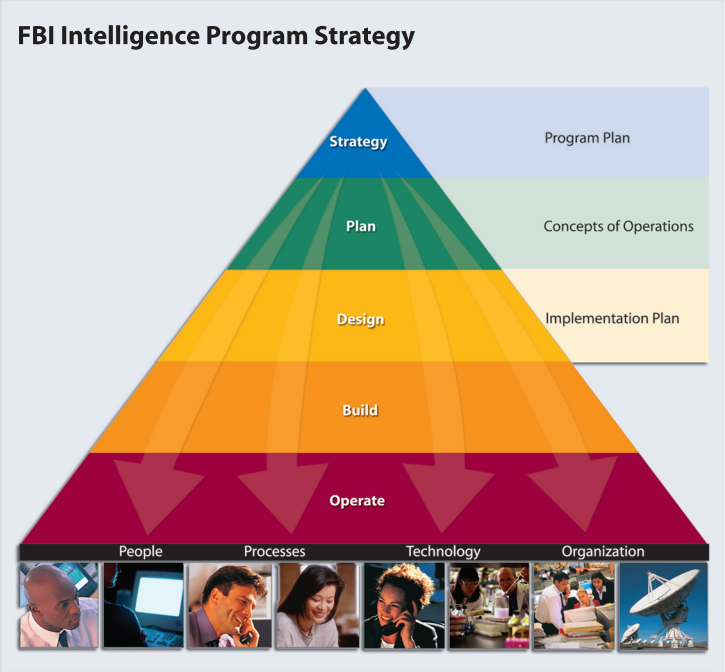
Situation
Intelligence is more important than ever in today's evolving threat environment. Having the right information at the right time is essential to protecting our nation. The FBI has always had outstanding intelligence collection capabilities. Intelligence is a core competency that is organic to the FBI's investigative mission and is embedded in Headquarters' divisions, field offices, and Legats as an enabling function. The FBI's many successes in addressing seemingly intractable criminal and terrorist organizations such as La Cosa Nostra, the Sicilian Mafia, Russian Organized Crime, Fuerzas Armadas de Liberacion Nacional (FALN), and the Weathermen were directly attributable to an extensive intelligence base and a proactive posture. However, a changed threat requires a new approach.

The FBI has a mandate from the President, Congress, the Attorney General, and the DCI to protect national security by producing intelligence in support of its own investigative mission, national intelligence priorities, and the needs of other customers. The FBI must serve the American people with an enterprise-wide Intelligence Program that effectively uses investigations to serve national security, homeland security, and law enforcement purposes, that meets external needs for FBI information and analysis, and that protects civil liberties.

The FBI has already made substantial progress in establishing a preeminent national Intelligence Program. The Director elevated intelligence collection, analysis, production, and dissemination to a level equal to that of our traditional Investigative Programs. He established an Executive Assistant Director for Intelligence and selected a 24-year senior intelligence professional to serve in that position. Concepts of operations for each of the intelligence functions have been developed and are currently being implemented. The importance of the FBI's national Intelligence Program cannot be overstated. In fact, an enterprise-wide intelligence capability is fundamental to the success of each of the FBI's investigative responsibilities from terrorism to violent crimes.

Strategic Objectives

IIA.1 Create a common approach to intelligence work through enterprise-wide doctrine, policy, and production standards.



The elevation of the FBI's intelligence function to the program level allowed us to centralize management and create and implement a detailed blueprint for the Intelligence Program. The FBI will uniformly implement, across all programs, its obligation to produce intelligence and share it with our customers. The FBI views its mandate to produce intelligence as one part of a three-pronged set of responsibilities. In addition to producing intelligence, the FBI will also ensure that the constitutional rights of all citizens are protected and that it uses its intelligence resources responsibly. The intelligence work of the FBI is threat-based, but constitutionally bound.

Priority Actions

- Develop and communicate to internal and external stakeholders doctrine and policy for: (1) the production and use of intelligence among the practitioners of intelligence, the managers of FBI intelligence resources, and the users of intelligence within the FBI; (2) the scope of the FBI's authority to conduct intelligence activities; (3) the framework to implement that authority; and (4) the role of the intelligence function within the FBI.

- Prescribe a set of standards for intelligence production that relate to: (1) recognizing and understanding requirements; (2) communicating with customers and processing feedback; (3) conducting research and analysis; (4) writing; and (5) reviewing and coordinating products.

IIA.2 Fill intelligence gaps by means of a uniformly managed intelligence process.

An intelligence gap is an unanswered question about a terrorism, counterintelligence, cyber, or criminal issue or threat. In essence, it is "knowing what you don't know." Requirements are set by the national Intelligence Community, and analysts identify intelligence gaps within that framework. Intelligence gaps will be communicated to investigative program managers at FBI Headquarters and the Office of Intelligence through the submission of program assessments; responses to crime, threat, or capabilities surveys; as components of operational plans or strategies; or in single issue communications. Additionally, requirements managers at FBI Headquarters and in Field Intelligence Groups will maintain a list of existing intelligence gaps for each FBI investigative priority. Intelligence gaps will be incorporated by the Office of Intelligence into FBI-wide requirements and collection plans and strategies to ensure that the intelligence needs of the FBI and those of our national, international, state, and local partners are addressed. Both Headquarters operational entities and Field Intelligence Groups will be tasked with satisfying these intelligence requirements. Requirements that cannot be satisfied within the FBI will be communicated as requests to external agencies.

Priority Actions

- Establish and oversee the Intelligence Requirements and Collection Management process to fill the intelligence needs of internal and external customers.

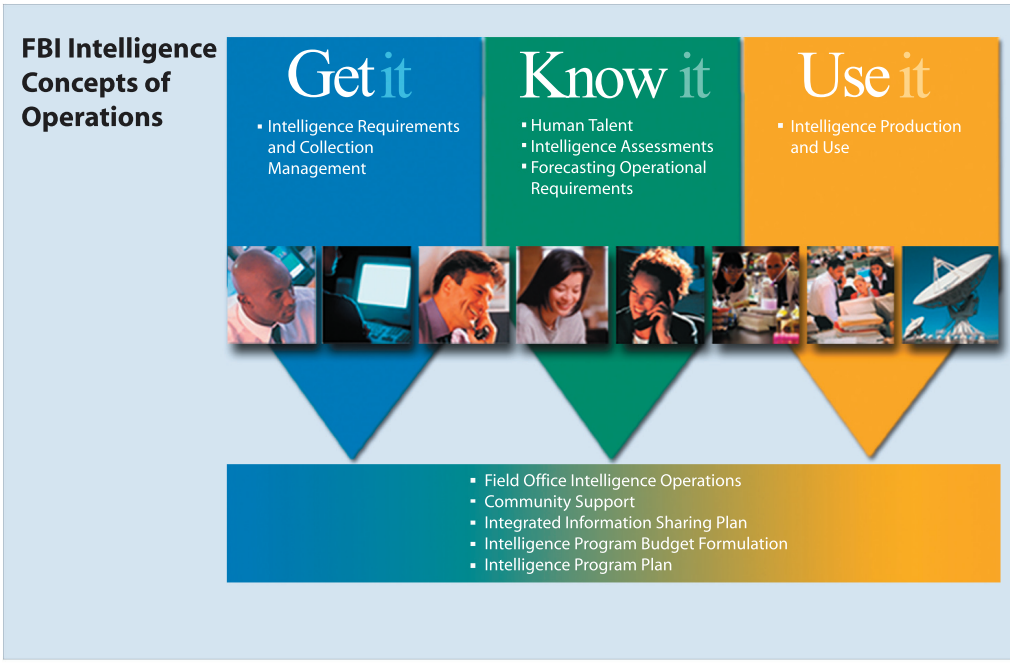
- Oversee intelligence functions by establishing a Field Intelligence Group in every field office to support the field requirements process and target collection efforts.

- Oversee and coordinate intelligence work that is conducted by Headquarters components.

The Intelligence Process

IIA.3 Align operations and capabilities with the threat environment.

To carry out its mission, the FBI requires a variety of capabilities or tools, some unique to the FBI and some leveraged from the larger federal, state, and local government and business communities. The FBI uses these capabilities according to their utility in countering emerging threats. When a terrorism, counterintelligence, cyber, or criminal threat is perceived, the FBI strategically employs its limited personnel and financial resources, using the appropriate operational capabilities



to counter or eliminate the threat. To ensure maximum preparedness of these capabilities and strategic deployment of its operations, it is imperative that the FBI have an organizationally shared view of the current and future threat and operating environment. This shared view can only be achieved by fully integrating intelligence and investigative components. Investigations must be intelligence-driven in order to maximize their effectiveness and impact. Likewise, intelligence components must make full use of information gleaned during investigative activities in order to accurately update and project the future threat and operating environment.

Priority Actions

- Fully integrate intelligence and investigative work by ensuring that strategies are based on an enterprise-wide understanding of the current and future threat environment.

- Continually develop, motivate, and retain a highly trained, diverse and appropriately-sized intelligence workforce that is aligned with the Intelligence Human Talent Needs Forecast. This includes assessing, evaluating, and implementing policies and procedures related to recruiting, hiring, training, and career development for analysts and Special Agents who choose a career specialty in intelligence.

- Establish organizational processes for developing, acquiring, and maintaining the information management infrastructure based upon the Intelligence Technology Needs Forecast.

- Identify, justify, and communicate the financial resources required to support the FBI intelligence mission, with a cross-programmatic budget formulation process that is aligned with the forecasting process.

IIA.4 Support internal and external intelligence customers and partners with corporate information sharing and appropriate support strategies.

The FBI is the nation's foremost collector of terrorism, counterintelligence, cyber, and criminal activity information. Historically, the challenge has been to share this information effectively within and outside the FBI. The Office of Intelligence serves as the FBI's primary interface for the dissemination and receipt of intelligence information with the Intelligence Community, Law Enforcement Community, and national and international government agencies. It is charged with establishing systems to ensure timely sharing of intelligence information in a useful format across program lines. It also has final review authority over intelligence products to be disseminated outside the FBI. Dissemination is performed at FBI Headquarters and field offices. Tasks and requests to satisfy intelligence requirements will clearly identify customers who should receive products so that intelligence is disseminated horizontally, as well as vertically.

Priority Actions

- Effectively share FBI data internally and externally; share by rule, and hold back by exception, with appropriate use and dissemination.

- Create an identifiable FBI intelligence brand that is rooted in quality, timeliness, responsiveness, and consistency through both customer support plans and ongoing assessment of customer satisfaction.

- Facilitate the management of partnership relations by presenting a coherent picture of the FBI Intelligence Program to partners in the Intelligence and Law Enforcement Communities.

B. Counterterrorism

Strategic Goal

Protect the United States from terrorist attack.

Situation

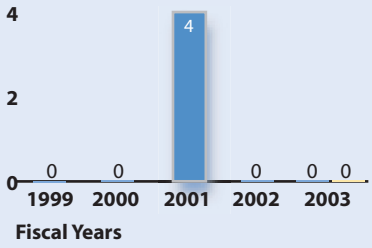
Terrorism is the most significant national security threat our country faces. The FBI counterterrorism goal is specific and compelling — it must prevent, disrupt, and defeat terrorist operations before attacks occur. Effectively combating this threat presents unique and unprecedented challenges. The terrorists' target is clear: the United States and its interests both here and abroad. However, terrorist planning, methods, sponsorship, and operational timing are typically obscured by meticulous and compartmentalized planning, the effective use of permeable international borders and often friendly state-sponsors, and the ability to adapt and evolve as efforts against them become effective. Terrorists' ability to obtain and use WMD materiel and technology for mass casualty attacks must be curtailed.

In the international terrorism arena, FBI investigations have revealed an extensive militant Islamic presence in the United States. The activities of these militants are focused principally on fund-raising, recruitment, and training, but they have a sufficiently well-structured and well-developed support system that could be activated to carry out operations within the United States and abroad.

The FBI's greatest concern currently is the threat from al-Qaeda attack cells, which retain the ability to inflict serious harm with little or no warning. These cells maintain strict operational and communications security and minimize contact with militant Islamic

Terrorist Acts Committed by Foreign Nationals Against United States Interests within U. S. Borders

6 Terrorist acts by foreign nationals



Data Definitions: Terrorist Acts Committed by Foreign Nationals counts separate incidents that involve the "unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives." (28 C.F.R. Section 0.85). For the purposes of this measure, the FBI defines a terrorist **act** as an attack against a single target (e.g. a building or physical structure, an aircraft, etc.) Acts against single targets are counted as separate acts, even if they are coordinated to have simultaneous impact. For example, each of the 9/11 acts (North Tower of the World Trade Center (WTC), South Tower of the WTC, the Pentagon, and the Pennsylvania crash site could have occurred independently of each other and still have been a significant terrorist act in and of itself. The FBI uses the term terrorist **incident** to describe the overall concerted terrorist attack. A terrorist **incident** may consist of multiple terrorist **acts**. The 9/11 attacks, therefore, are counted as four terrorist acts and one terrorist incident.

groups and mosques in the United States to avoid drawing attention to themselves. Al-Qaeda will continue efforts to acquire and develop various WMD (biological, chemical, radiological, and nuclear) and will continue to favor sensational attacks.

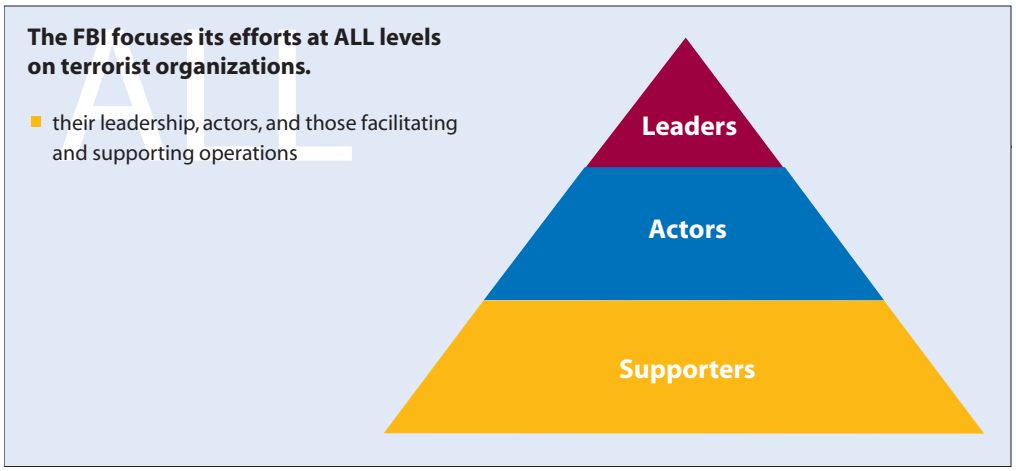
Although al-Qaeda is the most lethal of the groups associated with the Sunni jihadist cause, there are numerous other terrorist groups, any one of which could attack U.S. interests. Groups that are committed to jihad and offer al-Qaeda varying degrees of support include: Algerian extremists; Al-Gama'at al-Islamiyya; 'Asbat al-Ansar; Al-Ittihad al-Islami; Ummah Tameer-E-Nau; The Libyan Islamic Fighting Group; Hizb-e-Islami Gulbideen; and An Nahda.

HAMAS and Hizballah also have an extensive presence in the United States, and have the ability to carry out attacks domestically. Up until 9/11, Hizballah had killed more Americans than any other terrorist organization.

The events of 9/11 shifted the FBI's focus to international terrorist groups operating inside the United States, but not to the exclusion of domestic groups that threaten the safety of our citizens. The threat of domestic terrorists launching large-scale attacks to inflict mass casualties is low compared to that of international terrorist groups, due, in part, to longstanding efforts to disrupt and dismantle these groups. The most significant domestic terrorism threat over the next five years will continue to be the "lone wolf" terrorist. Inspired by the ideologies of formal terrorism groups, their relative anonymity limits law enforcement detection capability and makes prevention extremely difficult, while their ability to mount successful and high-profile terrorist events remains — as evidenced by the 1995 bombing of the Murrah Federal Building in Oklahoma City by Timothy McVeigh and bombings by Eric Robert Rudolph at the 1996 Atlanta Summer Olympics, health clinics in Georgia and Alabama, and an alternative lifestyle bar in Atlanta, Georgia.

Right wing domestic terrorism groups will continue to target law enforcement officials and minority groups. Militias will primarily disrupt the personal and financial lives of their targets (government workers and elected officials) by misuse of property claims or liens against personal assets. White supremacists, traditionally the most violent right wing group, have strengthened their recruiting and rhetoric since 9/11.

As left wing terrorism groups regenerate over the next five years, they will again pose a threat to economic and law enforcement targets. Violent protests against the perceived effects of trade globalization on human rights, labor rights, and the environment will continue and likely escalate. Recent examples of left wing "anarchist movement" activity include large-scale, destructive protests at World



Trade Organization and International Monetary Fund meetings. Special-interest extremism incidents have increased over the last several years and will continue to be problematic, primarily in the violent fringes of animal rights and other social movements. Research laboratories, pharmaceutical and cosmetic companies, and organizations that monitor or lobby against animal rights/"eco-terrorist" groups will be potential victims.

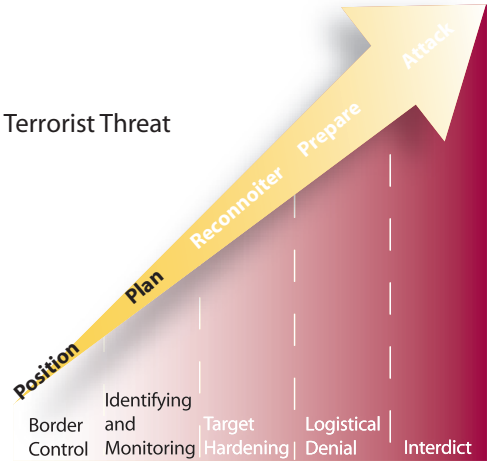
The FBI's counterterrorism successes to date have been largely determined by its flexibility, leadership, and collaboration with the U.S. Intelligence Community and its foreign and domestic law enforcement partners. Since 9/11, the FBI has: (1) shifted its counterterrorism culture and organization from reactive to proactive and "threat-based"; (2) developed a nationally-driven, fully integrated Intelligence and Investigative Program; (3) improved information sharing with other federal agencies, state and local governments, and international counterterrorism partners; (4) enhanced operational capabilities within FBI Headquarters and the field; and (5) evaluated lessons learned to better equip the nation in preventing terrorism. The FBI will continue to work closely with its intelligence and law enforcement partners focusing on full disruption of terrorist operations.

The danger of the convergence of terrorism and traditional crime presents obvious and acute dangers. Fortunately, the USA PATRIOT Act enables the FBI and its Intelligence Community partners to address all aspects of the threats posed by terrorist organizations by using both information and the tools of intelligence and criminal investigators to maximize the impact on terrorist organizations and their supporters. The FBI has the unique ability to bring national security and law enforcement efforts under the same roof and to integrate the intricacies of intelligence work with the authority to investigate and arrest terrorist suspects.

The FBI is strategically positioned, through its multi-agency Joint Terrorism

Task Forces (JTTFs) located at Headquarters and in every FBI field office, to protect against terrorists by merging international intelligence efforts with the work of local law enforcement first responders. Similarly, FBI efforts to internationalize its counterterrorism efforts — from Special Agents integrated with the U.S. Military in Afghanistan, Iraq, and Guantanamo Bay, to pursuing investigations initiated in the United States to their logical conclusion overseas — have yielded dramatic results. The FBI will continue to expand its Legal Attaché Program, in which experienced agents are assigned to critically located U.S. Embassies abroad. We will also continue ongoing efforts to shift our international operations from simple liaison to dynamic operational partnerships with host country law enforcement and intelligence counterparts. Domestically, the FBI will continue to work closely with Department of Homeland Security (DHS) and community stakeholders in the counterterrorism preparedness arena — to protect the nation's critical infrastructure from attack; to protect major special events that present an operational opportunity for terrorists; to prepare against the use of WMD materiel and technology within the United States; and to focus on traditional domestic terrorism groups planning criminal acts in attempts to effect political change.

Counterterrorism Challenge: Attack Terrorism at Any Stage



Strategic Objectives

IIB.1 Prevent terrorist attacks against the United States and its interests.

Limited windows of time exist for penetration of terrorist planning, and terrorists limit their exposure to insulate themselves. The FBI will increase its ability to uncover potential terrorist plots through analysis of information from the Intelligence Community coupled with robust human source reporting in field offices, as well as intelligence derived from the Foreign Intelligence Surveillance Act (FISA). Newly established threat protocols at FBI Headquarters provide rapid warning of threats and threat mitigation for successful disruption by JTTFs. Recognizing that creating an inhospitable terrorist environment within the United States is the best way to prevent attacks, the FBI will enhance local law enforcement first responders' and stakeholders' awareness of terrorist profiles and methodology through training and our enterprise-wide Intelligence Program.

Priority Actions

- Expand the intelligence base on terrorist groups and their supporters.
- Establish effective partnerships through the JTTFs.
- Expand the scope and breadth of human source reporting on terrorist groups and their supporters.
- Provide timely and accurate intelligence and analysis to the Intelligence Community, Law Enforcement, and senior policy makers.
- Engage in vigorous and effective information sharing initiatives both nationally and internationally.

IIB.2 Deny terrorists and their supporters the capacity to plan, organize, and carry out logistical, operational, and support activities.

The FBI will protect the United States from terrorist attack by disrupting terrorists' ability to conduct an attack. Training, financing, recruiting, logistical support, and pre-attack planning and preparation are all required components of terrorist operations and these interdependencies create vulnerabilities. As the centerpiece of its counterterrorism national strategy, the FBI will focus on exploiting intelligence developed by Special Agents and others working in the United States and overseas, and integrating Intelligence Community products into actionable information targeting those terrorist vulnerabilities.

Priority Actions

- Identify and disrupt leaders, actors, and facilitators/supporters.
- Enhance operations and intelligence gathering by developing and using emerging investigative techniques.
- Bolster international participation through foreign government liaison and enhanced Legal Attache operations.

IIB.3 Pursue appropriate sanctions against terrorists and their supporters.

Prevention of a terrorist attack requires neutralizing members of a terrorist organization before their actions lead to a terrorism-related prosecution. To successfully neutralize terrorists, the full range of available and appropriate government sanctions must be used.

Priority Actions

- Work with other Law Enforcement and Intelligence Community partners to fully and appropriately apply criminal and non-prosecutorial sanctions.
- Deny terrorists access to financial resources, using both civil and criminal actions, to disrupt critical support for terrorist organizations.
- Provide information that denies foreign terrorists and their supporters entry into the United States, or leads to their exclusion, removal, surveillance, or prosecution.

IIB.4 Provide incident response and investigative capability.

Just as the terrorists targeting the United States and its interests abroad operate with adaptability and flexibility, so too must the FBI. The FBI maintains a robust incident response capability, as well as an ability to adjust to emerging and evolving circumstances provided by the new threat environment. The FBI is poised to respond immediately to any threat, both domestically and internationally, with all necessary resources to pursue terrorism investigations and intelligence operations with specially trained investigators using a wide array of tools, including state-of-the-art forensics.

Priority Actions

- Expand the capability to immediately deploy, both domestically and abroad, elements such as the FBI "Flying Squad" and Rapid Deployment Teams to emerging terrorism investigations and incidents.
- Ensure the readiness of each field office to provide crisis management.
- Develop training courses and competency baselines needed for maintaining the effective investigative capability of counterterrorism personnel.

- Establish an operational management training program for select counterterrorism personnel, ensuring ongoing management and leadership expertise.

IIB.5 Identify and respond to WMD threats and fully coordinate the investigative response of the U.S. Government to a WMD threat or attack.

Recent findings indicate that terrorist organizations are showing an increasing interest in the acquisition and development of weapons of mass destruction. As proven by the anthrax attacks following the 9/11 terrorist attacks and the plot by Jose Padilla to detonate a radioactive "dirty bomb," the use of WMD by terrorists is a very real possibility. The FBI must be prepared to mitigate the threat from a WMD attack through training and cooperation with state and local law enforcement partners, as well as federal agencies with homeland security responsibilities.

Priority Actions

- Each division will support a specially trained WMD coordinator to manage the preparedness and response effort in that division.
- Each division will establish and maintain a WMD Working Group with state, local, and federal first responders in the division's area of responsibility.
- Each division will conduct incident response exercises with members of the WMD Working Group and other community partners.

C. Counterintelligence

Strategic Goal
Protect the United States against foreign intelligence operations and espionage.

Situation
The foreign intelligence threat within the United States is far more complex than it has ever been historically. The threat is increasingly asymmetrical insofar as it comes not only from traditional foreign intelligence services but also from non-traditional, non-state actors who operate from decentralized organizations. Intelligence collection is no longer limited to classified national defense information but now includes targeting of the elements of national power, including our national economic interests. Moreover, foreign intelligence tradecraft is increasingly sophisticated and takes full advantage of advances in communications security and the general openness of U.S. society. In short, the foreign intelligence threat is more challenging than ever. In the fall of 2003, the Foreign Counterintelligence Program had investigations involving dozens of countries that focused on hundreds of known or suspected intelligence officers who were assigned to enter or travel within the United States. These investigations spanned all 56 field offices.

In order to meet these challenges, the Foreign Counterintelligence Program is being redesigned to become more nationally focused and directed. Through a more centralized program, the FBI will ensure its ability to establish priorities, be more proactive, and better engage other Intelligence Community agencies so that cooperation in important cases is immediate and seamless. A centralized program will also ensure that infrastructure issues will be consistently addressed and coordinated in order to ensure workforce expertise, that staffing matches the articulated foreign intelligence threat, and that a sufficiently broad and reliable intelligence base is developed. From this foundation, the Foreign Counterintelligence Program will be positioned to achieve its strategic objectives and ultimately reach its goal to prevent harm to the United States through foreign intelligence activity inimical to U.S. interests.

During the past year, the Foreign Counterintelligence Program has been invigorated by the introduction of a new and innovative National Strategy for Counterintelligence and a Program Plan, both of which are proactive in emphasis. At the same time, additional resources were introduced to the program. To enhance counterintelligence workforce expertise, a new four-week Counterintelligence Operations course was developed. All Special Agents assigned to the Counterintelligence Program are required to successfully complete this course. Computer-based distance learning courses are also available to all personnel on a

variety of counterintelligence topics. A counterintelligence training course for mid-level and executive managers was also initiated, covering topics in both the tactical and strategic areas of counterintelligence management.

The FBI plays an essential role in the U.S. Government's counterintelligence efforts and has the responsibility to produce domestic foreign intelligence in support of other members of the Intelligence Community. The FBI also has the responsibility to oversee the integration of domestic law enforcement and intelligence efforts to address intelligence threats in support of DCI imperatives. Our counterintelligence strategy involves centrally-managed, proactive, and nationally-directed initiatives, with prioritized and strategic objectives that support DCI imperatives, overseen by experienced and innovative Headquarters managers.

Success for the Foreign Counterintelligence Program will be reflected in the extent to which we are able to: (1) identify the objectives, the assets, and the operations of foreign intelligence services operating in the United States; (2) disrupt the operations of those foreign intelligence services; and (3) change the behavior of targeted institutions and individuals to minimize opportunities for their exploitation.

Strategic Objectives

IIC.1 Prevent or neutralize the foreign acquisition of WMD technology or equipment which, if acquired, would constitute immediate danger to the United States.

The devastating results of WMD being successfully used against the United States or its interests are self-evident. Therefore, eliminating the potential for a hostile group or foreign nation to enhance its capability to produce or use WMD is our top counterintelligence priority. We will strive to prevent WMD-related technologies from being openly or clandestinely transferred from the U.S. Government or the private sector to any foreign power, be it nation-state or non-state actor.

Priority Actions

- Know the potential WMD targets of interest to foreign services in the United States.
- Form strategic partnerships within the Intelligence Community, and with targeted industries and facilities.
- Conduct sophisticated operations against those foreign services targeting WMD to disrupt their efforts.

IIC.2 Prevent the penetration of the U.S. Intelligence Community.

The Intelligence Community holds the nation's most sensitive and essential secrets, and the continued security of our country demands that the FBI help prevent any foreign power from penetrating the Intelligence Community in any manner. The FBI will work closely with its Intelligence Community partners to enhance their ability to protect vital information and will engage in proactive measures to rapidly and aggressively identify and neutralize penetrations.

Priority Actions

- Know the potential Intelligence Community targets of interest to foreign services in the United States.
- Form strategic partnerships within the Intelligence Community.
- Increase human source coverage of foreign services targeting the United States.
- Understand the threat from the foreign intelligence officers and agents in the United States.
- Conduct sophisticated operations against foreign services targeting the Intelligence Community to disrupt their efforts.

IIC.3 Prevent the penetration of U.S. Government entities and contractors.

U.S. Government support of critical national research and development initiatives in a large number of agencies and involving thousands of government contractors must be protected. Compromise of these initiatives by those hostile to the United States would do irreparable harm. The FBI must effectively meet its responsibility to assess the threat against those projects and, with other Intelligence Community agencies, initiate operations to counter the threat.

Priority Actions

- Know U.S. Government entities and contractors of interest to foreign services.
- Form strategic partnerships with targeted agencies, industries, and facilities to understand the threat.
- Conduct operations to disrupt foreign targeting of U.S. interests.

IIC.4 Prevent the compromise of Critical National Assets.

Critical National Assets are any information, policies, plans, technologies, or industries that, if stolen, modified, or manipulated by an adversary would seriously threaten U.S. national or economic security. The FBI has a major role in identifying threats to Critical National Assets and assessing their overall vulnerability, especially in the areas of economic espionage, academic research, and private sector research and development.

Priority Actions

- Know Critical National Assets of interest to foreign services.
- Form strategic partnerships with the public and private sectors to identify Critical National Assets.
- Identify foreign targeting of those Critical National Assets.
- Conduct sophisticated operations to protect Critical National Assets.

IIC.5 Conduct counterintelligence operations focusing on countries that constitute the most significant threat to U.S. strategic objectives.

As the remaining world superpower, the United States is targeted from nearly every corner of the globe. The FBI will focus its counterintelligence resources on those countries and non-state actors having the greatest potential to harm U.S. interests, and will work to gain a greater understanding of the threats they pose. Specifically, the FBI will examine threats related to terrorism, espionage, weapons proliferation, national infrastructure, U.S. Government perception management, and foreign intelligence activities.

Priority Actions

- Understand the potential threat from the foreign presence in the United States.
- Conduct sophisticated operations against priority threat foreign intelligence services to identify their personnel, operations, and targets in order to disrupt their efforts.
- Advise policymakers of the threat and intelligence activities conducted by foreign powers in the United States.

IIC.6 Collect, produce, and disseminate domestic foreign intelligence and counterintelligence.

The FBI is authorized by Executive Order 12333 to collect, produce, and disseminate foreign intelligence and counterintelligence. Both the Executive Order and the National Security Act define "foreign intelligence" to include information about foreign governments, organizations, and persons. Historically, the FBI's focus has been on counterintelligence collection, and yet the FBI has a tremendous collection capability that can address collection requirements on numerous national intelligence topics that implement the National Intelligence Priorities Framework.

Priority Actions

- Leverage the FBI's expansive network of human sources to collect domestic foreign intelligence.
- Expand the FBI's domestic foreign intelligence collection capabilities.
- Ensure all domestic foreign intelligence is disseminated to the Intelligence Community.

D. Cyber

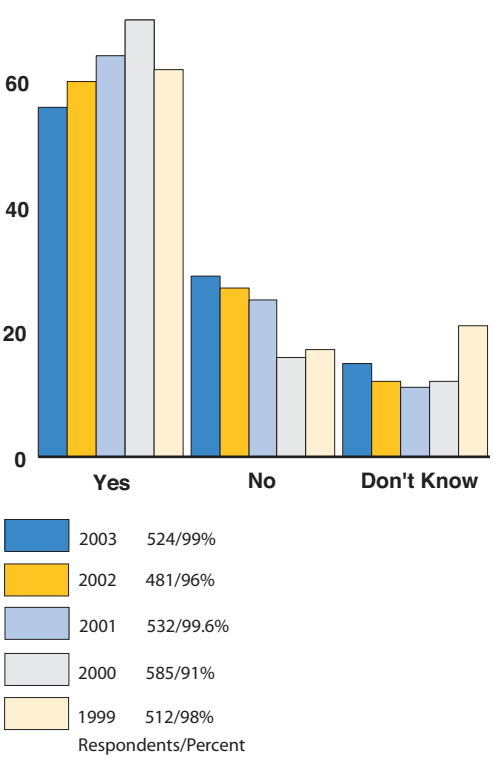
Strategic Goal

Protect the United States against cyber-based attacks and high-technology crimes.

Situation

The cyber threat confronting the United States is rapidly increasing as the number of actors with the tools and abilities to use computers against the United States or its interests is rising. The country's vulnerability is escalating as the U.S. economy and critical infrastructures become increasingly reliant on interdependent computer networks and the World Wide Web. Large scale computer attacks on our critical infrastructure and economy would have potentially devastating results.

Unauthorized Use of Computer Systems Within the Last 12 Months

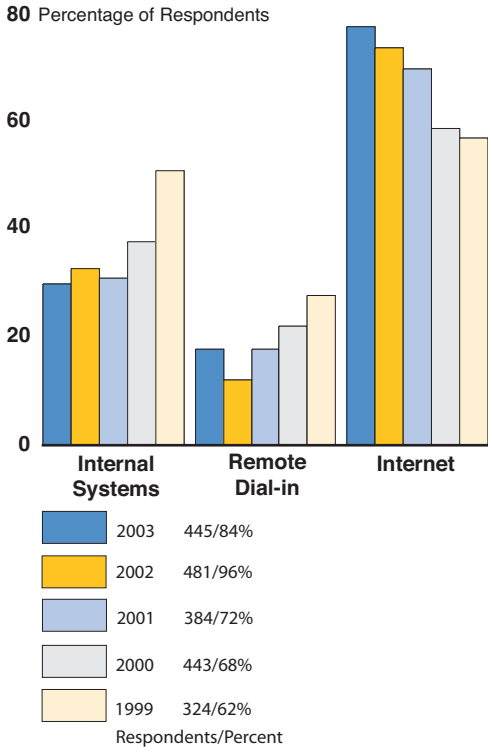


CSI/FBI 2003 Computer Crime and Security Survey
Source: Computer Security Institute

Cyber threats fall into two distinct categories: (1) threats affecting national security that emerged with Internet technology, such as cyber terrorism, foreign-based computer intrusions and cyber theft of sensitive data; and (2) traditional criminal activity facilitated by computers and the Internet, such as theft of intellectual property, online sexual exploitation of children, and Internet fraud. In both categories, cyber attacks, intrusions, illicit file sharing, and illegal use of cyber tools are the basic instruments used by perpetrators. Domestic and foreign terrorist organizations, foreign intelligence actors, and criminal enterprises are increasingly using encryption technology to secure their communications and to exercise command and control over operations and people without fear of surveillance. The FBI must be able to identify and penetrate the command and control elements of these organizations and actors.

Recognizing the international aspects and national economic implications of cyber threats, the FBI created a Cyber Division at the headquarters level to manage and direct this nationally-developing program. The rapid evolution of computer technology, coupled with ever-creative techniques used by foreign intelligence actors, terrorists, and criminals, requires FBI investigators and professionals to have highly-specialized computer-based skills. The FBI Cyber Program uses a centrally-coordinated strategy to support crucial counterterrorism, counterintelligence, and criminal investigations whenever aggressive technical investigative assistance is required. The Cyber Program also targets major criminal violators with a cyber nexus.

Internet Connections Increasingly Cited as a Frequent Point of Attack



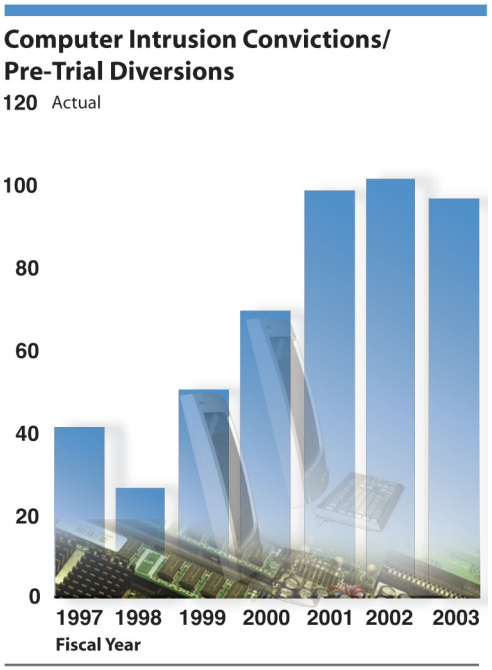
CSI/FBI 2003 Computer Crime and Security Survey
Source: Computer Security Institute

Strategic Objectives

IID.1 Identify and neutralize the most significant individuals or groups conducting computer intrusions, the dissemination of malicious code, or other computer supported operations.

The FBI must increase its capability to identify and neutralize enterprises and individuals who illegally access computer systems, spread malicious code, or support terrorist or state-sponsored computer operations. The FBI will proactively investigate counterterrorism, counterintelligence, and criminal investigative cyber-related threats having the highest probability of threatening national security. To do so requires the FBI to constantly upgrade its skills and technology to meet the evolving threat.

Priority Actions



- Reduce the cyber intrusion threat by fully identifying the scope, objectives, methods, and operations of perpetrators, specifically targeting those affecting national security.
- Working with DHS, develop a comprehensive list of cyber-related targets for monitoring and protection.
- Increase the number of Cyber Action Teams available for rapid deployment to enhance operational response to cyber events that have a significant impact on the United States or its interests.
- Increase the breadth and depth of human sources that have first-hand knowledge of computer intrusions.

IID.2 Identify and neutralize operations targeting U.S. intellectual property.

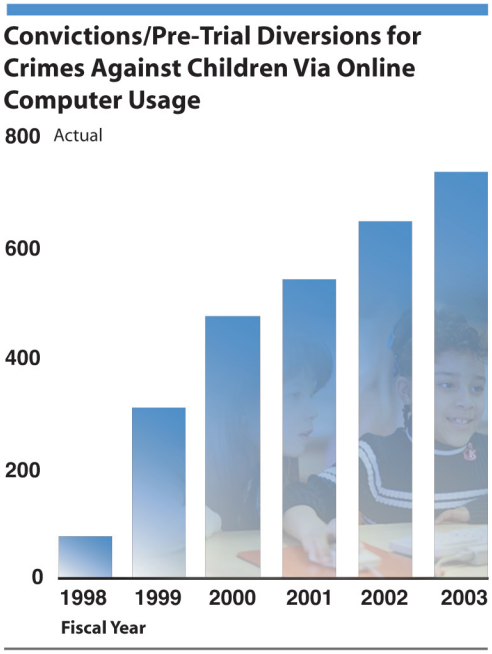
Theft of intellectual property affects U.S. competitiveness and economic viability. U.S. copyright industries and derivative businesses account for more than $433 billion, or nearly six percent of the nation's economy. Similarly, theft of trade secrets presents a serious economic and security threat. Trade secrets represent some of the most valuable assets within the nation's corporate community, as much as 85 percent of a company's value, the loss of which would do irreparable or fatal damage. Yet unlike buildings or products, the "mobility" of trade secrets make them one of the country's most vulnerable economic assets. Some intellectual property is so singular, or is so closely tied to national security research and development, that its loss to thieves or foreign intelligence services would cause incalculable harm. The FBI will primarily focus its intellectual property investigative efforts to protect those assets representing the greatest potential loss to the country. The FBI will also focus on theft of other proprietary information, particularly computer software, to outpace those targeting this area of our country's economic success.

Priority Actions

- Coordinate with federal, state, local, international, and industry partners to create and populate an intellectual property rights intelligence database.
- Create a "Cyber Stagehand" to provide backstopping and operational support to undercover operations targeting sophisticated perpetrators and criminal groups.
- Increase the breadth and depth of human source coverage of computer-based intellectual property theft.

IID.3 Identify and neutralize online predators or groups that sexually exploit and endanger children for personal or financial gain.

Multi-jurisdictional, and often international, sexual exploitation of children strikes at the heart of the country's most valuable and vulnerable asset — its youth. One in five Internet users in the United States is sexually solicited, usually at home. By 2005, 14 million child Internet users will be solicited, 2.3 million of those aggressively. The FBI will prioritize investigations involving organizations, e-groups or enterprises exploiting children for profit, and identify and neutralize the most significant online child sexual predators by expanding the Innocent Images database. The FBI will also target "travelers" meeting children they have lured online, and those producing, distributing, and possessing child pornography.



Priority Actions

- Further develop international partnerships to address online child sexual exploitation crimes.

- Expand efforts to educate children and parents about Internet dangers.
- Increase the breadth and depth of human source coverage of computer-based sexual exploitation of children.

IID.4 Identify and neutralize the most significant perpetrators of Internet fraud.

Organized criminal enterprises using the Internet for fraudulent activities present a significant and increasing criminal threat in the cyber arena. Typically, one or more components of the Internet is used to present fraudulent solicitations to prospective victims, conduct fraudulent transactions, or transmit the proceeds of fraud to financial institutions or others connected with the scheme. This crime problem is international and many schemes originate in the former communist countries of Eastern Europe. E-commerce is growing in all sectors of the U.S. economy, and while most is business-to-business, the dollars associated with e-commerce retail sales are growing exponentially. When Internet users — whether they are businesses or consumers — are crippled by Internet fraud schemes, the viability of e-commerce is compromised, adversely impacting the national economy. The FBI will focus its efforts on dismantling enterprises engaged in significant levels of fraudulent activity, especially those that are national and transnational.

Priority Actions

- Expand the intelligence base on criminal enterprises engaged in Internet fraud.
- Utilize the Internet Crime Complaint Center as the primary port for receipt and exchange of federal and industry Internet crime data, including cyber-related fraud.
- Conduct closely coordinated multi-jurisdictional investigations that identify and dismantle those organizations representing the greatest threat in terms of impact on Internet fraud.
- Increase the breadth and depth of human source coverage of Internet fraud.
- Penetrate hacking organizations through the recruitment and placement of human sources.

E. Public Corruption

Strategic Goal
Reduce the level of public corruption that has an impact in the United States.

Situation
Public corruption poses the greatest single threat to the credibility of government institutions at all levels. Corruption by those controlling the nation's ports of entry and handling the issuance of visas and other identity documents opens our country's borders to potential terrorists and other criminal actors. The serious increase in cases of law enforcement officers forming or supporting drug trafficking enterprises threatens the safety and security of our streets. Corruption within correctional facilities undermines our criminal justice and judicial system. When military contracts involving vital defense and weapons systems become the subject of bribery and kickbacks, national security is directly weakened. Many major metropolitan areas have witnessed the indictment and conviction of public officials for corruption-related activity, with public money being misused for private gain. Along with the increasing frequency of all types of corruption, the level of sophistication and complexity of this criminal activity present special challenges.

Corruption allegations are among the most sensitive matters addressed by the FBI. They must be investigated quickly, fairly, and accurately. Using a variety of federal statutes and investigative techniques, the FBI focuses investigations on all levels of government — federal, state, and municipal — and all branches of government — executive, legislative, and judicial. Approximately 50 percent of the FBI's public corruption investigations involve law enforcement officers, chiefly due to the sheer number of officers in the United States. Similarly, allegations against municipal and state public officials, frequently involving contract or regulatory matters, are regularly investigated because of the large number of such officials. Some of the FBI's most sensitive and highest impact investigations center on executive and legislative officials, as evidenced by the recent indictment of a former Illinois Governor, a former Texas Attorney General, and a sitting member of Congress. The FBI's Southwest Border Corruption Initiative will continue to target those officials who, by misuse of their public office, negatively affect commerce between the United States and Mexico, aggravate drug trafficking and violent gang activity, and endanger the security of our nation. Finally, when U.S. businesses bribe foreign officials to illegally compete in the international marketplace, the FBI investigates under the Foreign Corrupt Practices Act to prevent adverse impact on national security and foreign policy priorities.

In almost every case, greed is the principal motivating factor in public corruption. Over the next five years, government funding will expand, providing increased opportunity for government officials to engage in corruption. Similarly, as the United States increases security at the borders and in the issuance of identification documents, criminal enterprises will expand their recruitment efforts of public and law enforcement officials to bypass the increased security.

Strategic Objectives

IIE.1 Reduce law enforcement corruption within the United States to increase our country's public safety and national security.

Recognizing that any corruption within our nation's law enforcement agencies directly undermines public safety, the FBI aggressively investigates these crimes. The proliferation of drug trafficking enterprises in the past decade has led to increased corruption of public officials along the southwest border of the United States, who facilitate drug transhipments into the United States. Corrupt officials also facilitate illegal immigration, and this is expected to increase over the next five years. There is a serious concern that drug and alien smuggling organizations could be used by terrorists to facilitate their entry into the United States, and corrupt officials dramatically increase the success of smuggling operations. The FBI will need to increase its efforts in this arena to minimize the national security implications.

Priority Actions

- Expand the intelligence base to identify significant law enforcement corruption activity.
- Increase and strengthen membership in public corruption task forces to aggressively pursue significant law enforcement corruption.
- Increase training of Internal Affairs executives, investigators, and others regarding public corruption within state and local law enforcement and correctional entities to identify individual and systemic corruption, and increase coordination of operational activities when appropriate.
- Increase outreach to federal, state, and local stakeholders to identify public corruption trends and methodologies, increase reporting of potential violators, and educate to reduce corruption within the agencies.

- Conduct investigations that fully address significant law enforcement corruption.
- Expand the scope and breadth of human source reporting of law enforcement corruption.
- Deter significant corruption along the U.S. borders by aggressively pursuing regional anti-corruption strategies.

IIE.2 Reduce public corruption in the country's federal, state, and local governments and judicial systems to increase public confidence in our nation's government institutions.

Rapid, fair, and accurate investigation of corruption allegations against federal, state, and local officials will remain an FBI imperative. This is critical because of the sensitive nature of accusations against public officials, coupled with the tremendous loss of public funds and confidence when corruption occurs.

Priority Actions

- Deter corruption by aggressively pursuing high-level corruption.
- Strengthen partnerships with watchdog groups, the American Bar Association, ethics committees, the Federal Election Commission, and other stakeholders to identify public corruption issues and trends.
- Create and enhance media awareness campaigns to increase public support of anti-corruption initiatives and maintain confidence in government institutions.
- Expand the scope and breadth of human source reporting on corruption matters.
- Expand the public corruption intelligence base.

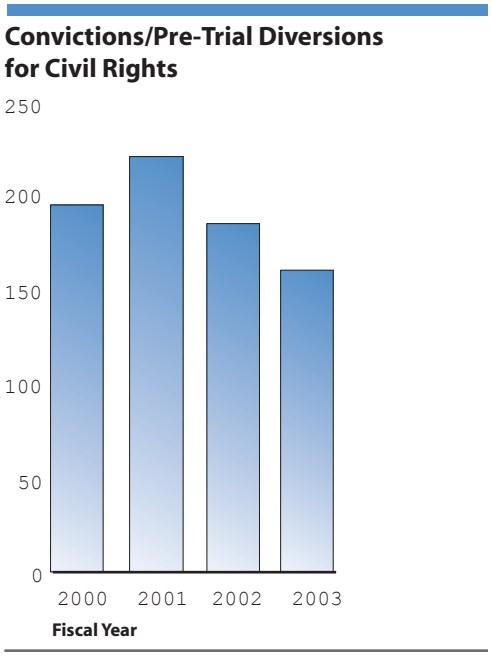
F. Civil Rights

Strategic Goal

Prevent the violation of federal civil rights as guaranteed by the U.S Constitution.

Situation

Federal criminal civil rights statutes protect individuals from hate crimes which interfere with protected activities such as voting, use of public accommodations, and access to housing. World and national events trigger periods when specific groups become targets of increased levels of hate crimes. For example, the 9/11 atrocity and its aftermath made the Arab, Muslim, and Sikh communities in the United States especially vulnerable to a wide range of hate crimes. Other groups that have been, and continue to be targeted are the African-American and Jewish communities because of their clear racial, ethnic, or religious identities.



In 2002, nearly 7,500 hate crimes incidents were reported to U.S. law enforcement agencies; nearly one-half were based on race, and the remainder primarily on ethnicity or national origin, religion, sexual orientation, or disability. These cases will dramatically increase if another international terrorist attack against the United States occurs.

Civil rights violations under "Color of Law" occur when those acting under the authority of local, state, or federal laws deprive an individual of rights, privileges, or immunities protected by the U.S. Constitution. The FBI has investigative responsibility for these violations and conducts approximately 1,400 preliminary investigations annually, including those involving allegations against members of state and local law enforcement and non-Department of Justice (DOJ) agencies. It is anticipated that over the next five years, increasing numbers of law enforcement officers will be hired. Although the Law Enforcement Community is overwhelmingly comprised of dedicated professionals, there remains a very small percentage that will violate the Color of Law statutes. As the number of law

enforcement personnel increases, so will the number of these violations.

The Involuntary Servitude and Slavery Act also protects individual civil rights and addresses a worldwide crime problem. According to the Department of State, between 18,000 and 20,000 persons, many women and children, are trafficked into the United States each year for involuntary servitude. The FBI investigates violations of the Act, and alarmingly, the number of cases grew over 2,000 percent from 1996 to 2003. The number of humans smuggled into the United States for this purpose will continue to increase over the next five years, and so will the opportunity for criminal enterprises to exploit these individuals.

The Freedom of Access to Clinic Entrance (FACE) Act protects individuals seeking to obtain or provide reproductive health care services from force or physical obstruction. Nationwide incidents related to abortion clinics include murder, death threats, assault, arson, burglary, harassing telephone calls, hate mail, and other acts of intimidation. The FBI aggressively investigates violations of this statute, which often have links to domestic terrorists who violently oppose abortion-related services.

Over the next five years, the FBI will likely need to enhance its capacity to investigate crimes involving violation of federal criminal civil rights statutes — laws designed to protect the invaluable civil rights of all persons within the country's territories.

Strategic Objectives

IIF.1 Reduce the incidence and adverse impact of hate crimes against at-risk groups.

The wave of backlash hate crimes against Muslim, Sikh, and Arab-Americans following 9/11 represents an example of the reactive demands often placed on the FBI. More than 500 hate crimes-related investigations were initiated in the immediate aftermath of 9/11, resulting in more than 160 federal and local prosecutions. The FBI will increase its ability to rapidly respond to hate crimes following triggering events, and expand its outreach to potential victim groups.

Priority Actions

- Increase partnerships with civil rights advocacy organizations, political and religious leaders, minority student organizations, and other groups related to at-risk populations to identify trends and provide education to reduce the incidence of hate crimes.

- Increase partnerships with local and state law enforcement agencies to address hate crimes.
- Develop and broaden media strategies to increase community hate crimes awareness, and ultimately decrease the number of hate crimes.
- Increase hate crimes training to federal, state, and local law enforcement agencies, and increase the readiness of law enforcement agencies to notify the FBI of significant incidents.
- Create a surge capability and develop strategies to augment existing resources after triggering events.

IIF.2 Minimize the occurrence of crimes under the Color of Law statutes.

The overwhelming majority of law enforcement and correctional officers in the United States are dedicated professionals, and through continued training the percentage of Color of Law violations are not expected to increase. However, while the percentage might not increase, the actual number of violations has the potential to expand due, in part, to the increasing numbers and turnover of law enforcement and correctional officers expected in the next decade. In addition, according to DOJ statistics, the number of individuals in U.S prisons and jails surpassed two million in 2003. With these large numbers of officers and inmates, Color of Law violations will likely increase in the next five years.

Priority Actions

- Identify law enforcement agencies and correctional facilities needing Color of Law-related training to reduce violations, and expand Color of Law training curricula to meet evolving trends and issues.
- Strengthen partnerships with local law enforcement agencies, Internal Affairs components, and citizens' oversight boards to address systemic police brutality where it exists.
- Deter Color of Law violators by aggressively pursuing all serious allegations.

IIF.3 Reduce the incidence of Involuntary Servitude and Slavery violations in the United States.

With the drastic increase of the number of Involuntary Servitude and Slavery violations within the last several years, the investigative priority of these crimes within the FBI has risen. Extensive education and training initiatives have been undertaken. The initiatives also focus on the proper handling of these sensitive cases, which are complicated by language barriers, victims' relocation by their captors to avoid law enforcement contact, captors' threats of victim deportation, threats of harm to family members in victims' home countries, and the victims' mistrust of law enforcement in general.

Priority Actions

- Expand the intelligence base on criminal enterprises engaged in significant human trafficking activity.
- Increase coordination with federal, state, and local law enforcement agencies nationwide to identify and assess potential violations, recognizing they are often strongly linked to other crimes such as prostitution and organized crime.
- Strengthen partnerships with non-governmental organizations to better coordinate the investigation of human trafficking crimes.
- Increase the breadth and depth of human sources on human trafficking activity.
- Identify, target, and dismantle those criminal enterprises engaged in significant acts of Involuntary Servitude and Slavery.

IIF.4 Reduce the incidence of FACE Act violations.

While overall criminal incidents against reproductive health care providers have decreased, there has been an increase in bioterrorism threats to them. In 2001 alone, dozens of clinics received hundreds of hoax anthrax letters, disrupting clinic activities and inflicting psychological trauma on clinic staff and patients. Significant federal, state, and local law enforcement resources were expended to restore access to facilities and identify perpetrators. Such cases continue to receive extensive interest from the media and advocates on all sides of abortion rights issues. Within the next five years, it is likely that lone actors will resort to violence against

reproductive health service staff. The FBI will continue to address allegations of FACE Act violations rapidly and fairly, without violating lawful demonstrators' First Amendment rights.

Priority Actions

- Expand the intelligence base on domestic terrorist organizations that violate the FACE Act.
- Increase the breadth and depth of human source reporting on domestic terrorist organizations.
- Strengthen established partnerships, community task forces, and working groups with local, state, and federal law enforcement components and organizations involved with FACE Act matters, such as the National Task Force on Violence Against Health Care Providers.
- Increase leveraging of resources with entities engaged in counterterrorism efforts in those cases where violations of the FACE Act are perpetrated by individuals or groups with a domestic terrorism nexus.

G. Transnational/National Criminal Enterprises

Strategic Goal
Reduce the impact transnational/national criminal enterprises have on the United States.

Situation
Criminal enterprises represent a near and long-term threat to our nation. The criminal activities of these enterprises are increasing in scope and magnitude as they network with each other to expand operations worldwide. The geopolitical and technological changes of the last decade have allowed these enterprises to flourish globally, and their impact on the United States is expected to increase over the next five years.

Organized crime groups from Russia and other former members of the Soviet Union are engaged in racketeering activity, and are deeply involved in large scale white collar crime. They are skilled in the use of monetary systems to funnel and conceal the proceeds of their criminal activity, employing state-of-the-art encryption to safeguard their communication networks against traditional forms of detection. Asian criminal enterprises are composed of U.S.-born citizens and immigrants. They are multi-crime organizations that, like other ethnically-based criminal enterprises, often victimize their own ethnic immigrant communities. These communities are typically hesitant to report victimization to authorities. As the immigration of Russian, former Soviet Union, and Asian populations into the United States increases in the next five years, so too will related ethnic organized crime. La Cosa Nostra (LCN) and Italian organized crime enterprises still pose a significant threat and will continue to influence the political and economic structure of the United States through engagement in racketeering-related activity. Alien smuggling and human trafficking will continue to pose significant threats to the national security, as transnational criminal enterprises expand their activities in this area for economic profit. In addition, the ability to facilitate the entry of illegal aliens into the United States could potentially be used to increase the membership of these criminal enterprises.

An emerging crime problem is Balkan criminal enterprises, specifically Albanian transnational organizations or clans. They are rapidly expanding their criminal activities to include loan sharking, weapons trafficking, alien smuggling, stock market manipulation, human trafficking, and drug trafficking. Additionally, these clans are forming partnerships with LCN crime families, as well as challenging traditional organized crime enterprises for territory.

Major theft rings account for billions of dollars in losses suffered by our nation's businesses, with corresponding price increases passed on to the U.S. consumer. Loss prevention and asset protection are top priorities for corporate America as increasingly sophisticated and highly organized criminal enterprises engage in cargo theft, high tech theft, vehicle theft, jewelry and gem theft, organized retail theft, art and cultural antiquity theft, and other major theft activity.

Drug trafficking remains a significant problem. The impact of illegal drug abuse is estimated to be over $160 billion in U.S. economic losses each year, including costs associated with health care, violent crime, and lost productivity. Colombian criminal enterprises are the largest source of cocaine in the world, and are also major heroin suppliers to the U.S. market. Mexican criminal enterprises manufacture and supply much of the methamphetamine available in the United States, and transport the majority of cocaine and heroin into our nation. The ability of Mexican enterprises to corrupt public officials in Mexico and the United States has enhanced their capability to transport and distribute these illicit drugs. Caribbean-based criminal enterprises specialize in the transportation and smuggling of drugs into Puerto Rico and the U.S. mainland. Over the next five years, South American and Mexican drug trafficking organizations will continue to maintain their dominance, and Caribbean-based groups will provide alternate importation routes.

A rise in homicides from 1999 through 2002, and continued incidence of other violent crimes have been attributed to the resurgence of violent street gangs in major metropolitan areas, such as Chicago, Los Angeles, and New York, which average approximately 600 homicides per year. Over the next five years, the FBI must continue to focus the resources of Safe Streets Task Forces to combat those violent street gangs having major impact in our communities.

Strategic Objectives

IIG.1 Disrupt and dismantle transnational/national criminal enterprises impacting the United States.

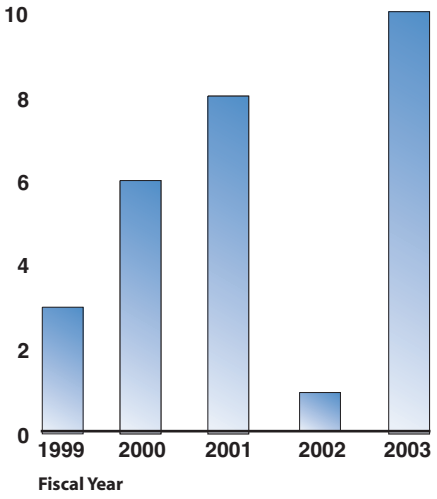
The FBI is uniquely qualified to combat organized crime groups, which themselves are diverse in the scope and location of their operations. Although success has been evident against LCN and the Sicilian mafia, challenges lie ahead in dealing with Russian, former Soviet Union, and Asian criminal enterprises, which are constantly establishing new footholds among immigrant communities in the United States. Particularly troubling are these organizations' involvement in human smuggling, which presents a threat to our national security.

Major Theft Criminal Enterprise operations are focused on conducting intelligence-driven investigations which target organizations engaged in these highly profitable crimes. Major Theft Task Forces, which combine interagency law enforcement resources, are often utilized to address this nationwide problem.

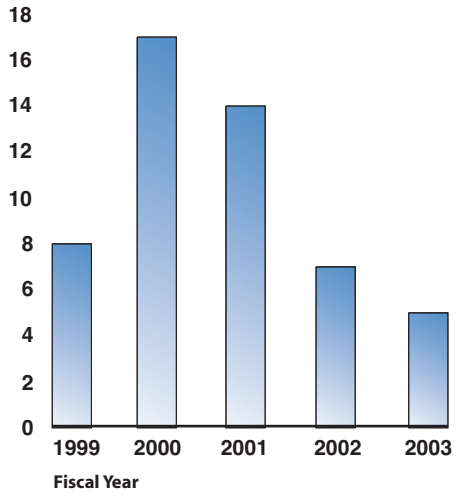
Priority Actions

- Expand the intelligence base on transnational/national criminal enterprises engaged in racketeering or major theft activities.
- Increase the use of multi-national initiatives such as the International Organized Crime Center and FBI-Hungarian National Police Organized Crime Task Force to target Eurasian criminal enterprises.
- Utilize and enhance alliances, task forces, and coordinated investigative efforts with domestic and foreign law enforcement counterparts to target and dismantle the most significant criminal enterprise threats
- Establish strong partnerships with corporate loss prevention and asset protection professionals to enhance the sharing of intelligence.
- Increase Intelligence Community partnerships to develop positive intelligence on transnational/national criminal enterprises.

Dismantled Eurasian Criminal Enterprises (FBI)



Dismantled Asian Criminal Enterprises (FBI)



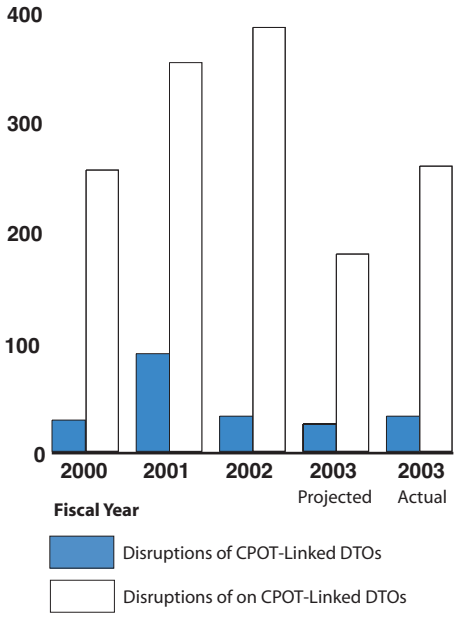
- Penetrate these organizations through the development and placement of human sources.

- Support the national security mission through the identification, disruption, and dismantlement of Major Theft Criminal Enterprises that support terrorist activity, target key U. S. industries, and threaten the nation's intermodal transportation system.

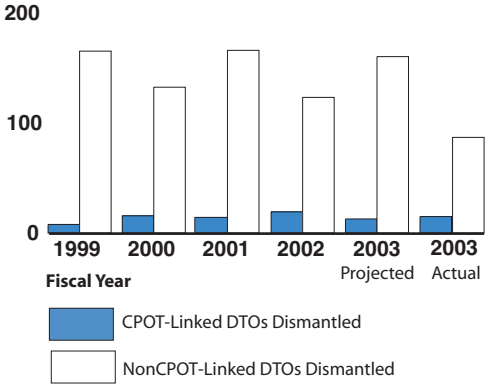
IIG.2 Reduce the impact drug trafficking criminal enterprises have on the United States.

The Drug Enforcement Administration (DEA) is the U.S. Government's primary investigative agency to combat drug trafficking. The FBI also has an important role to play, but seeks to complement DEA's efforts through an integrated approach. This strategy is essential in order to maximize our impact. The FBI will increasingly leverage its investigative resources by combining forces with DEA and state and local law enforcement agencies through joint efforts such as the Organized Crime Drug Enforcement Task Force (OCDETF) and High Intensity Drug Trafficking Area (HIDTA) initiatives. Through implementation of the National Intelligence Program, the FBI will provide DEA, the Intelligence Community, DHS, and state and local law enforcement agencies, with intelligence and other information needed to combat drug trafficking at all levels.

New Measure–Disruptions of Drug Trafficking Organizations (DTOs)



Dismantled Drug Trafficking Organizations (DTOs)



The FBI considers a DTO **dismantled** when, at a minimum, three objectives have been met:

1. the organization's leaders have been completely incapacitated;
2. the organization's financial base has been completely destroyed; and
3. the organization's drug supply conntection/network has been irreparably disrupted.

A **disruption** has occurred when the usual operation of an identified organization is significantly impacted so that it is temporarily unable to conduct criminal operations for a significant period of time.

Priority Actions

- Expand the intelligence base on significant drug trafficking organizations.
- Increase the co-location of FBI drug investigative resources with the DEA.
- Increase the use of the Special Operations Division and other specialized drug intelligence resources to identify and target the most significant drug trafficking criminal enterprises in cooperation with our partners.
- Increase participation in OCDETF task forces, HIDTA initiatives, and joint investigative operations with the DEA and state and local anti-drug units to maximize resources, expertise, and impact.

IIG.3 Work closely with local, state, and federal law enforcement partners to reduce the incidence of gang-related violence by eliminating or incapacitating the nations' most violent gangs.

Violent gangs pose one of the most significant violent crime problems in our nation's history. In major cities such as Chicago, Los Angeles, and New York, violent street gangs terrorize whole neighborhoods and control life in entire public housing complexes. Driven by a desire to protect drug sale locations and gang turf, these violent criminal enterprises are a large contributor to the high murder rates in our nation's metropolitan areas. Within the first six months of 2003, murder rates in the northeast United States continued to rise. New York, Newark, Philadelphia, and Baltimore all had significantly more murders in the first half of 2003 as compared to the same period in 2002.

In the summer of 2003, officials in Washington, D.C. declared a crime emergency during a spike in violent activity, much of which was gang-related. Conversely, in Los Angeles, where aggressive gang policing and investigations were a top priority, murders were reduced from 323 to 258 over the same time period. Due to its experience in conducting investigations of criminal enterprises, the FBI can provide expertise and resources to assist local, tribal, and state law enforcement agencies in the disruption and dismantlement of significant violent gangs. The FBI projects that the threat of gang-related violence will increase over the next five years and will require an increase in the number of Safe Street Task Forces to reduce this threat.

Priority Actions

- Expand the gang intelligence base to identify and prioritize the gangs responsible for a disproportionate amount of violent criminal activity.

- Develop integrated violent gang strategies with other federal, state, and local law enforcement agencies to maximize the impact on violent gangs.
- Establish a coordinated national strategy with federal law enforcement partners to ensure the most efficient deployment of various task forces.
- Utilizing Safe Street Task Forces and other inter-agency cooperation, develop investigations on these criminal enterprises, and use the enterprise theory of investigation to dismantle major violent gangs.

H. White Collar Crime

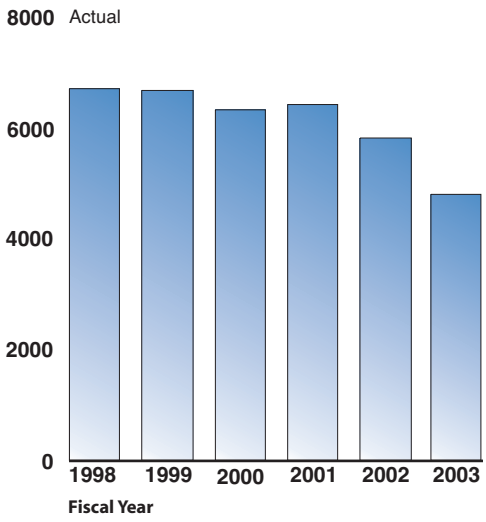
Strategic Goal

Reduce the level of significant white collar crime.

Situation

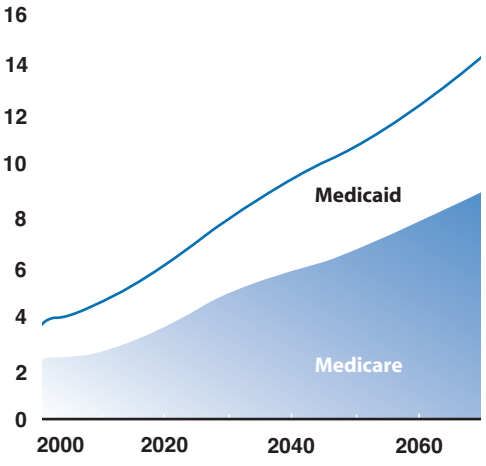
Since the 1990s, tremendous growth of and involvement in the securities and commodities markets at the institutional, corporate, and private investor levels have led to great numbers of individuals involved in intentional corporate fraud and misconduct, particularly senior corporate executives. For example, the FBI is currently investigating over 189 major corporate frauds, 18 of which have losses over $1 billion. The erosion of public confidence in the management of public companies will, if left unchecked, have a negative impact on the stock markets and capital raising, which will in turn have a negative impact throughout the U.S. economy.

Convictions/Pre-Trial Diversions in White Collar Crime



Health care fraud continues to plague the United States, with losses exceeding $50 billion annually. Frauds involving durable medical equipment, staged auto accidents, and medical transportation services are examples of this pervasive crime problem. In addition to Medicare/Medicaid and private insurers, state providers lose billions of dollars per year to blatant fraud schemes in every sector of the health care industry. As health care spending increases over the coming years with the aging of the "baby boom" generation and Medicare prescription drug coverage, health care fraud is expected to have a corresponding increase.

Percentage of GDP



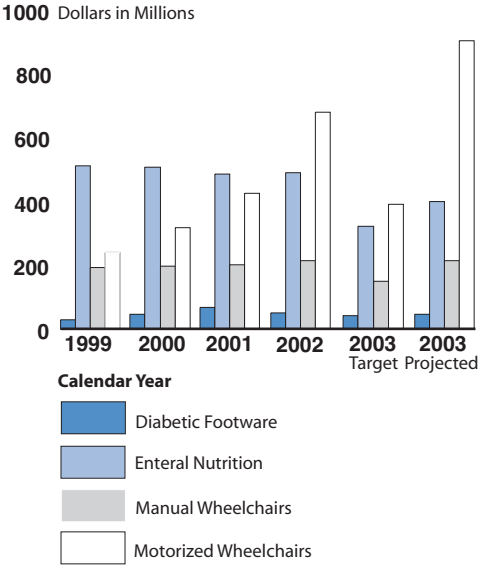
Source: center for Medicare and Medicaid Services' Office of the Actuary and Congressional Budget Office

Financial institution fraud (FIF) continues to be a significant white collar crime problem throughout the country. Since 9/11, the FBI has refocused its FIF program and is now investigating higher-priority cases to a much greater degree. Large-scale mortgage fraud and identity theft operations, many perpetrated by organized criminal enterprises, also continue to plague the United States.

Aggressive use of anti-money laundering statutes and forfeiture of ill-gotten assets are integral parts of nearly every financial crime prosecution. Many top executives involved in corporate scandals have been charged with money laundering in addition to other criminal violations. Additionally, corrupt money launderers introduce illegal proceeds into the financial community, and this asset flow must be reduced through aggressive prosecution, seizure, and forfeiture.

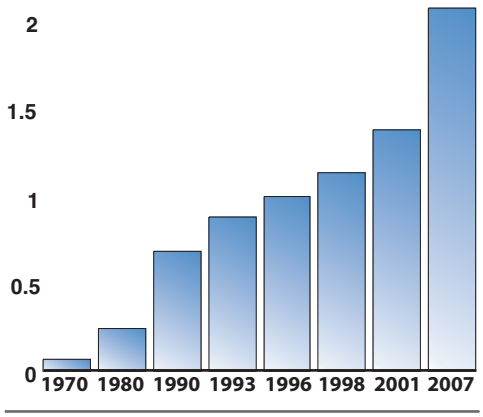
The ability of the U.S. Government and industry to function effectively is likewise threatened by complex frauds. The amount of taxpayer funds involved in the government procurement process is staggering, as billions of dollars are spent each year on everything from highways to rockets. The GAO estimates that as much as 10 percent of appropriated funds for domestic programs may be lost to fraud in the government procurement and contracting process, and this type of crime is critically linked to public corruption imperatives.

Medicare Billings for Durable Medical Equipment Target for Fraud



Data Definition: **Enteral Nutrition** is defined as the provision of nutritional requirements through a tube into the stomach or small intestine.

Projected Health Care Expenditure
(Projected 2012 $3.1 Trillion)



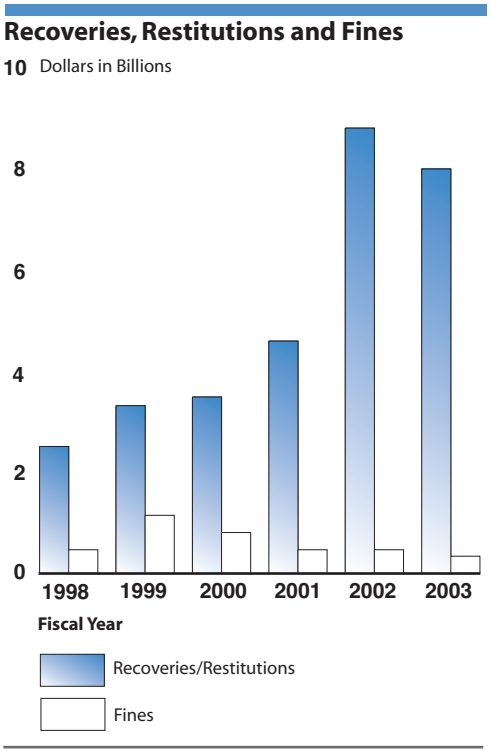
Insurance, telemarketing, and investment frauds often operate across jurisdictional and international boundaries. When losses to individual victims are aggregated, the economic impact can be dramatic. Additionally, anti-trust offenses and bankruptcy fraud have a significant negative affect on the U.S. economy, and environmental crimes represent a serious threat to the public health and natural resources of our nation.

The FBI will continue its successful efforts in the white collar crime arena by using its expertise, broad criminal investigative resources, and strong relationships with regulatory agencies to maintain public confidence in the country's financial institutions and markets, ensure the integrity of government expenditures of taxpayer funds, and protect individuals and businesses from catastrophic economic loss.

Strategic Objectives

IIH.1 Reduce levels of corporate fraud by targeting those groups or individuals engaged in major corporate fraud schemes that significantly impact the investing public and financial markets.

Fraud by company executives and those in positions of trust not only damages stockholders, but also erodes public confidence in the corporate community at large. The FBI will continue increasing its efforts in this area by using agents and analysts with high degrees of expertise in financial investigations. The sheer complexity of illegal corporate transactions require extraordinary time and commitment to investigate.



Priority Actions

- Expand the intelligence base through private sector and community outreach specifically focused on private industry personnel, government regulators, and all levels of law enforcement.

- Initiate major investigations on all aspects of corporate fraud.
- Incorporate aggressive asset forfeiture actions in every criminal case to strip violators of their ill-gotten gains.
- Develop human sources that can substantially reduce the time and resources dedicated to complex investigations.

IIH.2 Reduce the incidence of large scale health care frauds, involving both government-sponsored and private insurer programs.

Because the illegal profit potential for this crime problem is virtually unlimited, and because the health care industry is among the most complex, the FBI must continue to build on its relationships with related government agencies and stakeholders to effectively prevent abuse.

Priority Actions

- Expand the intelligence base to identify regional fraudulent billing patterns within vulnerable segments of the health care industry such as pharmaceuticals, durable medical equipment, transportation services, outpatient services, and home health services.
- Deter health care fraud by identifying and targeting national regional chains of service providers engaged in systemic health care schemes.
- Incorporate aggressive asset forfeiture actions in every criminal case to strip violators of their ill-gotten gains.

IIH.3 Reduce fraud perpetrated by criminal enterprises targeting financial institutions.

The health of our country's financial institutions remains a national economic priority. The FBI will continue to prevent financial losses to these institutions by focusing on criminal enterprises engaged in financial institution fraud, including insider fraud, major check fraud, mortgage fraud, and identity theft.

Priority Actions

- Improve relationships with traditional, as well as non-traditional and expanding industries.

- Expand the intelligence base in order to identify major criminal enterprises that victimize financial institutions on a regional and national basis.
- Conduct worldwide investigations to dismantle criminal enterprises engaged in significant financial institution fraud.
- Implement strategies to increase the number of asset forfeiture actions in criminal cases to strip violators of their ill-gotten gains.
- Expand the use of nationally-coordinated initiatives and investigations, using emerging investigative techniques.

IIH.4 Disrupt and dismantle the most significant money laundering institutions and facilities.

The FBI will target the most significant corrupt money laundering industries and facilities in the United States by increasing the cost of criminal activity, creating barriers to entry of illegal proceeds into the financial community, developing national strategies to address the mechanisms and industries commonly used to launder funds, and by reducing the flow of criminal assets through seizure and forfeiture.

Priority Actions

- Expand the intelligence base to identify methodologies, geographic anomalies with domestic and international criminal proceeds, and significant money laundering enterprises, industries and facilities.
- Conduct worldwide investigations that result in the dismantlement of those enterprises, industries, and facilities engaged in significant money laundering.
- Incorporate research and analysis software products into the overall intelligence base.
- Increase the number of human sources reporting on significant money laundering activities.
- Ensure potential money laundering strategies are incorporated into counterterrorism and criminal enterprise investigations to maximize asset forfeiture potential.

- Provide extensive training to the entire Law Enforcement Community to promote the use of asset forfeiture and money laundering statutes in all investigations.

IIH.5 Reduce the impact of telemarketing, insurance, and investment fraud on businesses and individuals, particularly schemes originating from outside the United States.

Telemarketing fraud typically targets the elderly, one of the most vulnerable sgements of our society. The FBI will focus on major telemarketing enterprises, recognizing the difficulties faced by state and local investigators because criminal operations typically cross jurisdictional lines — often internationally. Insurance and investment fraud have similar multi-jurisdictional attributes, making enterprises difficult to investigate and prosecute by state and local agencies.

Priority Actions

- Expand the intelligence base on telemarketing fraud.
- Develop and execute a public awareness campaign about telemarketing and insurance fraud to reduce its impact on communities and business.
- Increase the number of human sources that can provide detailed information on criminal enterprises engaged in telemarketing fraud.
- Expand the use of nationally-coordinated initiatives and investigations, using sophisticated and innovative investigative techniques.

IIH.6 Address those investigative matters which represent the most significant economic losses within federally-funded procurement, contract, and entitlement programs, environmental crimes, bankruptcy fraud, and anti-trust offenses.

Because government fraud is inextricably linked to the FBI's obligation to combat public corruption and national security threats, the FBI will focus efforts on major schemes with those links. Because serious public health and safety concerns relate to environmental crime, the FBI will enhance its working relationships with federal, state, and local investigative and regulatory agencies to address this crime problem. We will also focus on bankruptcy and anti-trust offenses having the greatest negative economic impact.

Priority Actions

- Increase the intelligence base on government fraud, environmental crimes, and major bankruptcy fraud.
- Establish a deterrence by identifying, prioritizing, and targeting most egregious violators and enterprises.
- Incorporate aggressive asset forfeiture actions in every criminal case to strip violators of their ill-gotten gains.

I. Significant Violent Crime

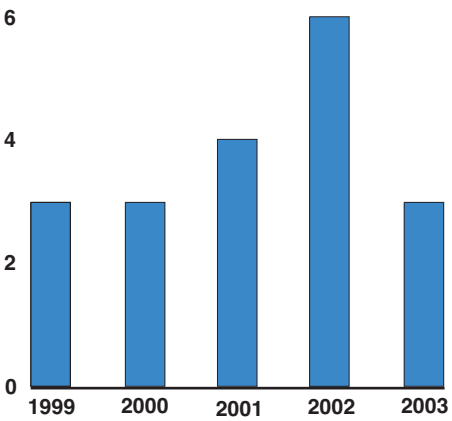
Strategic Goal

Reduce the level of significant violent crime.

Situation

Significant violent crime continues to plague our nation's metropolitan areas, threatening the well-being of countless innocent residents. Although violent crime rates have generally decreased over the last five years (1997-2002), murders have increased over the last three years (1999-2002), and violent crime continues to plague certain cities. Major violent crime incidents, such as sniper murders and child abductions, can paralyze whole communities and stretch state and local law enforcement resources to their limits. Notorious fugitives, such as those listed on the FBI's Top Ten fugitive list, remain uncaptured, avoiding the measure of justice they richly deserve. Over 300,000 children per year are forced into prostitution, where they are exploited in an organized fashion that extends across state lines. Interstate theft rings cost U.S. companies billions of dollars each year in losses, increasing the costs of goods to all Americans.

Number Dismantled of the 30 Targeted Gangs Identified As Most Dangerous



From the days of fighting our nation's first "gangsters" during the 1920s and 1930s, through the institution of Safe Streets Task Forces to combat emerging violent street gangs in our major cities, the FBI has successfully employed its unique resources to make America safer. However, in the current threat environment where our resources must also be used to combat terrorism, foreign intelligence activities, and cyber crime, the FBI must sharply focus its violent crime resources and efforts to obtain the greatest impact. We will do so by integrating our violent crime efforts with local, state, and federal partners and by establishing a coordinated national strategy with DOJ, United States Attorney's Offices, DEA, Bureau of Alcohol, Tobacco, and Firearms, and the United States Marshals Service.

II/I.1 Ensure a rapid, effective, and measured reactive capability to address those violent incident crimes that pose the most significant threat to our citizens.

Major violent incident crimes, such as the "Washington, D.C. Sniper" murders, which claimed the lives of 10 citizens, including FBI Analyst Linda Franklin, and child abductions, such as the kidnaping of Elizabeth Smart, require significant infusions of Law Enforcement Community resources and include the duty to provide the public with timely updates and suitable public safety information. These crimes often have an inherent interstate aspect, necessitating coordination of investigative leads from across the country. The FBI plays a critical role in the Law Enforcement Community's response to these major violent crimes, because of its resources, experience, technical capabilities, investigative acumen, national and international lead coverage, and expertise in crisis management, command post operations, tactical operations, crime scene processing, and forensic analysis.

Priority Actions

- In partnership with other federal, state, and local law enforcement agencies, aggressively investigate significant violent crime incidents through deployment of focused resources in task force environments.

II/I.2 Reduce the incidence of other violent federal crimes.

Violent crime incidents continue to threaten our citizens. Bank robberies, extortions, kidnapings, product tampering, transportation crimes, and crimes on federal lands cause significant loss of life and economic damage. Violent fugitives who have committed heinous crimes attempt to escape justice by crossing state lines or fleeing our nation's borders. Due to our national and international presence, the FBI is uniquely situated to address these violent crimes and reduce their incidence by aggressive and comprehensive investigations.

Priority Actions

- Expand the intelligence base on violent criminal activity.
- Arrest the most dangerous violent fugitives who pose significant and continued threats to the citizens of the United States.
- Enhance the safety and security of domestic transportation systems by reducing violent incidents or threats of violence involving transportation modes over which the FBI has investigative jurisdiction.

- Ensure an operational readiness to immediately respond to special jurisdiction incidents over which the FBI has investigative jurisdiction.

II/I.3 Reduce the incidence of crimes against children.

Our nation's children constitute our most vulnerable and easily victimized population segment. Child abductions and homicides affect entire communities and often shatter the victim families. The "Amber Alert" system has raised public awareness about child abductions and has served as an effective tool in the quick resolution of some cases. However, other incidents require long-term, resource intensive investigations to bring the perpetrators to justice. Additionally, the problem of child prostitution is just now being fully recognized. Thousands of children per year are forced into this illicit industry in order to survive. They are exploited by organized criminal organizations that often operate across state lines.

Priority Actions

- Expand the intelligence base in order to identify and prioritize those criminal enterprises engaged in child prostitution.

- Increase the solution rate of child abduction cases by enhancement of the Child Abduction Response Plan and by FBI field offices providing immediate, effective response to reports of child abductions.

- Fully develop and implement a Child Prostitution National Initiative and conduct multi-divisional, enterprise-based investigations of child prostitution criminal enterprises.

- Disrupt and dismantle child prostitution enterprise infrastructure by appropriate use of sophisticated investigative techniques, asset forfeiture, and incarceration of enterprise leaders.

II/I.4 Reduce the incidence of significant violent crimes in Indian Country.

Crime trends in Indian Country generally mirror those of our nation, particularly violent crime trends. Murders, aggravated assaults, and crimes against children plague our nation's reservations. Reservations have also become home to drug trafficking organizations and violent street gangs. Legitimate Native American gaming establishments are susceptible to corruption due to the vast amounts of cash inherent in their operation. A vital partnership between the FBI, Bureau of Indian Affairs, and Tribal Police is crucial to ensure the safety of our Native American nations.

Priority Actions

- Expand the intelligence base on all criminal activity occurring in our Indian Country including criminal enterprise activity.
- Expand the Safe Trails initiative to focus on unaddressed or under-addressed significant violent crime matters.
- Conduct joint enterprise investigations to dismantle significant criminal enterprise activity in Indian Country.
- Develop a greater capacity to address Indian gaming matters, and initiate investigations into allegations of corruption of Native American nations' gaming operations.
- Conduct training of Tribal Police and other law enforcement agencies involved in Indian Country law enforcement to enhance investigative capabilities.

J. Partnerships

Strategic Goal

Increase support to our federal, state, county, municipal, and international partners.

Situation

An important part of the FBI's mission is to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners. This mission has never been more important than today with the globalization and convergence of crime and terrorism. Criminal enterprises operating around the world, enabled by new technologies and seamless borders, now have the ability to threaten the public safety in townships, municipalities, and counties throughout our nation. The FBI must be able to serve as a national focal point for information and provide accurate and timely services to local, state, federal, and international law enforcement agencies, the private sector, academia, and other government agencies. In so doing, our nation will be better positioned to address current and evolving terrorist, foreign counterintelligence, cyber, and criminal threats.

To emphasize the importance he places on partnerships, Director Mueller created a new Office of Law Enforcement Coordination (OLEC) within months of assuming the directorship in mid-2001. Headed by an Assistant Director who is a former Chief of Police and charged with overseeing the FBI's revitalized commitment to partnership activities, this office has done much to improve the flow of information and enhance support services.

Every investigative program and most support functions in the FBI rely on partnerships to achieve success. As can be seen elsewhere in this plan, each FBI program that has a partnership element within its planning efforts has already listed goals and objectives that address specific aspects of these relationships. This section provides further testimony to the FBI's expanded commitment to partnerships by highlighting those programs where liaison and cooperation are particularly significant and have a major impact across program lines and agency boundaries.

Strategic Objectives

IIJ.1 Expand the FBI's ability to provide local and state law enforcement agencies worldwide investigative support.

Over the next five years, transnational criminal organizations will have an increasingly negative impact on local communities throughout the United States. The FBI will need to expand its Legal Attaché Program to better assist local, state, and federal law enforcement agencies in covering time-sensitive investigative leads and in seeking international assistance. The FBI will increasingly be asked to assist local and state law enforcement authorities in addressing major violent criminal activity, including sniper attacks, serial murders, and violent gangs, all of which have a direct impact on public safety. The FBI will need to increase its flexibility to provide immediate resources to support local law enforcement when the need arises. Likewise, the FBI is often called upon to assist its international partners with investigative and technical expertise, requiring the deployment of personnel.

Priority Actions

- Increase the level of investigative and technical support to local and state law enforcement agencies.
- Increase the level of investigative support the FBI can provide to our international partners.
- Develop Violent Crimes Response Teams to assist Law Enforcement Community response to major violent crime incidents.

IIJ.2 Provide our local, state, federal, and international partners the intelligence and information they need to perform their duties.

The FBI is in the process of establishing an enterprise-wide Intelligence Program that integrates the intelligence needs of our local and state law enforcement partners into its collection, production, and dissemination processes. The Global Intelligence Working Group of the International Association of Chiefs of Police has agreed to serve in an advisory capacity to this process. The Global Intelligence Working Group is comprised of local and state law enforcement experts who have provided leadership in the criminal intelligence arena.

Priority Actions

- Fully incorporate the intelligence needs of local and state law enforcement into the FBI enterprise-wide intelligence processes.

IIJ.3 Increase the level of forensic support the FBI provides to local, state, federal, and international agencies.

The FBI Laboratory was created in 1932 and today is one of the largest and most comprehensive crime laboratories in the world. The Lab supports federal and non-federal criminal justice systems by: (1) conducting scientific analyses of physical evidence; (2) providing specialized scientific and technical support to ongoing investigations; (3) developing an automated database of DNA patterns from evidence or individuals for examination and comparison; (4) providing expert testimony in court; (5) developing a database and network software to match and exchange images of firearms evidence from violent crimes; and (6) providing specialized forensic science training, analysis, and technical assistance to laboratory personnel and crime scene training to law enforcement personnel. The proper and timely collection, preservation, and forensic analysis of evidence is a vital part of criminal investigations, and the FBI will increasingly be called upon to provide this service to our partners. (See pages 103-107 for greater detail on forensic services.)

Priority Actions

- Provide correct, unassailable, and timely evidentiary results and objective testimony in support of other agencies.
- Support law enforcement operations through the improvement and enhancement of scientific and forensic response capabilities.
- Improve existing, and establish and implement new technical capabilities, databases, protocols, policies, procedures, standards, and guidelines.
- Strengthen liaison with national and international forensic laboratories and law enforcement agencies in order to improve training and burden-sharing.

IIJ.4 Increase the level of investigative technology support the FBI provides to local, state, and federal agencies.

The FBI provides technical and tactical services in support of investigators and the Intelligence Community, including electronic surveillance, cyber technology, and wireless and radio communications. The FBI also develops new investigative technologies and techniques and trains technical agents and personnel. These technologies and techniques are essential tools in combating sophisticated terrorist organizations, foreign intelligence services, and criminal enterprises. (See pages 92-96 for greater detail on investigative technology services.)

Priority Actions

- Fulfill all legislative and regulatory Communications Assistance for Law Enforcement Act (CALEA)-related mandates, to include overseeing the industry's development and testing of solutions and capability enhancements and deploying technical electronic surveillance solutions.

- Increase the digital forensics capabilities available to state and local law enforcement through the expansion of the Regional Computer Forensic Laboratory (RCFL) Program.

IIJ.5 Increase the level of support the FBI provides to local, state, federal, and international agencies through the Criminal Justice Information Services (CJIS) Division.

The CJIS Division, located in Clarksburg, West Virginia, provides essential services to our federal, state, and local law enforcement partners through the Integrated Automated Fingerprint Identifications System (IAFIS) and the National Crime Information Center (NCIC). IAFIS is a state-of-the-art automated system which accepts and processes fingerprint submissions and related transactions electronically. NCIC serves as a repository for criminal history records, which are accessed by users when searching for arrest record information. IAFIS maintains the FBI's national database of fingerprint features and has the capability to process up to 62,500 ten-print fingerprint searches and 635 latent fingerprint searches daily. NCIC is a nationwide computerized information system accessed by more than 80,000 law enforcement and criminal justice agencies. It provides a computerized index of documented criminal justice data on crimes and criminals, and includes locator-type files on missing and unidentified persons. NCIC averages 3.5 million transactions per day. CJIS must continue to provide first-rate services to the increasing demands of its customers and look for new ways to deliver service more efficiently, including the Internet. (See pages 97-102 for greater detail on CJIS services.)

Priority Actions

- Streamline the entire fingerprint business for faster processing.

- Make the delivery of CJIS services more efficient.

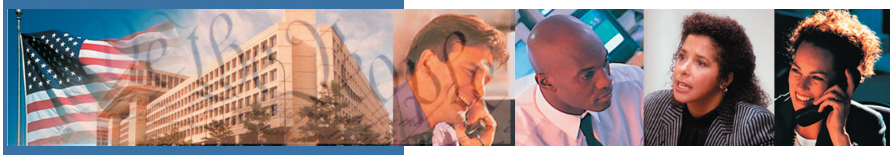
IIJ.6 Increase the level of training support the FBI provides to local, state, federal, and international agencies.

Since 1935, the FBI has offered executive police training programs to experienced law enforcement managers from the United States and around the world. These programs include the National Executive Institute, Law Enforcement Executive Development Seminar, and the FBI National Academy. In fiscal year 2002, the FBI provided training to more than 8,000 foreign police officers and executives representing 118 countries through courses offered at FBI facilities and at on-site, in-country seminars. The FBI also administers an International Law Enforcement Academy (ILEA) in Budapest, Hungary and supports a second ILEA in Bangkok, Thailand. The curricula of both ILEAs are based on the FBI National Academy model.

Priority Actions

- Provide increased training in intelligence, leadership, and strategic planning to local, state, federal, and international agencies.
- Increase the amount and quality of other training opportunities provided to international agencies in support of institution building.

SECTION III



HUMAN CAPITAL

The MEN *and* WOMEN *of the* FBI *are its* GREATEST ASSET.

As Director Mueller has stated many times, the men and women of the FBI are its greatest asset. The mission requires that Special Agents, analysts, scientists, managers, and professional support employees not only perceive and comprehend complex threats, but also attack them as a team, working together with a shared sense of urgency.

Strategic Goal

Establish a human capital capability that ensures the FBI maintains a preeminent workforce at all times.

Situation

The GAO's Comptroller General recently told attendees at a conference sponsored by the National Academy for Public Administration that "the key competitive difference in the 21st Century will be people. It will not be process. It will not be technology. It will be people."

This statement could not be more true for the FBI today as it faces incredible new challenges. As Director Mueller has stated many times, the men and women of the FBI are its greatest asset. The mission requires that Special Agents, analysts, scientists, managers, and professional support employees not only perceive and comprehend complex threats, but also attack them as a team, working together with a shared sense of urgency.

Historically, the FBI has used the Special Agent position as the primary resource tool for addressing issues across the entire spectrum of the organization. This included assigning agents to numerous non-investigative positions such as laboratory examiners, technical and language specialists, and legal counsel at FBI Headquarters. Today's dynamic environment requires a paradigm shift so that every Special Agent is involved in the core business of the FBI — addressing threats and crimes through investigative work, and performing other mission-critical jobs in the intelligence arena. Concurrently, other important tasks can and should be performed by professionals trained and hired in specific disciplines, or contracted out to the private sector. While we expect great progress with improved investigative and information technology, and a reengineered organization dedicated to operating in a threat-driven environment, only a refocused workforce can execute the strategic plan and guarantee the success of our mission.

A. Recruitment and Hiring

Strategic Objective

IIIA.1 Establish a system to recruit and hire critically skilled and diverse individuals to address our intelligence and law enforcement missions.

The FBI has always had great success attracting some of the best candidates available from either the public or private sector. Historically, the FBI hired lawyers, accountants, and former military or law enforcement officers as Special Agents, and hired general clerical employees for its support staff functions. As the mission has become increasingly more complex, the FBI has reevaluated its hiring goals while continuing to recruit the best possible talent. The FBI has identified critical skills required in both the Special Agent and professional support ranks to meet its new challenges. They include skills related to science and information technology, engineering, life sciences, intelligence and counterterrorism, financial analysis, accounting, and investigative technology. Recruiting and hiring people with these skills is challenging because they are in high demand across a broad spectrum of employers. We also need a cadre of highly talented clerical employees to sustain daily operations. Fortunately, it has long been considered an honor to be an employee of the FBI, and in the post-9/11 environment of renewed patriotism, that spirit is manifested in continually larger pools of qualified applicants for most positions. A fundamental requirement for employment is a demonstrated record of excellence achieved in a professional occupation. The FBI may have to make allowances to address critical skill gaps; however, we have found that the best indicator for future success is past performance.

Priority Actions

- Develop a needs forecasting integration system to identify new skills needed, and incorporate these into the business plan.
- Develop a marketing plan using proven business strategies to aggressively promote FBI employment in critical skill areas as a significant contribution to the national security of the United States.
- Utilize technology and centralize the hiring process for Special Agents and critical skills professional employees to reduce the time it takes to get these employees recruited, processed, and hired.
- Develop significant partnerships between senior FBI executives and recognized members of national minority interest groups to increase the diversity of our workforce.

B. Training and Development

Strategic Objective

IIIB.1 Develop a system that dramatically expands the total training and career development of the FBI's professional workforce.

For many generations of Special Agents and state and local law enforcement officials, the FBI Academy and the FBI National Academy at Quantico, Virginia, have represented the pinnacle in law enforcement training. In recent years, the FBI expanded its employee training efforts beyond training for new agents to include a robust in-service training program for both Special Agent and professional support employees, mostly based at the FBI Academy. However, the changing threat environment and the FBI's new priorities require the organization to develop new training programs on a continuing basis to assist employees in developing skills necessary to address evolving threats. The FBI has already adjusted its curriculum to meet today's challenges. For example, the FBI established the College of Analytical Studies to train and develop the critical skills of analysts who assess and evaluate data to detect threats to the nation. The FBI also partnered with other intelligence agencies to cross-train our analysts at their prestigious facilities in the latest analytical techniques. Training in counterterrorism and counterintelligence for new Special Agents has been increased by approximately one week, and will be increased further in the future in order to properly prepare the next generation of agents in this critical area. The FBI also has established and promoted world-class investigative and forensic training for our own employees, and also for our federal, state, and local law enforcement partners.

Priority Actions

- Continue expanding the new Office of Training and Development. This office is accountable for the development and distribution of training for all FBI employees across all job families and programs.
- Increase the initial training new Special Agents receive at Quantico in counterterrorism, counterintelligence, and cyber matters.
- Capitalize on the latest technologies, including distance learning, to develop a Learning Management System with the ability to deliver training from a variety of instructional platforms, including instructor-led, web-based, and video teleconferencing and satellite broadcasts.

- Expand current partnerships with premiere academic institutions to develop executive management training opportunities that expose current and future FBI leaders to the latest theories and practices in management, leadership, and professional development.

- Ensure the FBI National Academy successfully transitions from an institution that excels at teaching state and local law enforcement officers the latest criminal investigative techniques, to one that promotes the study of intelligence threats, management techniques, leadership development, and strategic planning.

- Improve the FBI's application of technology by maintaining a corps of trained technology specialists capable of delivering technical tools and services in support of field investigative efforts to collect intelligence and evidence.

C. Performance and Reward

Strategic Objective

IIIC.1 Provide timely and accurate feedback to all employees concerning their job performance and ensure the maximum use of appropriate award systems to reward outstanding performance.

The FBI spends 65 percent of its resources on personnel, evidencing once again that employees are its most valuable assets. All of the organization's employees have an expectation that they will be informed ahead of time what their professional responsibilities entail, and then receive timely feedback on how well they are meeting their responsibilities relative to expectations. The FBI currently has a performance appraisal system that is relevant, time sensitive, and legally defensible. However, the current system seemingly restricts employee evaluation to a determination that the employee meets or does not meet expectations. Many employees consider this a limited assessment of their job performance in critical functions. Therefore, appropriate ratings or mechanisms that allow for accurately describing extraordinary performance, and emphasizing the FBI's value on excellence, need to be developed, validated, and implemented.

As new job families are added to the organization, and new priorities are established for current employees, the FBI must ensure that these new positions and priorities are swiftly and accurately integrated into the performance and award system. For example, with the mandate that the FBI quickly transition from a case-driven to a threat-driven environment, the development and use of human sources is more critical than ever. Therefore, the FBI should restate and reprioritize the critical element of developing an intelligence base in the Special Agent and Intelligence Analyst performance plan. Increased attention to the intelligence function and identification of threats can be similarly integrated into numerous other job families as well. The FBI should ensure that its focus on counterterrorism and counterintelligence matters is reflected in a defined career path for Special Agents, and that agents who are promoted into executive management positions have significant experience and training in these two programs.

Priority Actions

- Upgrade existing technology to facilitate electronic performance appraisals to increase their timely preparation and presentation to all employees.
- Develop additional ratings or mechanisms to be used with FBI performance plans to better acknowledge outstanding achievement.
- Rewrite performance plans across all job families to ensure critical elements are consistent with the FBI's latest strategic plan.
- Ensure timely initiation of relevant performance plans for the newest categories of FBI employees in analytical and other positions to facilitate their recruitment and hiring in the shortest time frames.
- Continue efforts to develop innovative award recognition programs to highlight the efforts of deserving employees.
- Create a defined career path for Special Agents with an emphasis on counterterrorism and counterintelligence, with requirements that promotions be tied to experience and training in identified skill areas.

D. Discipline

Strategic Objective

IIID.1 Ensure the FBI maintains professionalism, excellence, and integrity by aggressively and impartially addressing allegations of employee criminality and misconduct in a timely manner.

To preserve the trust and respect of the American people, FBI employees must be held to rigorous standards of personal and institutional responsibility, enforced both internally and through responsiveness to external oversight. If recognized as a model of effectiveness, the Office of Professional Responsibility disciplinary program materially enhances confidence in and support for the FBI, thereby enabling the institution to better perform its mission.

Priority Actions

- Promote and enforce disciplinary policies and practices that balance the welfare of employees with the needs of the organization.
- Cultivate an organizational spirit of fairness by thoroughly and expeditiously investigating and adjudicating allegations of misconduct by FBI employees.
- Foster the values of integrity and ethics in the professional lives of FBI employees.
- Preserve the high-level of respect and cooperation that the FBI receives from the American public and throughout the national and international Law Enforcement and Intelligence Communities.

E. Leadership Development and Promotion

Strategic Objective

IIIE.1 Establish career development and succession planning initiatives that identify future leaders, and that further forecast the matriculation of each new wave of senior FBI executives through important leadership positions within the organization to ensure continuity.

All successful organizations accomplish their missions through effective leadership. Effective leaders are particularly important for organizations in environments of rapid change, and those leaders that are best able to drive successful change may do so more and more through motivation. As James Champy and Michael Hammer pointed out in their recent book on corporate reengineering, "In a reengineered environment, the successful accomplishment of work depends far more on the attitudes and efforts of empowered workers than on the actions of the task-oriented functional managers. Therefore, executives must be leaders who can influence and reinforce employees' values and beliefs by their words and their deeds."[1] While the FBI has always strived to promote effective leaders to senior executive management positions, the process has been more candidate-driven than strategically planned. The FBI first needs a forward-looking process to identify employees who display important leadership qualities early in their careers, and effectively mentor them into the ranks of management. Secondly, in order to successfully and rapidly transform the organization, the FBI needs to establish a tangible succession planning process. The goal of the program will be to systematically identify and develop talent to ensure leadership continuity for key positions within the organization.

Priority Actions

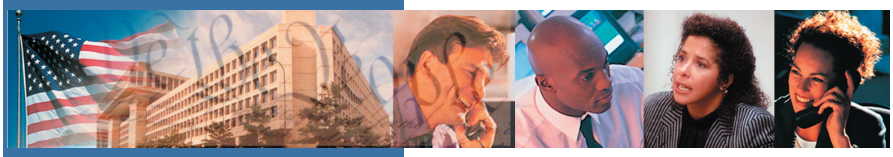
- Evaluate and acquire software capable of tracking the career progression of future senior FBI executives.
- Formalize a mentoring plan within the career development program that places responsibility for identification and development of future leaders on every incumbent manager in the FBI.

[1] Champy, James and Hammer, Michael, 2001. Reengineering The Corporation. Harper Collins, New York, p. 84.

- Develop key survey instruments to be completed by the candidate and others in the organization early in the career development process that gauges each candidate's skills and interests to assist with future assignments.

- Establish a Director's Executive Council comprised of Executive Assistant Directors, the operational Assistant Directors, and the Assistant Director, Administrative Services Division, that will be charged with tracking the career development of the highest potential senior executives in the FBI for appointment to future critical positions.

SECTION IV



TOOLS

Tools are fundamental to the FBI's ability to achieve its mission. Tools empower the FBI and its partners to gather necessary data more effectively and efficiently, convert it to actionable intelligence, and disseminate it to the parties best able to make use of it. Tools include such items as communications equipment and electronic surveillance devices (investigative technology); laboratory and psychological evaluation services (forensics); and databases and analytic software (information technology). Security is also a fundamental tool that must be fully integrated into the organization and its activities to protect our people, information, and techniques.

A. Security

Strategic Goal

Establish an enterprise-wide Security Program that protects our people, information, and capabilities.

Situation

Security is vital to the FBI's efforts to protect the United States. As the agency responsible for counterintelligence, counterterrorism, cyber, and major criminal investigations, the FBI is a high-priority target for virtually every hostile and many otherwise friendly intelligence services, terrorist organizations, criminal groups, and individuals with grievances against the U.S. Government. The nature of the threat posed by these various groups and individuals is a function of their intent, and thus varies with the particular agenda of each. Criminal groups, for example, benefit from knowing specifics of ongoing investigations. Timely knowledge of who is under investigation, which communication lines are under surveillance, or who is providing information to the government can effectively cripple an ongoing case. Because of its high visibility as a well-known element of the U.S. Government, many terrorist groups view the FBI as a desirable target for attack. Because of these threats, the Director of the FBI took immediate action to consolidate and centralize management of security programs by placing responsibility and authority for all such programs under the new Security Division. The Security Program will expand over the next five years guided by a philosophy of evolutionary rather than revolutionary change. It is assuming an oversight role in the management of security programs that were previously controlled by the field offices and the FBI Headquarters' divisions. The FBI recognizes that all security threats, vulnerabilities, and risks must be identified, assessed, evaluated, and managed using a systematic and rational process as part of a continuing operational strategy.

Strategic Objectives

IVA.1 Protect the FBI from compromise of its employees.

Security and counterintelligence professionals generally agree that the most significant threat to an organization's internal security is betrayal by a trusted insider. An individual with legitimate access who chooses to betray the FBI's trust is particularly damaging because compromise of information may continue over an extended period of time and encompass a wide range of programs. Worse, the insider can target his or her activities to compromise the information most relevant to the needs of the adversary. If undetected over a period of time, a person

could rise to a leadership position within an organization from which he or she may influence policy. To enhance countermeasures against these threats, the FBI developed, implemented, and expanded its Financial Disclosure and Personnel Security Polygraph Programs. These measures have already minimized the threat, but additional actions are needed to further protect the FBI and the nation.

Priority Actions

- Establish a Security Center of Excellence to provide expert security guidance to the FBI and its customers.
- Develop and implement the Security Division Management Information System which 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.

IVA.2 Protect the FBI from compromise of its communications and information.

The proliferation of information technology in recent years has resulted in dramatic changes in the threat environment. The explosion in electronic data handling has profoundly altered the manner in which most modern organizations, including the FBI, manage information. While modern technology allows the storage, movement, and retrieval of vast amounts of data to the benefit of investigators and analysts, it also allows, absent highly sophisticated security precautions, the lightning-fast theft of vast amounts of information, or the crippling of response capabilities in a time of crisis. Experience has shown that the cyber threat is typically a human problem, not a technical problem. Even though it is true that information systems and networks offer attractive targets, it is invariably the human element in those systems that make them exploitable. Information systems and networks have human involvement during the complete system life-cycle. They are vulnerable during construction, shipment, installation, operation, maintenance, and disposal. Advanced technology solutions alone will not solve the problem. The approach must be multi-disciplinary and must cover the complete life-cycle of information systems, data, and human intervention. To meet these threats, the FBI developed and implemented a Certification and Accreditation process that has been incorporated into the organization's information technology investment and development life-cycle, including all legacy systems. However, additional measures are needed to further protect the FBI from the compromise of its information technology systems.

Priority Actions

- 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 (ISSM) Program, with ISSMs assigned to all operational and major support divisions.

IVA.3 Protect the FBI from physical attack.

The unique position occupied by the FBI within the U.S. Government and in the public consciousness makes it a high priority target for terrorist groups seeking publicity, for criminal organizations wishing to intimidate or take reprisal, and for lone malcontents with specific grievances. No other federal government agency deals as directly, in what is nearly always an adversarial fashion, with the variety and number of violence-prone groups as does the FBI. Bomb threats and threats of other violence involving FBI facilities and personnel, while not commonplace, occur with sufficient frequency to generate increasing concern. There are an increasing number of threats directed at individual agents and their families as intimidation or retribution for activities carried out in the performance of their official duties. Additionally, since 9/11, increasing numbers of FBI personnel have been dispatched to areas of recurring terrorist and insurgent activities including Afghanistan, Saudi Arabia, and Iraq. The Security Division established a Risk Analysis Staff, which uses analytical risk management methodology to guide the development of threat analysis and development of appropriate risk mitigation decisions. Additional measures will be implemented to further reduce both the risk and consequences of an attack.

Priority Actions

- Establish intelligence-driven processes to proactively assess new security threats and the effectiveness of existing countermeasures, and make appropriate changes in protection strategies.
- Develop a Critical Mission Assurance Program with Continuity of Operations Planning at FBI Headquarters and in all field divisions.

B. Information Technology

Strategic Goal

Establish a secure, flexible, and modern information technology system that fully supports the collection, analysis, and dissemination of information.

Situation

Prior to 9/11, the FBI made substantial investments to upgrade technologies that directly supported investigations (e.g., surveillance equipment, IAFAS), but little attention was paid to technology related to the more fundamental tasks of records creation, maintenance, dissemination, and retrieval. As a result, the FBI's information technology infrastructure became antiquated and unable to support operations effectively. Most of the FBI's computer systems were designed at a time when the conventional wisdom and prevailing technology were that data was "owned" — collected and manipulated — in discrete systems. Such systems are now viewed as "stove-pipes" because the information stored in them cannot be quickly shared or cross-referenced. The FBI has been hamstrung by outdated technology in terms of networks, hardware, software, and infrastructure support.

Information technology requires constant upgrading in order to remain viable and flexible to changing requirements. The FBI hired experts from outside to modernize its systems. The first imperative was to develop an Enterprise Architecture . However, 9/11 created immediate critical needs to prevent further terrorist attacks. Decisions were made and actions taken to meet those exigent needs. As noted by the GAO, there are inherent risks in modernizing information technology systems without the benefit of an Enterprise Architecture. The decisions that were made took into account such risks. The FBI chose to be an early majority technology adopter with a strong bias toward purchase versus development. We selected a few key standards, and in some cases specific mainstream products, to anchor the technology portion of our architecture. Even without a comprehensive architecture, the FBI was still able to achieve enumerable successes as a result of the character and resolve of its personnel. It is imperative that the FBI have the ability to view, conjoin, and analyze data already in its possession in ways and places not previously anticipated. The FBI threat forecast predicts the continued emergence of temporal threats and the need to quickly shift to emerging threats. The FBI must be able to quickly search all in-house data or legally accessible external data, regardless of source or location, for relevant intelligence. Moreover, the FBI will need to ensure that its systems are compatible for sharing information electronically to the widest extent possible to meet the intelligence needs of our partners.

Strategic Objectives

IVB.1 Ensure all current and future information technology plans work towards a harmonized system.

One significant hurdle for all organizations moving from older to newer technology is the recognition that neither developers nor users can completely predict the ways in which the technology will be used in the future. Thus, over time, we have all learned that unanticipated technical and data connections will be needed. Such connections are not only internal to our own organization but external to it as well, as the importance of data and work-sharing rises. In order to be able to meet such requests, all technology must be included within a single, conceptual Enterprise Architecture. GAO and many other governmental entities have recognized the importance of having a single such scheme and all require explanations of how any new technology will fit within an Enterprise Architecture before approving spending or building. An Enterprise Architecture must be developed using recognized industry methodology that will best support the existing information management systems while allowing new development to benefit from the enhanced infrastructure. One of the most important hurdles that must be considered is that the FBI is not operating in a static environment. While a new Enterprise Architecture is being developed, ongoing investigations must remain largely unaffected. The Director and FBI senior executive staff are committed to an Enterprise Architecture and will interact with the Enterprise Architecture team and make decisions based on input and recommendations from the FBI's Network Architect. Lastly, a solid proven methodology will be employed to ensure that all the necessary requirements and concerns are being addressed.

Priority Actions

- Fully staff the Enterprise Architecture Core Team.
- Complete and disseminate an Enterprise Architecture Management Plan that fully addresses external data-sharing and work-sharing.
- Establish a high-level baseline architecture; high-level target architecture; initial Transition Plan and partial products.
- Complete an Information Technology Strategic Plan.
- Create a Business Reference Model, Data and Information Reference Model, Service Component Reference Model, and a Performance Reference Model.

- Establish a system that revises annually the Enterprise Architecture, Strategic Plan, and the Transition Plan.

IVB.2 Make all technology available to employees wherever they work or travel.

The FBI must provide tools that will allow it to take full advantage of surge capabilities and make additional or specialized personnel available wherever they are needed to address threats. This may mean that an employee in Phoenix will be temporarily assigned to work on an issue for Los Angeles or Headquarters, without ever leaving his or her desk. Information technology will be at the forefront of that toolset as employees will need to store the results of their collection efforts; retrieve and correlate from the larger pool of available information; and share the resulting intelligence. In order to implement this vision, all relevant information technology must be potentially accessible and transferable to any employee in any office. The FBI's Trilogy project has begun that process by upgrading to communications facilities, network servers, and desktop workstations that can accommodate the same enhanced technologies. The future challenge is to continue upgrading in order to keep pace with the technical prowess of our adversaries.

Priority Actions

- Complete Trilogy upgrades currently underway.
- Ensure a technology refresh cycle of 36 months for mission-oriented work.
- Establish and implement a plan to make all technology available to any employee at any fixed office location.

IVB.3 Build or adapt data storage and retrieval systems to permit the flexibility to respond to changing threats and priorities.

Newer database and data warehouse technologies separate storage functions from access functions, making it possible for different divisions, sections, or units to place all data in a single virtual repository and get different views of it based upon their needs. Through "extensibility," storage elements can be added later to accommodate new participants or programs. This is not without challenges. Although data need not be stored with the tool that accesses it, access technology still dictates the format it can retrieve and, therefore, the format in which data is stored. In order to work with currently available access technology (and to conform to e-gov standards), significant programming is required to make all of the data compatible. The FBI has undertaken the important effort of converting its data to XML and,

with its partners, to establish metadata standards which will facilitate data sharing. Current data access technology also requires that data be stored according to a data schema that anticipates the desired flexibility; the FBI is working towards this by creating a logical data model and offering to share it with partners. The information technology industry is working to establish mechanisms to access disparate data without these expensive and time consuming processes and it is possible that the breakthrough will come within the next five years. If so, we must be prepared to capitalize on such an advance.

Priority Actions

- Ensure all new data collection occurs in compliance with the metadata standards.
- End "stove-pipe" systems by converting all investigative and intelligence data into formats which can be accessed via a virtually linked storage facility.
- Implement new application software for field investigations and, subsequently, upgrade the software until functionality entirely replaces identified "stove-pipe" systems.
- Revise plans to take advantage of newer, more effective and efficient technologies as they are made available.

IVB.4 Provide tools to increase the speed and efficiency of data use.

Improving the tools for data access is an increasingly critical requirement. Advances in the ability to collect and store text, graphics, audio, and video data have resulted in a tremendous amount of information which outstrips the human ability for processing. Concomitant tools must be used to parse, analyze, and meaningfully report the available data. Many such tools are currently available throughout the FBI, but they need to be provided more consistently. The data tools industry is constantly enhancing its offerings, providing real opportunities to improve the speed and accuracy of obtaining results. These advances will become increasingly important as the FBI, in addressing rapidly developing threats, works to prevent events before they occur rather than solving them after they occur.

Priority Actions

- Ensure all virtually linked data can be accessed by tools which allow for analysis, visualization, and reporting of text, graphics, video, and audio data.

- Consolidate efforts in developing analytical tools and provide this capability across-the-board.
- Revise plans to take advantage of newer, more effective and efficient technologies as they are made available.
- Deliver additional tools which enable investigators and analysts to triage, exploit, and share intelligence and other information collected via electronic means.

IVB.5 Ensure that data is secure.

Data is one of the greatest weapons of our time. Because of its great power, we must ensure that FBI data is secure and available at all times. This is accomplished through both intrusion detection/protection and the creation of a viable continuity of operations plan (COOP) in the event of system disruption. While the FBI gathers and uses data in the fight to reduce the threats against our citizens, it is clear that the very same data can be turned against us as a weapon of immeasurable force. It also has the potential to be used for less disastrous but equally illegal or inappropriate purposes. As the FBI places more data in a single repository and provides more access points and views, it must be increasingly vigilant in ensuring that the data is handled in ways that are consistent with the U.S. Constitution, privacy and record-keeping laws, classification standards, and federal regulations and policies.

Priority Actions

- Ensure that a COOP is in place and updated annually to address changes in environment and technology.
- Ensure that back-up data and processing is available at regional off-site locations.
- Continue to require regular review of all information technology plans to ensure conformity to all legal standards.
- Seek to ensure that both in-house and external punishment measures for willful inappropriate use of data is commensurate with the damage caused.
- Ensure that data security tools and measures have the capacity to identify inappropriate or suspicious access, use, or dissemination.
- Ensure that data security measures keep pace with developments in tools.

C. Investigative Technology

Strategic Goal

Effectively utilize applied science and engineering resources to empower the FBI's investigative and intelligence operations and thwart the techniques of our adversaries.

Situation

In addressing today's terrorists, intelligence operatives, and criminals, computers and electronic media have become the evidentiary equivalent of yesterday's paper files. Moreover, the potential sources of audio, video, and image evidence continue to expand as technologies advance and as adversaries make wider use of them. Video cameras and other audio and imaging technologies, such as solid-state recording devices, voice mail systems, Internet audio, digital cameras, and flatbed scanners, are becoming commonplace throughout the world. The electronic surveillance (ELSUR)[2] of criminals, and of foreign powers and terrorists, has proven to be one of the most effective tools of the U.S. Government. The FBI's emphasis on proactive and preventive counterterrorism, counterintelligence, and cyber activities requires technical collection and analysis activities that adapt from historically simple technology to a more complex systems approach, resulting in the development of new tools and the retraining of investigative, translation, intelligence, and technical personnel. In June 2002, the FBI established the Investigative Technology Division in order to consolidate all responsibilities for technical investigative support and increase the emphasis on future investigative technologies.

Strategic Objectives

IVC.1 Improve the speed of access to and dissemination of information collected through data and telecommunications intercepts.

The FBI must enhance its collective capacity to expeditiously identify, understand, and take appropriate action to counteract crime problems and threats against the United States. In the furtherance of these efforts, the FBI will develop and implement tools that enable investigators and analysts to triage collected data, permitting them to crystallize actionable intelligence obtained from an ocean of collected information.

[2] There are two federal statutory regimens pertaining to electronic surveillance — one regarding criminal investigations and another regarding foreign intelligence, counterintelligence, and terrorism investigations. The former is derived from (1) Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (commonly referred to as "Title III"), as amended; (2) portions of the Electronic Communications Privacy Act of 1986, as amended; and (3) portions of the Communications Assistance for Law Enforcement Act (CALEA), enacted in 1994. The latter is derived from the Foreign Intelligence Surveillance Act of 1978 (FISA), as amended.

In this regard, the Investigative Technology Division has developed and deployed a system to monitor, minimize, exploit and disseminate over the FBI's TRILOGY network the product of lawful ELSUR operations in a collaborative user environment. This initial capacity will be expanded through the development and implementation of an integrated capability that enables FBI users, as well as our partners in the Intelligence Community, to process, view, analyze, and disseminate all digital evidence collected pursuant to a lawfully-authorized seizure or intercept order. Upon implementation, the Electronic Surveillance Data Management System (EDMS) will provide an enterprise web-based collection management and information retrieval capability for all FBI field offices. EDMS will automate the capability to prepare reports, locally conduct investigative analysis, and provide users with analytical tools for automated speaker identification, text key word spotting, voice key word spotting, and language identification.

Priority Actions

- Implement EDMS as means to establish a common user interface that will enable appropriate personnel to have enterprise-wide access to collected data, as well as the capacity to engage in remote collaborative and intelligence sharing activities.
- Research and implement analytic tools which will assist in the prioritization of collected material.
- As authorized by pertinent laws and guidelines, support joint exploitation of collected information by establishing an architecture for sharing collected data, comments, and analysis.

IVC.2 Improve the delivery of existing tools, technologies, and services, and develop and deliver new technologies, tools, and services to investigators and analysts.

Keeping abreast of advancing technologies is critical to empower our employees in their duties and to thwart the technical capabilities of our adversaries. The anticipated growth in the number of Internet users, continued consumer demand for broadband technologies, and the mobility associated with wireless Local Area Networks (LANs) and Third Generation Wireless systems which converge voice communications and Internet access, requires constant vigilance by the FBI. The number of broadband households in the United States is growing at a rate of about 100 percent per year, from 6.2 million in 2000 to an estimated 34.7 million by the end of 2004. This higher bandwidth access increases by about 50 percent the

volume of material looked at and, as a result, the volume of data intercepts and potential evidence also increases.

Changes in cellular technology recently caused the Federal Communications Commission to announce plans to phase out all analog systems within three to five years. Also, the increasing emphasis on digital connectivity and electronic commerce has been a catalyst for the introduction of stronger, more user-friendly data protection (e.g., encryption technology) and destruction systems. While this is beneficial for legitimate users, others have taken advantage of this technology to conceal or destroy evidence. The FBI must expand its efforts to make critical technology leaps by aggressively exploring, developing, and delivering significant new, even "generation-skipping," technologies, operational capabilities, tools, and services. These efforts include, but are not limited to, those pertaining to computer-based evidence; communications; facial recognition; audio, visual, and imaging forensics; tactical operations, and surveillance operations.

Priority Actions

- Increase the level of technical support to investigations involving intercepted electronic information employing data protection.
- Expand capacity to provide field investigators with body recorders; data and communications interception and dissemination equipment; audio sensor systems; and video equipment.
- Meet investigators' demand for physical surveillance/tracking and audio/video/image enhancement tools.
- Enhance investigators' capacity to conduct physical surveillance and tracking operations.
- Improve capabilities to compromise security and countermeasure devices confronted during entry and search operations.

IVC.3 Improve the technical ability of law enforcement to ensure intercept capabilities are consistent with private industry's advances in technology.

Several mandates have been dictated to the FBI by Congress and oversight agencies. These responsibilities include but are not limited to efforts to implement CALEA; and to vacate the microwave band from 1700 MHz to 1755 MHz as required by the Omnibus Budget Reconciliation Act of 1993.

Advances in telecommunication technologies and services have impaired the Law Enforcement Community's ability to conduct fully effective, lawfully authorized electronic surveillance operations. CALEA was enacted to preserve electronic surveillance operations as tools for investigating our nation's most serious and violent offenses. CALEA requires the telecommunications industry to proactively address law enforcement's needs and directs the industry to design, develop, and deploy technical solutions meeting certain assistance capability requirements, including capacity requirements. CALEA authorized appropriations of up to $500 million to reimburse carriers for certain "reasonable costs" in complying with the statute.

Nearly nine years after its enactment, the statute has not yet been fully implemented. The industry has not adopted the development and deployment of electronic surveillance capabilities as a basic element of providing service, and has resisted full implementation of CALEA through multiple litigations, requests for extensions, and other means. By the end of 2004, we expect only 40 percent of law enforcement priority switches to have CALEA technical solutions deployed. The FBI will work with its law enforcement partners at all levels to foster relationships with individual carriers and their respective equipment manufacturers, as well as to expand law enforcement's understanding of technologies and services where industry-setting standards do not exist or industry sectors have to date refused to develop technical standards.

Priority Actions

- Develop strategies to motivate industry to implement CALEA.
- Ensure CALEA implementation team is staffed with technically trained agents familiar with operational requirements as well as technical requirements.

IVC.4 Improve radio communications within the FBI.

The FBI has had its own dedicated tactical wireless system, the Land Mobile Radio System (LMRS), since the 1940s. Beginning in 1999, sufficient funding has not been available for maintenance or upgrades, and the system has begun to deteriorate. Some of that equipment is so dated that replacement parts are no longer available. Concurrently, the proliferation of wireless technologies has created unprecedented demand for radio spectrum which is a finite natural resource. The Congressionally-mandated narrowband communication initiative requires legacy radio equipment to be replaced with equipment using the narrowband by 2005. In this regard, the FBI must replace more than 32,000 radios, both portable and mobile. The new compliant

systems will be more technically advanced, and will offer a multitude of enhanced technical and security capabilities. An aggressive training initiative will be needed to ensure the viability of the new systems. The migration to "narrowband" is being accomplished through the joint Department of Justice — Treasury Department — Department of Homeland Security Integrated Wireless Network. Until that system is fully implemented and operational, the FBI will be required to concurrently purchase and maintain equipment for the LMRS system that is migratable to the narrowband.

Priority Actions

- Ensure the complete and timely implementation of the Integrated Wireless Network and continue to maintain the legacy LMRS in the interim.
- Provide increased level of guidance regarding the development, procurement, and installation of a secure wireless communication system.

D. Criminal Justice Information Services

Strategic Goal

Provide timely and relevant criminal justice services to the FBI and to authorized law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

Situation

The CJIS Division was established to provide nationwide criminal justice information services. To meet expected increases in future demand due to programs such as civil fingerprint-based background checks for employment and licensing, and border entry activities to detect terrorists attempting to enter the United States, CJIS needs to significantly increase its systems' capacity. Future fingerprint requirements are pushing towards immediate, instantaneous responses. Additionally, law enforcement's daily NCIC transactions have significantly increased. These and other increasing demands call for the "next generation" of CJIS systems.

Automation and computer technology necessarily require constant upgrading and enhancement if such systems are to remain viable and flexible in response to changing customer requirements. As a general rule, computer capabilities double in performance every two years. Software companies constantly upgrade and enhance their software to accommodate the improved hardware. At some point, early technology versions will not work with newer hardware or software. This will result in an expensive retooling of the entire system. Inevitably, if a computer system is to remain viable, reliable, and able to meet growing customer demands, technology systems must continually upgrade.

Improving technology will also include expanding Internet usage. The transmission over the Internet of fingerprint images, Criminal History Reports (CHRs), crime statistics, gun checks, etc., provides all agencies the ability to benefit from information sharing at a lower cost than a dedicated Wide Area Network (WAN). This is an area that the CJIS Division will explore for future use.

The Law Enforcement OnLine (LEO) system has tremendous potential to meet law enforcement's growing requirements for Internet connectivity and information sharing. While LEO has been able to operate and provide an acceptable level of service, it will need to be enhanced to meet future demands.

A critical external issue that negatively impacts the CJIS is CHR accuracy. Half of the CHRs do not have a final disposition (e.g., conviction or dismissal). This

impacts the quality of information provided through the fingerprint identification, NCIC, and National Instant Criminal Background Check System (NICS) services. In the case of NICS, it consumes significant resources to retrieve dispositions in order to provide gun dealers information on an individual's qualification to purchase a gun.

In addition to the expansion of its existing services, CJIS is embarking on a major new endeavor relating to information sharing between different FBI, law enforcement, and civilian databases and information services in a manner that provides richer and more relevant information to its customers. When developed, the system will provide the ability for a single query to profile all of an individual's contacts with law enforcement. By tracking crime in real time and presenting it in a graphic representation, law enforcement can improve its analysis of criminal and terrorist activities and discern connections that previously would have been impossible.

Strategic Objectives

IVD.1 Expand information sharing capabilities to support customer needs.

An array of state-of-the-art technology in the Uniform Crime Report (UCR) Program is needed to provide more efficient, optimum quality, and timely products and services to law enforcement and other consumers of UCR crime data. The new system will optimize the production capabilities of the existing CJIS information systems by leveraging the immense amount of data already regularly contained in each system repository. It will deliver an efficient, automatic correlation of all CJIS data. Once achieved, law enforcement and national security stakeholders will have the ability to run data against other information residing on the various agency-based systems, so that the optimum level of correlations between current and past criminal and homeland security matters can be accomplished without the need for labor intensive, human intervention. The requestor would not only receive specific information based upon regular, electronic queries, but would also gain knowledge about any other law enforcement entity's actions, past or present, which has commonality with the requestor's current subject.

Priority Actions

- Conduct a pilot program of the Concept of Operations.
- Develop an implementation plan based on the results of the assessment of the pilot project.

IVD.2 Expand the National Incident-Based Reporting System (NIBRS) data fields for distribution to law enforcement and others throughout the United States.

The System of Services Information Sharing Initiative requires participants to utilize an "enhanced NIBRS" data set for the data input to support the information sharing process. This enhanced data set combines the current 53 NIBRS crime descriptors with the specific personal and event identifiers which form the core of most police department incident reports. Many states collect more information than the current 53 NIBRS data elements describing incidents for their own in-house purposes. To realize the full potential of the information sharing capabilities of NIBRS data, additional identifying data (e.g., victim, offender, and suspect) must be included, which will provide law enforcement additional investigative leads. This information will serve as a valuable tool in criminal and national security matters.

Priority Actions

- Closely coordinate with state, local, and federal NIBRS stakeholders in the development of an implementation plan.

IVD.3 Improve the availability of dispositions and other information used to evaluate individuals for firearm and other civil background checks.

Because of the lack of availability of dispositions, the FBI and the states cannot always complete the necessary firearm background checks within the legally mandated three business days. In order to improve this performance gap, the NICS Section will work to increase information sharing with state and federal agencies. This not only benefits NICS, but should also impact the overall disposition problem.

Priority Actions

- Initiate an Outreach Program to increase information availability from state and federal agencies.
- Develop and automate the Disposition Document File and any restoration of rights files submitted to the NICS Section.
- Increase Protection Order records, Felony Flags, and Brady Indicators.

IVD.4 Develop, implement, and promote the Next Generation IAFIS for fingerprint identification and criminal history information services.

If CJIS is to meet growing customer requirements, it must develop, implement, and promote the Next Generation IAFIS for fingerprint identification and criminal history services. Significant improvements in the availability and timeliness of services are required in order to share valuable criminal history information with an ever-increasing customer base in an expeditious manner. IAFIS currently provides a two-hour or less response time on electronic criminal submissions and a 24-hour or less response time on electronic civil submissions. However, customer requirements for fingerprint identification services are changing at a rapid pace. CJIS must maintain a state-of-the-art Automated Fingerprint Identificcation System technology to keep pace with the ever-increasing demands of the Law Enforcement Community, as well as the civil community. CJIS must improve and expand its ability to receive flat, ten-print fingerprint data for identification and latent purposes, as well as its ability to extract fingerprint data for export to the Department of Homeland Security for the United States Visitor and Immigrant Status Indication Technology (US VISIT) Program. For many customers, a fully electronic fingerprint process from the customer to the FBI and back has not yet been achieved. Enhanced fingerprint capabilities are also sought by the Terrorist Threat Integration Center and the Terrorism Screening Center.

Priority Actions

- Assess the status of IAFIS customers by state, federal, and regulatory agencies where appropriate. Identify customer requirements for Next Generation IAFIS.
- Implement phased testing of Next Generation IAFIS.
- Determine the feasibility of implementing a national, rapid, and positive fingerprint-based identification background check system for authorized noncriminal justice purposes.
- Complete the National Fingerprint Applicant Check System testing and field work.
- Provide IAFIS data to support the US VISIT Program.

IVD.5 Expand the availability of CJIS services using the Internet.

The Internet provides a valuable tool for exchanging fingerprint identification, criminal history, and other relevant information by improving CJIS's ability to interact with its customer base. The Internet allows CJIS to: (1) exchange data among local law enforcement agencies, courts, and other entities; (2) increase the number of dispositions on file within the CHR repository, which will enable law enforcement and regulatory agencies to make better, more timely decisions regarding issues such as employment, firearm purchases, and criminal activity; and (3) offer training at the convenience of our customers with information in real time.

Priority Actions

- Develop a strategy to use the Internet to enhance and promote fingerprint identification and CHR services.
- Initiate a feasibility study for the transmission of CHR updates via the Internet (i.e., disposition information, expungement information).
- Implement training initiatives via the Internet.

IVD.6 Expand the content and services available on LEO.

LEO's objective is to use the Internet to provide the Law Enforcement Community with an expandable, reliable Sensitive But Unclassified service for sharing information, communicating alerts, and educational purposes. Unfortunately, there are still state, local, and federal first responders without LEO's critical support services. As LEO implements its initiatives and transitions them to an operational status, improvements and enhancements will be needed. LEO will provide an Enterprise Domain for connectivity between users throughout various agencies. This expansion includes Continuity of Operations, thus, increasing LEO's reliability and availability for all users. In order to achieve these activities; however, upgrades in hardware, software, business processes, and features are needed to enhance and improve the services.

Priority Actions

- Expand LEO's services with additional antiterrorism and law enforcement features.
- Develop a management plan and supporting documentation consistent with FBI/DOJ/Office of Management and Budget approval and direction.

IVD.7 Develop and Implement a Business Continuity Plan for CJIS.

A Business Continuity Management process improves procedures and practices and increases the organization's resilience in the event of interruption or loss. It will ensure that CJIS's services will be available (proaction), and if an incident occurs, CJIS can minimize the impact to the customer (reaction). There are two aspects to this goal: the technology and the staff. The effort to protect the technology requires a significant amount of resources and planning, particularly in the case of a catastrophic event. Even a seemingly insignificant event, such as a short-term but substantial snowstorm, can impact the available staff to service customers.

Priority Actions

- Implement a Disaster Recovery System that provides business continuity for the CJIS Division's critical services.
- Develop a comprehensive contingency plan.

E. Forensics

Strategic Goal
Establish a worldwide network of scientific services that maximizes forensics in combating terrorism, cyber-based attacks, and crime.

Situation
The proper collection, preservation, and forensic analysis of evidence is a tremendous tool that must be fully exploited. Since its inception, the FBI has been the world leader in using science to solve crimes. During its first year of operation in 1932, the FBI's forensics unit conducted 963 examinations. Currently, the FBI conducts more than one million forensic examinations annually. The types of investigations addressed forensically by the FBI include terrorism, espionage, public corruption, civil rights, criminal organizations and enterprises, white collar, and violent crime. Not only has the volume of evidence received increased dramatically, but the complexity of the examination methods, as well as the complex nature of the investigations themselves have increased. Often, forensic analysis is the only means to provide conclusive information to a jury to assist them in their determination of guilt or innocence.

Forensics is also an essential tool in combating terrorism in that it provides evidence that establishes links and associations that can withstand judicial scrutiny in the United States and abroad. Moreover, comprehensive crime scene searches and the subsequent forensic analysis of evidence is sometimes the only solid intelligence that exists or the only mechanism to corroborate other intelligence reporting. FBI forensic analysis was essential in piecing together the evidence to identify those responsible for, as well as the supporters of, every terrorist attack against the United States, including the mid-air bombing of Pan Am Flight #103, the bombing of the World Trade Center in 1993, the bombing of the Oklahoma City Federal Building in 1995, the bombing of the two United States Embassies in East Africa, the attack against the U.S.S. Cole, and the 9/11 attacks on the World Trade Center and the Pentagon.

In January 2003, the American Society of Crime Laboratory Directors — Laboratory Accreditation Board (ASCLD/LAB) board of delegates voted to adopt Digital Evidence as an accreditable discipline. The Investigative Technology Division conducts forensic examinations in the discipline of Digital Evidence as defined by the ASCLD/LAB. These examinations are performed at FBI Headquarters and field offices by certified forensic examiners.

The evolving threat environment increasingly requires the rapid deployment of FBI forensic examiners to locations around the world in order to collect and preserve evidence that could otherwise be lost forever. FBI forensic resources are increasingly being called upon to support high profile criminal investigations in other countries because of the FBI's unique forensic expertise and capability. The FBI will also need to help develop the forensic capabilities of other countries and to leverage existing capabilities within the United States through partnerships with other forensic laboratories and scientists to provide the optimum level of forensic services to meet the increasing demands. It is imperative that constant improvements in forensic analysis be sought through a robust research and development program and that these improvements be quickly deployed to support the entire forensic community.

With the exponential growth of the World Wide Web, terrorists, foreign actors, and criminals are increasingly using this technology, along with encryption, to facilitate their operations. The FBI and its partners must keep up with the increasing demands required in providing timely forensic analysis of computer-related evidence in support of terrorism, foreign intelligence, cyber, and criminal investigations.

Strategic Objectives

IVE.1 Increase the FBI's ability to provide forensic analysis in support of its own investigations as well as those of other agencies.

The FBI receives an increasing volume of evidence and an increasing number of requests for expert testimony from federal, state, and local law enforcement agencies. It is incumbent upon the FBI to provide operational assistance to international, federal, state, and local agency partners. While the completion of the new FBI Laboratory provides tremendous forensic capability to assist in these matters, increasing demands over the next five years will outpace the FBI's ability to deliver timely examinations.

Priority Actions

- Complete a comprehensive assessment of the FBI's future forensic resource needs.
- Expand the use of information technology in the conduct of examinations, comparisons, and the sharing of results, as part of the FBI's information technology modernization efforts.

- Expand the forensic capabilities of the Investigative Technology Division's Computer Analysis Response Team (CART) Program and its ability to quickly share the results of computer forensic exams.

- Continue to develop the Combined DNA Index System (CODIS) as a means to assist in the identification and capture of international terrorists.

IVE.2 Increase the FBI's forensic response capabilities.

The proper collection, preservation, and forensic analysis of evidence from the scene of a terrorist attack or major crime is critically important. There is only one opportunity to do it correctly; otherwise, critical links and evidence may be lost forever. The global threat of terrorism and international crime requires a timely forensic response capability around the world. The need for these services will increase over the next five years, and the FBI must be able to meet this demand. While the most dramatic increase of services will be overseas, the FBI's forensic expertise is often called upon to address major crimes in the United States as well, including initial processing of crime scenes.

Within the first six weeks after 9/11, the FBI's CART examined more than nine terabytes (nine million megabytes) of data. With the onset of world-wide access to computers and increased knowledge within the general population, it is reasonable to expect a computer to be involved in some fashion in virtually every investigation the FBI conducts. Furthermore, the FBI is Congressionally mandated to provide computer forensic support, in addition to other forensic support, to state and local law enforcement agencies which it accomplishes through its Regional Computer Forensic Laboratory (RCFL) Program. The RCFLs are partnerships among the FBI and other law enforcement agencies within a geographic area, and the program has continued to grow since its inception with the number of labs expected to exceed 10 by the end of 2004. As such, computer forensics are expected to play an ever-increasing role in the FBI's future operations.

Priority Actions

- Increase the number of employees participating in the FBI's Evidence Response Team Program in support of international and domestic crime scene searches.

- Establish specialized Rapid Deployment Teams to conduct expeditious examinations of both computer-related and other physical evidence in support of investigations and intelligence operations.

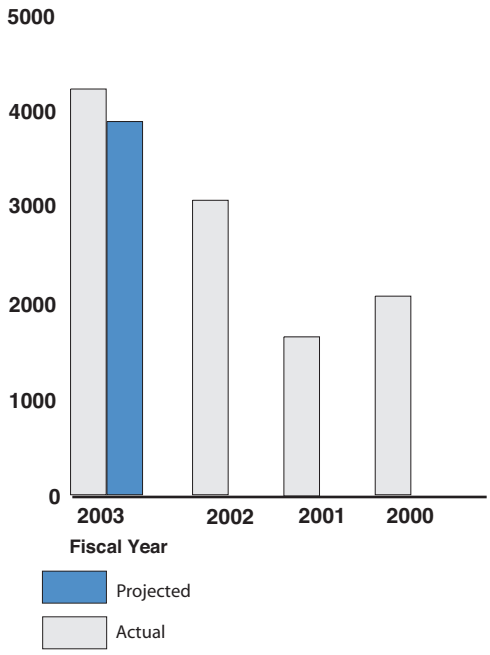
- Expand the CART Program's forensic capabilities and the ability for case investigators to review examination results.

- Develop, plan, and schedule for basic and advanced hazardous materials training to bring on line 10 additional field Hazardous Materials Response Teams and enhance the existing capabilities.

IVE.3 Increase the forensic capabilities of all law enforcement and intelligence agencies both within and outside of the United States.

FBI forensic resources are increasingly being called upon to support high profile criminal investigations in other countries because of the FBI's unique forensic expertise and capability. The FBI will need to help develop the forensic capabilities of other countries and leverage existing capabilities within the United States. This will be accomplished through partnerships with other forensic laboratories and scientists to provide the optimum level of forensic services to meet increasing demands worldwide.

Measure Refined: Total Number of Forensic and Offender Matches Identified at the NDIS, SDIS, and LDIS

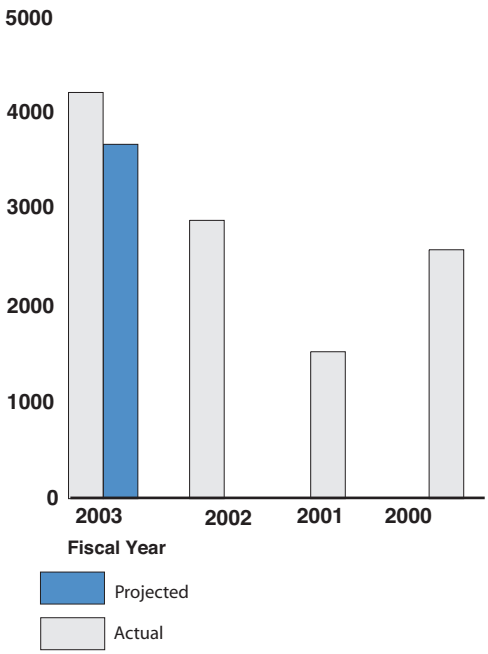


Data Definitions: NDIS, SDIS, & LDIS Matches: NDIS, SDIS, or LDIS finds a DNA match, CODIS software geerates a report that shows a match and/or "hit" has been made and then provides an offender or forensic profile based on the sample received.

Priority Actions

- Continue to provide training and certification to the FBI's state, local, and international forensic partners.
- Upgrade proficiency testing through the use of externally prepared tests.
- Expand the CODIS Program both domestically and internationally, via the Legats. Improve training and information for all CODIS users.
- Work with other federal crime laboratories to develop a Continuity of Operations Plan.

Total Number of Federal, State and Local Investigations Aided By the Combined DNA Index System (CODIS)



IVE.4 Increase forensic research and development projects.

The FBI will be able to accomplish its mission and support its priorities not only through the collection and examination of evidence, but also through continual state-of-the-art forensic science research, as well as training counterparts throughout the professional community. It is imperative that constant improvements in forensic analysis be sought through a robust research and development program and that these improvements can be quickly deployed to support the entire forensic community.

Priority Actions

- Establish joint partnerships with state and local laboratories for research and development.
- Work with the National Academy of Sciences regarding a review of bullet lead analysis.

F. Records Management

Strategic Goal
Establish a state-of-the-art record keeping system.

Situation
The FBI system of records must ensure that accurate records of all activities are created, maintained, and disposed of in accordance with all legal requirements. The system must provide timely and accurate responses to requests for information from government agencies that need FBI information to perform their mission. The system must also be responsive to requests for information under the provisions of the Freedom of Information and Privacy Acts (FOIPA). Currently the FBI has several electronic record keeping systems, but none have been approved by the National Archives and Records Administration (NARA) as a system of records. Only the paper-based, physical file has been approved as a system of records, and hence, the FBI must maintain tens of millions of paper files. This paper-based system is costly and inefficient. The FBI is modernizing its information technology systems, and a fundamental requirement is an electronic record keeping capability with unquestionable accuracy and integrity including the use of digital signatures.

Strategic Objectives

IVF.1 Establish an electronic record keeping system.

The FBI collects and produces a tremendous number of documents while performing its mission, most of which constitute official records. Dramatic efficiencies can be achieved if the FBI adopts an electronic record keeping system. The FBI's official system of records is currently paper-based and decentralized, and is maintained at 265 different locations, including FBI Headquarters, field offices, resident agencies, some Legal Attaché offices, Investigative Technology Centers, and various off-site locations. Advances in information technology provide an opportunity to dramatically improve the efficiency of this system of records, which is so critical to operational and administrative functions. A principal goal of our modernization efforts is the adoption of a Records Management Application that supports an electronic record keeping system for all legacy and future information technology systems.

Priority Actions

- Centralize all FBI records.

- Acquire and implement a Records Management Application that can address the record keeping requirements for all FBI legacy systems and the FBI's future information technology systems.

- Closely collaborate with NARA to ensure the electronic record keeping and automated record management applications meet all requirements for an electronic record keeping system.

IVF.2 Modernize the FBI's National Name Check Program.

The National Name Check Program is the FBI's system to provide information on individuals from FBI records to other federal agencies, congressional committees, intelligence agencies and other agencies that need this information to support their mission. The program historically conducted an average of 2.4 million name checks annually; however, an increased emphasis on homeland security has resulted in an exponential increase in requests. It is anticipated that the number of requests will continue to increase over the next five years at a rapid rate. Hence, the FBI must achieve dramatic improvements in the National Name Check Program to meet customer demands. This can only be achieved through information technology and improved processes.

Priority Actions

- Increase coordination with customer agencies to fully automate the process.

- As part of the FBI's information technology modernization efforts, upgrade the name check application to increase accuracy and speed.

IVF.3 Improve the processing and quality of FBI responses to FOIPA requests.

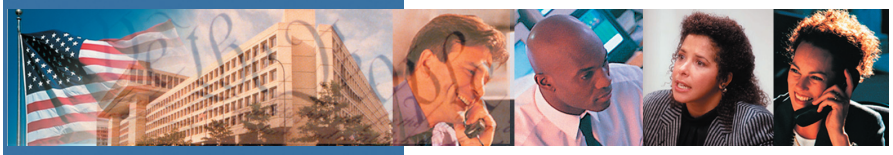
The FBI has made several process improvements to address the increasing public demand for FBI information. However, dramatic improvements can only be achieved through modernization of the FBI's information technology systems.

Priority Actions

- Develop a paperless FOIPA process including an Internet-based request and response capability.

- Ensure FOIPA processes are fully addressed in the FBI's future electronic record keeping system.

Appendix A



EXTERNAL and INTERNAL FACTORS:

FROM DRIVERS TO OPERATIONAL IMPACTS

Given the scope of its investigative and intelligence responsibilities, the FBI is subject to numerous influences, both external and internal, that affect its ability to achieve the goals and objectives laid out in the Strategic Plan. This section describes the seven most important factors, or global "drivers," that can alter the threat environment, affect forecasting, and interfere with the FBI's ability to meet its goals and objectives. This section also describes the potential impact of those drivers on FBI programs and processes, and provides actions the FBI can take to reduce or ameliorate their impact.

APPENDIX A FROM DRIVERS to OPERATIONAL IMPACTS

Underlying Global Driver	Results	Possible Shocks	Implications for United States National Security	Operational Impacts for FBI	Org'l and Recruiting Consequences
Global demographic changes	90 percent of population growth in developing countries Aging populations in richer countries Declining population in Russia, South Africa, Japan, other countries Increasing urbanization	Pandemic affecting particular regions or much of globe Less dramatic shocks would hollow out United States partners	Legal and illegal streams of immigrants to United States cover potential terrorists or criminals Rise in xenophobic rightwing groups Immigrants engage United States in politics and conflicts back home Age distributions create "youth bulges" in Africa and Middle East, including Saudi Arabia Refugee streams create instability in poorer recipient countries	Need to penetrate immigrant communities Further dispersion of targets More operations abroad Need for non-"terrorism"-associated agents to respond	Enhanced need for recruiting among immigrants More need for a wider variety of linguists
In particular for United States	Aging plus immigration produces "dumb-bell" age distribution		Increase in crime Easier for terrorists and criminals to hide in urban areas Non-English speaking criminals make investigations more difficult	Rapid turn-over creates opportunity to reshape FBI culture But also reduces corporate memory More criminal targets as well	

Underlying Global Driver	Results	Possible Shocks	Implications for United States National Security	Operational Impacts for FBI	Org'l and Recruiting Consequences
Communi-cations revolution	Universal wireless connectivity Uneven across globe, some countries left out Microsoft "monoculture" dominates Packet-switched communications dominate Increasingly "digital" western society	Major outbreak of disease would disrupt communications Attacks, other shocks could bring down parts of networks	Terrorists, militias, criminals communicate with ease Encryption ubiquitous if not infallible Operations very difficult in "unconnected" countries given dependence on commercial networks Many-to-one, many-to-many communications reinforce communities, from militias to pedophiles Increasing dependence on COTS and public networks (e.g., VPNs over public networks) Data flows means information on Americans available "abroad"	Increased efficiency of operations Constrains FISA operations – need to enter or get close to end-nodes in the Net Easier FBI peer-to-peer communications; supervisory agents have less opportunity for oversight Pervasive media makes reaching out to the public, e.g., to identify criminals, more possible Identity theft makes it harder to identify people, including perpetrators Intercepts are primarily on packet-switched or wireless networks Conduct Operation Continuity Planning for FBI digital networks, to include options for total network failure	Increased need for technical expertise throughout organization requires change in culture

APPENDIX A FROM DRIVERS to OPERATIONAL IMPACTS

Underlying Global Driver	Results	Possible Shocks	Implications for United States National Security	Operational Impacts for FBI	Org'l and Recruiting Consequences
Global economic changes	Distance, weight continue to matter less and less in international commerce Prospects for global prosperity good Asia biggest winner But uneven across countries and within them Increased speed, ease of transnational financial flows Energy resources underscore importance of Persian Gulf, Russia, Caspian region, coastal Africa, for instance	Major oil crisis Japan, Europe falter on labor shortages China and/or India falter on economic restructuring Debt crisis among LDCs	With demographics, unemployed "youth bulges" of males offer recruits for terrorism Population growth plus economic failure risks "failed states" as humanitarian problems and terrorist havens "Bads" – weapons, including WMD, drugs – move as easily as goods Global economy, plus thick migration abet organized crime Easier for criminal and terrorist groups to transfer currency globally	Terrorism and organized crime converge More operations abroad, more need to train for foreign operations Outsourcing abroad raises questions about security of information technology Greater need to coordinate countermeasures with other countries, international financial organizations	Need for close cooperation between CTD and CID
In particular, for United States	Widening cleavages between "red" and "blue" states With outsourcing, United States becomes dependent, loses know-how in crucial areas	Sustained downturn in United States economy Rising budget deficits lead to downward pressure on budgets	Gaps plus communication abet rise of radical groups		Continuing difficulty recruiting highly-paid technical and other talent

APPENDIX A FROM DRIVERS to OPERATIONAL IMPACTS

Underlying Global Driver	Results	Possible Shocks	Implications for United States National Security	Operational Impacts for FBI	Org'l and Recruiting Consequences
Rising belief in non-material – religion, tribe, ethnicity – "us" vs. "them"	Also fuels pool of potential terrorists Rise of new radicals from cults, to "new left" to anti-globalization forces Reaction to dominance of global culture identified as "American"	Fundamentalists take-over in major state, like Saudi Arabia	Feeds terrorism and state failure United States focus of hatred in much of the world, especially Muslim world Increased pressure on Muslim allies not to cooperate	Continued dispersion of targets Need to work abroad, but increasing danger to agents abroad	
In particular, for the United States	New cults, militias at home Increased divisions in United States including intensified partisanship	Divisions and discontents in United States much greater than expected More links between militias and "legitimate" society Militias "used" by more capable foes like Al Qaeda	Ethnic-based crime on the increase – for instance, staged accidents Crime embedded in culture that does not see it as "criminal" Increased ethnic and geographic basis for drug use, e.g. Meth in rural areas	Harder to penetrate many ethnic groups, especially new ones Issues of reliability within a much more varied workforce FBI actions perhaps focal-point in global battle to try to rein in "rogue" superpower	Increasing difficulty recruiting Arabs and other Muslims, also at home

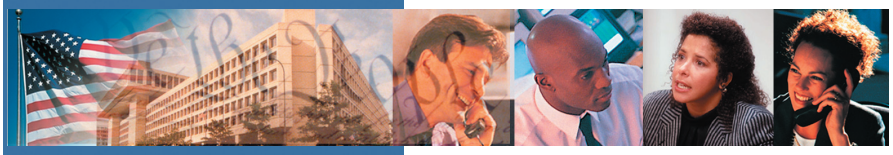
APPENDIX A FROM DRIVERS to OPERATIONAL IMPACTS

Underlying Global Driver	Results	Possible Shocks	Implications for United States National Security	Operational Impacts for FBI	Org'l and Recruiting Consequences
New revolutions in technology	Biotechnology permits genomic profiling, biomedical engineering, genetic modification Materials technology permits customized, "smart," sensor-rich products Nanotechnology changes the way everything is designed and made High-tech dominance of United States corporations Biotech, especially, will provide opportunities for the rich, and so be divisive across and within societies	Major accidents delay technology around the world Biotech becomes a source of conflict with United States allies Dramatic new lethalities emerge United States turns out to be not such a clear leader in some technol's	Proliferation of weapons, including mass destruction, easier Possible new "weapons" from biotechnology, other sciences Widening technological gap between United States and rest of world Potential to enumerate and uniquely identify individuals in a society	DNA, blood, genetic analysis advanced New sensors aid tracking bad items and people, but deception also facilitated "Tagging" property or items also permits targeting of agents Agents and informants abroad denied the use of multiple identities Increase in espionage and cyber crimes directed against United States corporations Improved sensors and new testing raises civil liberties concerns	Again, need to recruit and raise stature of technical talent throughout organization
Revolution in security technology and practice	Network manages precision strikes from afar, linked to an array of sensors Soldiers as sensors as much as shooters United States in class by itself Sensors and procedures for policing and contingency operations improve but more slowly	Major potential opponent leapfrogs United States, in concepts of operation if not technology Conspicuous United States vulnerability appears	Would-be United States foes driven to asymmetric attacks, seeking vulnerabilities, including at home Limited foreign capabilities limit number and depth of United States partnerships Perception of "hemorrhaging" in contingency operations leaves administration vulnerable in public opinion	Again, increased operations abroad, especially in "policing" operations Rise in espionage against United States government and defense contractors Need to be able to operate after attack against the FBI (including WMD), especially HQ Risk of political pressure for solutions quicker than technology will permit	

APPENDIX A FROM DRIVERS to OPERATIONAL IMPACTS

Underlying Global Driver	Results	Possible Shocks	Implications for United States National Security	Operational Impacts for FBI	Org'l and Recruiting Consequences
Changing role of state and law	Global economy, technology empower non-state actors, from terrorists, to corporations, to NGOs Role of state, including United States, becomes that of coalition-builder International law continues to shift from states as subjects to people	Continued dramatic terrorism creates new national security state Ungoverned, "gray areas" of globe increase dramatically Possible efforts, esp. religiously motivated, to end-run United States law	With technology, asymmetric threats, including WMD More and more states cannot police selves United States intervention, even armed, more acceptable, hence more likely But as "rights" of individuals extended, international scrutiny of United States actions increases	Need to cooperate with a wide variety of states and non-states FBI perhaps subject of special scrutiny, abroad and at home	Need for forms of cooperation beyond cases and task forces Need to rethink security procedures in dealing with many more "outsiders"

Appendix B



STAKEHOLDERS

While many organizations solicit input from stakeholders on an annual or semi-annual basis for updating their strategic plans, the FBI has incorporated its stakeholders into the day-to-day business of accomplishing its mission. Federal, State, local, foreign, and private sector stakeholders are a critical piece of the Bureau's strategy for transformation and their daily input is used to inform, guide and direct FBI activities. Across every FBI program, we recognize that a prerequisite for any operational coordination is the full and free exchange of information. Without procedures and mechanisms that allow information sharing on a regular and timely basis, we and our partners cannot expect to align our operational efforts to best accomplish our shared mission. Accordingly, we have taken steps to establish unified FBI-wide policies for sharing information and intelligence. Listed below are some of our key stakeholder initiatives:

Congress

Our relationship with Congress, and particularly with the eight primary Senate and House committees that oversee FBI funding and operations (Senate and House Judiciary, Intelligence, Appropriations, and Governmental Affairs/Government Reform Committees), is a key component of our revitalized efforts to solicit input from stakeholders. A constructive dialogue with Congressional committees and individual members of Congress is critical to achieving Director Mueller's vision of a transformed FBI, one that learns the lessons of 9/11 and is more focused on managing intelligence and fighting terrorism. The Bureau takes seriously, for example, its responsibility to keep members of Congress informed about FBI budgets, program accomplishments, and reform efforts, and to respond to their oversight inquiries, requests for documents, and constituent matters. Although these liaison and information sharing efforts have existed for decades, the FBI is more proactive in its outreach than ever before.

Since 9/11, FBI officials have testified at 112 Congressional hearings and provided 831 briefings to members of Congress and their staff. In addition, the FBI has responded to over 5,500 pieces of correspondence from Members of Congress. Our Office of Congressional Affairs has more

than tripled in size and is actively engaged in efforts to foster information sharing, including delivery of intelligence products to the Senate and House Intelligence Committees; delivery of our weekly Law Enforcement Bulletin to the oversight committees and Congressional leaders; tours of FBI facilities (Quantico, Engineering Research Facility, CJIS, etc.) as well as field office visits; and courtesy visits between Director Mueller and key lawmakers. We are also encouraging the Special Agents in Charge of field offices to engage Members of Congress on matters of local interest, with a recent focus on the accomplishments of our Joint Terrorism Task Forces (JTTFs) and improved information sharing with state and local law enforcement.

State and Municipal Law Enforcement

We have taken many steps to continue to improve our relationships with the approximately 750,000 men and women of state and municipal police departments around the country. This critical improvement is the direct result of new and expanded collaborative efforts, innovative approaches to information sharing, new policies and technologies, and above all a commitment to support our partners in law enforcement. We have worked closely with our partners as we developed and implemented these changes, seeking input and feedback each step of the way. This coordination is reflected in the following areas:

Task Forces

The FBI has long relied on strong operational relationships with state and municipal law enforcement. We work in partnership on a wide range of task forces, including JTTFs, Counterintelligence Task Forces, Field Intelligence Groups, Safe Streets Task Forces (that fight violent street gangs), Crimes Against Children Task Forces, Financial Institution Fraud and Identity Theft Task Forces, Health Care Fraud Task Forces, Organized Crime Drug Enforcement Task Forces (OCDETF), Major Theft Task Forces, Safe Trails Task Forces (that fight violent crime in Indian Country), and case-specific task forces related to serial murders, hate crimes, and other types of criminal behavior. FBI personnel on these task forces work side-by-side with their local counterparts to prevent acts of terrorism, solve crimes, and improve the level of safety and security in their communities.

Office of Law Enforcement Coordination (OLEC)

Director Mueller established the OLEC shortly after 9/11 to strengthen relationships between the FBI and its federal, state and local law enforcement

partners. The OLEC works closely with law enforcement groups such as the International Association of Chiefs of Police and the Fraternal Order of Police, providing a voice for these groups within the Bureau and giving them a place at the decision-making table when law enforcement and prevention strategies are being developed.

We selected a former Chief of Police to be Assistant Director in charge of OLEC and located him in an office near the Director. The Assistant Director has decades of experience in law enforcement and has earned a reputation for building bridges within the criminal justice community. He has initiated a number of initiatives to enhance coordination through his office, including:

a. Director's Law Enforcement Advisory Group – This advisory group is comprised of the heads of national law enforcement organizations and meets regularly with senior FBI executives to provide input on various issues of common concern. Issues discussed at recent meetings include: (1) the issuance of Homeland Security "alerts" and the impact on state and local agencies when threat advisory levels are raised; (2) the FBI's investigative priorities; (3) state and local law enforcement counterterrorism needs; (4) ways to enhance communication within law enforcement; and (5) recommended improvements to the training at the National Academy.

b. FBI Police Executive Fellowship Program – In 2002, OLEC established a fellowship program to give high-ranking state and local law enforcement managers an opportunity to spend six months working in an FBI Headquarters program such as the National JTTF or the Office of Intelligence. The four officers who have participated to date have brought vital law enforcement perspectives to Headquarters and have made important contributions to our information and intelligence sharing efforts.

c. Community Oriented Policing Training – OLEC has worked closely with the Training and Development Division to revise the curriculum for new agent trainees by incorporating Community Oriented Policing concepts. New agent trainees learn that a high level of involvement with the community is expected and required if they are to succeed in their jobs.

d. Terrorism Quick Reference Card – This small but practical guide is designed to fit into the overhead visor of police vehicles and lists suspicious factors that may indicate ongoing terrorist activity. To date, 430,000 cards have been distributed to state and municipal law enforcement officers.

Terrorist Screening Center

On September 16, 2003, the President directed the Attorney General, Secretary of Homeland Security, Secretary of State, and Director of Central Intelligence to develop the Terrorist Screening Center to consolidate information from terrorist watch lists and provide 24-hour, seven-days-a-week operational support for law enforcement, consular officers, and other officials. The FBI was directed to lead this effort and begin operations by December 1, 2003. Thanks to significant contributions by all participating agencies, operations began – and continue - on schedule.

Law Enforcement Online (LEO)

LEO is a real-time, interactive computer communications and information service – an Internet for the law enforcement, criminal justice, and public safety communities. LEO has been expanded significantly since 9/11 to facilitate information sharing with state and municipal law enforcement and other first responders.

Alert Notification System

In June 2003, we launched a new Alert Notification System to notify police chiefs or local command centers of alerts, threats, or other critical information. The system allows the FBI to send messages that pop up on computers – like instant messaging, but in a secure environment – and to send notifications to designated cell phones and pagers. Messages can be selectively sent to specific groups (as dictated by geography or function) or broadcast to all possible recipients. Messages can include text, photos, and maps.

Intelligence Bulletins

Since 9/11, the Counterterrorism Division has issued over 100 Intelligence Bulletins to state and municipal law enforcement agencies. These weekly reports share information from all sources that may aid the recipients in preparing for or responding to security threats in their areas. The information is intended for use by patrol officers and other law enforcement personnel who may encounter situations or information through their direct contact with the general public.

Information Sharing Pilot Projects

Ongoing pilot projects are helping us test new concepts for improving information sharing and coordination with our state and local partners

around the country. These include: a) a new counterrorism database that stores documented instances of suspicious behavior by individuals in one region of the country; and b) a new information management tool known as the Law Enforcement National Data Exchange (N-DEx), which will allow investigators to make the most of data in existing repositories and examine relationships among numerous criminal incidents.

New Counterterrorism Training Initiatives

After 9/11, we recognized the need to train not only our own employees, but also our state and municipal law enforcement partners to meet the challenge of international terrorism. Several new or updated training efforts are helping us share counterterrorism expertise and knowledge about terrorist activities.

a. State and Local Anti-Terrorism Training (SLATT) – SLATT is a new training initiative mandated by the USA PATRIOT Act. In partnership with DOJ's Bureau of Justice Assistance and the Institute for Intergovernmental Research, we developed a national counterterrorism "Train the Trainer" program. In the first phase, Institute instructor teams provided 200 FBI instructors with a counterterrorism "Train the Trainer" course. These 200, in turn, trained 25,036 police officers from April through December 2003 at minimal cost. This initiative has not only raised the level of counterterrorism expertise among state and municipal partners, it has also given FBI field agents an opportunity to interact with local officers and improve their professional relationships.

b. National Academy – Since 1935, the FBI has offered the National Academy program to experienced law enforcement managers nominated by their agency heads because of their leadership qualities. Counterterrorism instruction within the curriculum has been significantly enhanced since 9/11.

c. Field Office Initiated Training – Counterterrorism training is being provided by individual field offices to state and local law enforcement personnel in their regions.

d. WMD Training – FBI personnel are providing training related to WMD at DHS's Center for Domestic Preparedness.

Behavioral Analysis Unit

The FBI has long provided the law enforcement community with behavioral analysis support and advice in a variety of investigative matters, such as serial murders and child abduction cases. This service continues to be in demand

and we are now lending similar expertise and assistance in terrorism-related matters. In July 2003, we established a new behavioral assessment unit in the Critical Incident Response Group to provide behavioral analysis support on matters involving terrorism, threatening communications, bombings, stalkings, arsons, and anticipated or active crisis situations. The new unit also provides training and identifies behavior-focused anti-terrorism research projects to enhance investigative and preventive measures. In addition, we established a Communicated Threat Assessment Database which, when populated with historical and current case information, will serve as the repository for all communicated threats submitted to the unit for analysis.

Regional Computer Forensic Laboratory (RCFL) Program

The RCFL Program is another initiative designed to enhance our working relationships with state and municipal police departments and provide an important resource to our partners. RCFLs are laboratory facilities that conduct forensic examinations of digital media to support investigations and prosecutions and conduct local training. RCFLs are operated jointly by the FBI and other law enforcement agencies operating within a geographic area. The program has expanded quickly since the original laboratory was opened in 1999. The FBI expects to have more than ten laboratories operational by the end of 2004.

The Intelligence Community

The FBI has established much stronger working relationships with the CIA and other members of the Intelligence Community. From the Director's daily meetings with the DCI and his CIA briefers, to our regular exchange of personnel among agencies, to our joint investigations, and to our joint efforts at the Terrorist Threat Integration Center, the Terrorist Screening Center, and other multiagency entities, the FBI and its partners in the Intelligence Community are now integrated at virtually every level of operations.

Terrorist Threat Integration Center (TTIC)

TTIC is a good example of our collaborative relationship with the CIA and other federal partners. Established on May 1, 2003 at the direction of President Bush, the center coordinates strategic analysis of threats based on intelligence from the FBI, CIA, DHS, and the Department of Defense. Analysts from each agency work side-by-side to piece together the big picture of threats to the United States and its interests.

Exchange of Personnel

The FBI has several dozen employees detailed to CIA entities, with the largest contingent working at the CIA's Counter Terrorism Center. We also have FBI agents and intelligence analysts detailed to the National Security Agency (NSA), National Security Council, Defense Intelligence Agency (DIA), Department of Defense, and Department of Energy.

CIA personnel are working in key positions throughout the Bureau. The Associate Deputy Assistant Director for Operations in the Counterterrorism Division is a CIA detailee. Four CIA officers are detailed to the Security Division, including the Assistant Director and the Chief of the Personnel Security Section. An experienced manager from the CIA's Directorate of Science and Technology now heads the Investigative Technologies Division and a Section Chief in that division is on rotation from CIA.

Joint Briefings

Each morning, the Director is briefed by a CIA briefer. The DCI and the FBI Director jointly brief the President on current terrorism threats. In addition, CIA and DHS personnel attend the Director's internal terrorism briefings every weekday morning and afternoon.

Secure Networks

The FBI is now using secure systems to disseminate classified intelligence reports and analytical products to the Intelligence Community and other federal agencies. The FBI hosts a web site on the Top Secret Intelink/Joint World-Wide Intelligence Community System, a fully-encrypted system that connects more than 100 Department of Defense, CIA, and other Intelligence Community sites. In addition, a new top secret network is being piloted in several field offices, which will connect FBI Headquarters and field offices to the CIA and other members of the Intelligence Community.

Compatibility of Information Technology Systems

Improving the compatibility of information technology systems throughout the Intelligence Community will increase the speed and ease of information sharing and collaboration. Accordingly, the FBI's information technology team is working closely with the Chief Information Officers (CIOs) at DHS and other DOJ and Intelligence Community agencies, as we develop and implement our technology upgrades. This coordination has affected our decisions on several key upgrades in both software and hardware. To further facilitate coordination, our Executive Assistant Director for Administration

sits on the Intelligence Community CIO Executive Council. The Council recommends technical requirements, policies, and procedures and coordinates initiatives to improve the interoperability of information technology systems within the Intelligence Community.

Terrorist Explosive Device Analytical Center (TEDAC)
According to a recent State Department report, more than 85% of all terrorist attacks against U.S. citizens and interests during the past five years involved improvised explosive devices (IEDs), otherwise known as homemade bombs. Unlike manufactured military ordnance, these bombs often reflect the unique characteristics, or signature, of the terrorists who made them. A systematic examination of IEDs can help us draw linkages between terrorist devices and the individuals involved in their construction, and thereby improve our chances of preventing a terrorist attack. Until recently, there was no single federal agency responsible for the worldwide collection, forensic analysis, and timely dissemination of intelligence about IEDs, so the FBI established TEDAC. The center will provide "one-stop shopping" for all information on IEDs recovered both inside and outside the U.S. While the FBI manages the center, other federal agencies, including the CIA, DIA, NSA, and the Bureau of Alcohol, Tobacco, Firearms, and Explosives all contribute to its intelligence efforts.

Department of Homeland Security (DHS)

DHS plays a critical role in assessing and protecting vulnerabilities in our national infrastructure and at our borders, and in overseeing our response capabilities. The FBI is working closely with DHS to ensure that we maintain the integration and comprehensive information sharing vital to the success of our missions. Both agencies share database access at TTIC, the National JTTF at FBI Headquarters, the Terrorist Screening Center, and at local JTTFs around the country. We hold weekly briefings in which FBI and DHS counterterrorism analysts share information about current developments. We also now coordinate joint warnings through the Homeland Security Advisory System to address customers' concerns about multiple and duplicative warnings. We designated an experienced executive from the Transportation Security Administration to run the Terrorist Screening Center and detailed a senior DHS executive to the Office of Intelligence to improve coordination between the agencies.

On March 4, 2003, the Attorney General, Secretary of Homeland Security, and DCI signed a comprehensive Memorandum of Understanding (MOU) establishing policies and procedures for information sharing, handling, and use. Pursuant to that MOU, information related to terrorist threats and vulnerabilities is provided to DHS automatically without DHS having to request it. Consistent with the protection of sensitive sources and methods and the protection of privacy rights, we now share as a rule and withhold by exception.

Foreign Governments

With terrorists traveling, communicating, and planning attacks all around the world, coordination with our foreign partners has become more critical than ever before. We have steadily increased our international presence since 9/11 and now routinely deploy agents and crime scene experts to assist in the investigation of overseas attacks. As of January 2004, 413 FBI personnel were assigned overseas, over 200 of whom were permanently assigned. Their efforts, and the relationships that grow from them, have played a critical role in our successful international operations.

International Investigations

Bureau personnel participate in numerous investigations of terrorist attacks in foreign countries. Our approach to these investigations differs from the approach we traditionally have taken. Prior to 9/11, our overseas investigations primarily were focused on building cases for prosecution in the United States. Today, our focus has broadened in order to provide foreign partners with the investigative, forensic, analytical, or technical support that will enhance our joint efforts to prevent and disrupt terrorist attacks. Our partners have embraced this approach, and it is paying dividends with greater reciprocal cooperation and more effective joint investigations.

Expansion of Legal Attaché (Legat) Offices

Former Director Freeh recognized the need for greater operational collaboration with foreign government services, and during his tenure the FBI expanded the number of Legats from 23 to 44. This expansion has continued under Director Mueller in recognition of the importance of foreign cooperation in fighting terrorism. With Congressional approval, the FBI has opened ten more Legats since 2001, including ones in Beijing, Kuala Lumpur, and Abu Dhabi.

Joint Task Forces and Operations

The FBI is working with its international partners in new ways, including joint task forces, new information sharing initiatives and, in some cases, joint operations. One example is the U.S./Saudi Joint Task Force on Terrorist Financing, which was formed in 2003 to identify sources of financial support for terrorist groups and to develop strategies to stem the tide of such support. The FBI also continues to provide extensive support, such as technical assistance, laboratory testing, and forensic support, to several countries involved in investigating specific acts of terrorism, including Saudi Arabia and Indonesia. We have, for instance, provided assistance to Indonesian investigators in the case of the Bali bombings in October 2002.

Fingerprint/Identification Initiatives

Critical to our counterterrorism efforts is the use of biometric and biographical information to establish a person's identity conclusively. Several new initiatives are helping us expand our intelligence base with critical identifiers, such as fingerprints, DNA, photographs, and biographical information from foreign sources. The CJIS Division has led several overseas deployments to gather and exchange fingerprints of known and suspected terrorists. CJIS has obtained fingerprints and other identifying information for more than 10,000 terrorist suspects and detainees from more than 16 countries. CJIS is adding selected enemy combatant fingerprints to existing fingerprint databases and making them available for military, law enforcement, and homeland security needs. CJIS is also working closely with the military services to provide identification services and assistance in Iraq and Afghanistan. Lastly, CJIS personnel have provided basic training to foreign law enforcement entities on how to take viable and legible fingerprints that can be used reliably by the FBI and our partners.

International Training Initiatives

We are increasing training opportunities for our foreign partners at the FBI National Academy and at the International Law Enforcement Academies in Hungary and Thailand. Since 2001, we have trained over 20,000 international law enforcement students on topics ranging from management principles to law enforcement communications to forensic science. The relationships fostered by these training initiatives have borne fruit in improved operational coordination. In the aftermath of the May 2003 bombings in Riyadh that killed nine Americans, we received unprecedented cooperation from Saudi officials, partly because a number of Saudi police officials had received National Academy training in the science of evidence collection. As a result, our forensic technicians and their Saudi counterparts

were using the same terminology and methods of evidence collection. As our Saudi partners told us, "We were taught together, now we can work together."

The Private Sector

The FBI increasingly looks to partnerships with the private sector to enlist support for its law enforcement and intelligence missions. Among those partnerships are the following:

Community Outreach

If the FBI is to successfully predict and prevent terrorist attacks, it is imperative that we build and maintain close ties to key minority communities. The Muslim, Iraqi, and Arab-American communities have contributed a great deal to our successes, and we are grateful for their assistance and ongoing commitment to preventing acts of terrorism.

Beginning in late 2001, Director Mueller has met biannually with a group of leaders from the Arab American, Muslim American, and Sikh American communities to discuss issues, including terrorism-related money transactions, "no-fly" lists, cultural awareness training, and recruiting. In addition, each FBI field office was tasked with establishing contacts with Arab-American, Muslim, and Sikh community organizations and leaders in their territories. Since 9/11, senior field managers have attended over 1,880 town hall, community, or association meetings; participated in over 900 meetings with Middle East-American groups; and attended over 300 meetings with civil rights leaders to address their concerns. Field managers also sponsored over 130 sessions of training by representatives of Middle Eastern groups in order to improve our agents' cultural awareness and sensitivity.

InfraGard

InfraGard is a partnership between the FBI and the private sector designed to foster the exchange of information between law enforcement and the owners and operators of our nation's critical infrastructure. Using a secure web site, InfraGard members receive sensitive, but unclassified, information such as Alerts, Advisories and Information Bulletins from the FBI and DHS. InfraGard currently has 10,000 members and 79 chapters throughout the 56 field divisions. These members primarily represent small and medium-sized businesses in all of the critical infrastructure sectors. InfraGard chapters meet regularly to discuss cyber crime, terrorism, and criminal threats to critical infrastructures, and often include representatives from state, local, and federal government, academia, and law enforcement agencies. At a time when the

failure to report cyber crimes remains a major obstacle to stemming such crimes, InfraGard helps to build trust and encourages reporting. The program allows us to alert companies to threats so they can better protect themselves, and ultimately helps us identify and counter those groups and individuals who threaten our critical infrastructures.

Financial Sector Outreach

Expanding upon long-established relationships between our white-collar crime program and the financial services industry, the Terrorist Financing Operations Section conducts extensive liaison with the financial community through a series of national and international initiatives. In addition, in 2003, we established Special Agent Terrorism Financing Coordinators in each JTTF to share information and improve relationships with financial institutions in their areas.

Railroad Initiative

As evidenced by the recent bombings in Madrid, Spain, America's rail companies have critical assets that, if compromised, could cause serious disruption to our national infrastructure. To enhance our liaison with this important sector, a railroad police official has joined the National JTTF. Working through this representative, we now provide training to JTTFs that have critical railroad assets in their areas, familiarizing them with those assets and various measures for their protection.

Conclusion

The FBI seeks the input of hundreds of its key stakeholders on a daily basis to ensure that we are accomplishing our mission in the most effective and efficient manner. In addition, every field office surveys federal, state and local officials, as well as private sector entities, on a regular basis to ensure we understand the crime and intelligence issues they see as the most significant threats in their respective areas. Officials from across the FBI frequently brief members of Congress on all aspects of Bureau operations to solicit their input on and support of the direction of FBI programs. All of these efforts have led to a stronger FBI, a more collaborative law enforcement community around the globe, and a more secure America.

Appendix C

Program Evaluation

In order to measure whether the goals and objectives set forth in the Strategic Plan are being met, the FBI has developed a new multi-dimensional approach to evaluating its progress. There are three components of this new approach: field office reviews; inspections; and performance audits.

Field Office Reviews

For the first time, the FBI is requiring field offices to conduct standardized evaluative program reviews, the results of which are reported to FBI Headquarters on a semiannual basis. These reviews were designed by the Inspection Division in collaboration with the operational divisions and are based on enhanced performance metrics and improved performance assessment tools. The reviews are intended to strengthen field level implementation of the national strategic plan. They do so by examining the goals and objectives of each field office to ensure that they are compatible and consistent with national strategic goals and objectives, while also retaining some flexibility to meet the demands of the local communities they serve. More specifically, the reviews examine performance in the areas of program accomplishments, intelligence production, and utilization of resources.

Program managers at Headquarters analyze these evaluative field office reports and provide further feedback and direction, thereby strengthening national program management oversight and accountability through enhanced detection of performance anomalies and deficiencies. This enables the FBI to more proactively address resource and budget issues, identify best practices, and ensure a comprehensive assessment of our efforts to implement the Strategic Plan.

Inspections

The second component is the FBI's internal inspection process. The Office of Inspections conducts rigorous on-site reviews of all field offices, Headquarters divisions, and Legats on a rotating basis every three years. These inspections encompass an office or division's performance in every aspect of operations and administration. They are intended to determine whether a division or office is performing effectively and efficiently, and to aggressively address

significant performance issues when they are discovered. Subsequent to each on-site visit, the inspection team provides instructions and recommendations to the entity being inspected, as well as to program managers, on ways to improve performance and ensure that there is sufficient compliance with rules, regulations, policies, and procedures. Each inspection also verifies information provided in the semi-annual field office reports and follows up on the findings and recommendations provided in internal and external performance audit reports. The results of inspections are reinforced by the Director through post-inspection reporting and follow up.

Performance Audits

The third component of the FBI's efforts to evaluate its own progress is its internal performance audit capability. The FBI conducts comprehensive program evaluations on a regularly scheduled basis. These are independent and objective studies conducted by a dedicated office within the Inspection Division known as the Organizational Program Evaluation and Analysis Unit (OPEAU). Evaluation specialists from this office design and conduct performance audits of programs and activities in the FBI, using both qualitative and quantitative methods of data collection. Such research is intended to make judgments about programs or activities, and thereby inform decisions by management to change those programs or activities for the better. This information can be critical to ensuring that the FBI uses its limited resources in the most effective manner.

Authority for program evaluations derives from the Inspector General Act of 1978 and the Government Performance Results Act (GPRA) of 1993. During evaluations, the FBI adheres to the standards set forth in Government Auditing Standards, 2003 Revision (Yellow Book), published by GAO. These standards require FBI evaluation specialists to remain fully independent of the staffs of the programs under review. Evaluative studies are usually complex and multi-faceted, involving several organizational levels, processes, or functions throughout the Bureau, and can at times impact the entire organization.

The FBI has long had an internal evaluation capacity, but that capacity is now more firmly linked to its strategic planning and budget processes. The OMB has developed a new instrument for linking budget and performance in all federal programs entitled the Performance Assessment Rating Tool (PART). The PART is an accountability tool that helps government agencies focus on the results their programs produce. It does so by rating each program in four

areas (program purpose & design, strategic planning, program management, and program results) and calculating a composite "score" using a 100-point scale. Two of the questions within PART, accounting for 11% of the overall score, ask whether "independent and objective" evaluations have been conducted. In order to serve the PART process, the FBI has revised its evaluation schedule and enhanced its evaluation capacity. Under this new approach, OPEAU recently completed an evaluation of the Cyber Program and is currently working on a study of the Criminal Justice Services Program. It is expected that the new approach will also better meet the needs of the Director and executive management as they transform the FBI to achieve its new mission responsibilities.

The FBI's evaluation function augments the compliance audit function performed by the Office of Inspections. As part of the new reengineered inspection process, evaluation reports are provided to inspection teams prior to their on-site visits to assist them in identifying issues and concerns, and in turn, inspection data and findings are available to evaluation specialists as potential sources of information during the course of their research.

In addition to its own internal evaluation schedule, the FBI is also working cooperatively with the DOJ's Office of Inspector General (OIG) and the GAO to cultivate a strong external evaluation capacity. Both the OIG and GAO have significantly expanded their performance audits of FBI programs and operations since 2001. As of June 2004, the OIG had 61 ongoing audits and the GAO had 80 ongoing audits. These external evaluations have done much to improve FBI administrative practices and investigative operations in a wide range of areas.