U.S. Department of Justice
Federal Bureau of Investigation

FY 2012
Authorization and Budget Request to Congress

February 2011

Table of Contents

Page No.

I. OVERVIEW FOR THE FEDERAL BUREAU OF INVESTIGATION

A. Introduction

Budget Summary: The Federal Bureau of Investigation's (FBI's) Fiscal Year (FY) 2012 budget request proposes a total of $8,075,973,000 in direct budget authority, including 33,469 permanent positions (12,993 Special Agents (SAs), 2,989 Intelligence Analysts (IAs), and 17,487 professional staff (PS)) and 32,777 full time equivalents (FTE). The request includes a total of $7,994,991,000 for Salaries and Expenses (S&E) and $80,982,000 for Construction to address the FBI's highest priorities.

The request includes program increases of $131,450,000 and 181 positions (81 SAs, 3 IAs, and 97 PS) and 89 FTE. This funding would support several critical initiatives, to include:

- Cybersecurity and Digital Forensics;
- Intelligence training;
- Data Integration and Visualization System;
- High-Value Detainee Interrogation Group;
- Indian Country; and
- WMD Render Safe.

Note that of the $131,450,000, $10,495,000 is being requested to support Information Technology (IT) purposes.

The FBI continues to strategically assess current and prospective operations to ensure that mission requirements are met at the lowest possible cost to the U.S. taxpayer. The FY 2012 budget request is a product of these assessments and provides the resources to achieve the FBI's strategic objectives.

Electronic copies of the Department of Justice's Congressional Budget Justifications and Capital Asset Plan and Business Case exhibits can be viewed or downloaded from the Internet using the Internet address: http://www.justice.gov/02organizations/bpp.htm.

The FBI's Mission and Strategic Goals: The mission of the FBI is to protect and defend the U.S. against terrorism and foreign intelligence threats, to uphold and enforce the criminal laws of the U.S., and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners.

Organization of the FBI: The FBI operates field offices in 56 major U.S. cities and 394 "resident agencies" throughout the country. Resident agencies are satellite offices that support the larger field offices and allow the FBI to maintain a presence in and serve communities that are distant from field offices. FBI employees assigned to field offices and resident agencies perform the majority of the investigative and intelligence work for the FBI. Special Agents in Charge of FBI Field Offices report to the Deputy Director and Director. The FBI also operates 61 Legal Attaché (Legat) offices and 14 sub-offices in 66 foreign countries around the world.

Other major FBI facilities include the FBI Academy, the Engineering Research Facility (ERF), and the FBI Laboratory, all at Quantico, Virginia; a fingerprint identification complex in Clarksburg, West Virginia; and the Hazardous Devices School at Redstone Arsenal, Alabama.

FBI Headquarters, located in Washington, D.C., provides centralized operational, policy, and administrative support to FBI investigations and programs conducted throughout the U.S. and in foreign countries. Under the direction of the FBI Director and Deputy Director, this support is provided by:

- The National Security Branch, which includes the Counterterrorism Division, Counterintelligence Division, the Directorate of Intelligence, and the Weapons of Mass Destruction Directorate.
- The Criminal, Cyber, Response and Services Branch, which includes the Criminal Investigative Division, the Cyber Division, the Critical Incident Response Group, the International Operations Division, and the Office of Law Enforcement Coordination.
- The Science and Technology Branch, which includes the Criminal Justice Information Services Division, the Laboratory Division, and the Operational Technology Division.

A number of other Headquarters offices also provide FBI-wide mission support:

- The newly reorganized Information and Technology Branch oversees the IT Management Division, IT Engineering Division, and the IT Services Division.
- The Human Resources Branch includes the Human Resources Division and the Training Division.
- Administrative and financial management support is provided by the Facilities and Logistics Services Division, the Finance Division, the Records Management Division, the Security Division, the Resource Planning Office, and the Inspection Division.
- Specialized support is provided directly to the Director and Deputy Director through a number of staff offices, including the Office of Public Affairs, the Office of Congressional Affairs, the Office of the General Counsel, the Office of Equal Employment Opportunity, the Office of Professional Responsibility, the Office of the Ombudsman, and the Office of Integrity and Compliance.

B. Threats to the United States and its Interests

In an effort to better address all aspects of the FBI's requirements, the FY 2012 budget is structured according to the threats that the FBI works to deter. These threats have been identified by the Director as the FBI's priorities and thus must be resourced accordingly.

Terrorism Threat: Terrorism, in general, and al-Qa'ida and its affiliates in particular, continues to represent the most significant threat to the country's national security. Al-Qa'ida remains committed to its goal of conducting attacks inside the U.S. and continues to adjust its tactics and tradecraft in response to U.S. security countermeasures. Al-Qa'ida continues to seek to infiltrate overseas operatives who have no known nexus to terrorism into the U.S. using both legal and illegal methods of entry. Further, al-Qa'ida's access to chemical, biological, radiological, or nuclear material poses a serious threat to the U.S. Finally, al-Qa'ida's choice of targets and attack methods will most likely continue to focus on economic targets, such as aviation, the

energy sector, and mass transit; soft targets such as large public gatherings; and symbolic targets, such as monuments and government buildings.

Religious extremists are using increasingly-diverse methods of member recruitment and development, which pose a very serious threat. In FY 2010, there has been a sharp rise in incidents from radicalized Muslims who adopt their mindsets as a result of contact with extremists, whether through online contact or after returning from travel to a sympathetic country or camp.

The internet is evolving into an effective terrorist recruitment tool. Through chat rooms, websites, and social media pages, one can obtain data on and make contact with radical groups without the risk of alerting authorities through overseas travel. Maj. Hasan, the alleged shooter in the Ft. Hood incident, fit this profile; his email contact with a radical imam overseas may have played a part in his decision to attack fellow soldiers in November 2009. Further, in March 2010, Collen LaRose, who called herself 'Jihad Jane' in internet chat rooms, was indicted for plotting the murder of a Swedish cartoonist. LaRose allegedly converted to Islam as a result of visiting extremist websites and is accused of using email to solicit funding for jihadist causes.

Although the internet may provide a "below-the-radar" introduction to the radical side of Islam, it appears that many would-be terrorists still meet with their sponsors and trainers in person. FY 2010 has also seen an increase in U.S. citizens who have traveled overseas to countries or camps with terrorist ties and then returned to the U.S. to do harm, as was the case in both the Christmas Day and Times Square terrorism attempts.

While much of the national attention is focused on the substantial threat posed by radicalized religious terrorists who target the Homeland, the U.S. must also contend with an ongoing threat posed by domestic terrorists based and operating strictly within the U.S. Domestic terrorists, motivated by a number of political or social issues, continue to use violence and criminal activity to further their agendas. In March 2010, nine people in Ohio, affiliated with the Hutaree militia, were arrested for allegedly planning a war against federal and local law enforcement agencies.

Weapons of Mass Destruction Threat: The global Weapons of Mass Destruction (WMD) threat to the U.S. and its interests continues to be a significant concern. In 2008, the National Intelligence Council produced a National Intelligence Estimate to assess the threat from Chemical, Biological, Radiological, and Nuclear (CBRN) weapons. The assessment concluded that it remains the intent of terrorist adversaries to seek the means and capability to use WMD against the U.S. at home and abroad. In 2008, the Commission on the Prevention of WMD Proliferation and Terrorism concluded that "the United States government has yet to fully adapt…that the risks are growing faster than our multilayered defenses." The WMD Commission warned that without greater urgency and decisive action, it is more likely than not that a WMD will be used in a terrorist attack somewhere in the world by the end of 2013. Osama bin Laden has said that obtaining a WMD is a "religious duty" and is reported to have sought to perpetrate a "Hiroshima" on U.S. soil. Globalization makes it easier for terrorists, other groups, and lone actors to gain access to and transfer WMD materials, knowledge, and technology throughout the world. As noted in the WMD Commission's report, those intent on using WMDs have been active and as such "the margin of safety is shrinking, not growing."

Foreign Intelligence Threat: The foreign intelligence threat to the U.S. continues to increase as foreign powers seek to establish economic, military, and political preeminence and to position

themselves to compete with the U.S. in economic and diplomatic arenas. The most desirable U.S. targets are political and military plans and intentions; technology; and economic institutions, both governmental and non-governmental. Foreign intelligence services continue to target and recruit U.S. travelers abroad to acquire intelligence and information. Foreign adversaries are increasingly employing non-traditional collectors – e.g., students and visiting scientists, scholars, and businessmen – as well as cyber-based tools to target and penetrate U.S. institutions. On 16 July 2009, Dongfan "Greg" Chung was found guilty of six counts of Economic Espionage, one count of conspiracy to commit Economic Espionage, one count of agent of a Foreign Government, and one count of false statements. On 9 February 2010, Chung was sentenced to more than 15 years in prison. This was the first economic espionage case to go to trial and the first to get a conviction.

Cyber Threat: Cyber threats come from a vast array of groups and individuals with different skills, motives, and targets. Terrorists increasingly use the Internet to communicate, conduct operational planning, propagandize, recruit and train operatives, and obtain logistical and financial support. Foreign governments have the technical and financial resources to support advanced network exploitation, and to launch attacks on the U.S. information and physical infrastructure. Criminal hackers can also pose a national security threat, particularly if recruited, knowingly or unknowingly, by foreign intelligence or terrorist organizations. The FBI Computer Intrusions Program continues its efforts to counter increasingly sophisticated and expanding cyber threats in collaboration with its government, private sector, and international partners. In FY 2010, the FBI participated in cyber investigations ranging from the theft of 3.3 million college students' identities, to people selling counterfeit cancer drugs over the internet.

Regardless of the group or individuals involved, a successful cyber attack can have devastating effects. Stealing or altering military or intelligence data can affect national security. Attacks against national infrastructure can interrupt critical emergency response services, government and military operations, financial services, transportation, and water and power supply. In addition, cyber fraud activities pose a growing threat to our economy, a fundamental underpinning of U.S. national security.

White Collar Crime Threat: The White Collar Crime (WCC) program addresses the following principle threats: public corruption including government fraud, economic stimulus fraud, and border corruption; corporate and securities fraud; mortgage fraud and other financial institution fraud; health care fraud; money laundering; and other complex financial crimes.

- Public Corruption: Public Corruption involves the corruption of local, state, and federally elected, appointed, or contracted officials, both within the U.S. and internationally, which undermines our democratic institutions and threatens public safety and national security. Government fraud can affect everything from how well U.S. borders are secured and neighborhoods protected, to the quality of public infrastructure such as schools and roads, and the use of taxpayer dollars overseas. Many taxpayer dollars are wasted or lost as a result of corrupt acts by public officials.

- Economic Stimulus Fraud: The FBI has determined the influx of $787 billion in American Recovery and Reinvestment Act (ARRA) stimulus funding is at risk of fraudulent schemes. FBI intelligence analysis identified potential vulnerabilities related to the rapid implementation of the programs and the distribution of funds. Likely

vulnerabilities include risks in the government acquisition system, distribution requirements mandating swift spending by state and local government, and special interest groups earmarking monies for pet projects. Of particular vulnerability to corruption and fraud was money provided to localities for "shovel-ready" projects. Given historical precedent and preliminary open-source reports the potential for public corruption is high.

- The FBI anticipates corruption, government fraud, and corporate fraud during the administration of approximately $700 billion by the U.S. Department of the Treasury through the Troubled Asset Relief Program (TARP) established as part of the Emergency Economic Stabilization Act (EESA). An FBI Criminal Intelligence Section (CIS) Intelligence Note assessed the probability for public corruption and fraud due to historical precedent and preliminary open-source reports.

  The FBI foresees a significant increase in fraud and public corruption related to the Housing and Economic Recovery Act of 2008 (HERA). HERA authorized the establishment of the Neighborhood Stabilization Program (NSP), which will appropriate $3.92 billion to states and local governments for the management and redevelopment of abandoned and foreclosed homes. Additionally, the ARRA provides an additional $2 billion in competitive grants for NSP use. Through the NSP, the U.S. Department of Housing and Urban Development (HUD) will manage the distribution of funds through community development block grants (CDBG). Based on a study of foreclosed properties, 308 state and local governments (grantees) were chosen to receive CDBGs.

- Border Corruption: The Federal Government is responsible for protecting approximately 7,000 miles of the U.S. border and 95,000 miles of shoreline. Each day, approximately 1.1 million persons visit the U.S. and enter through one of the 327 official Ports of Entry (POEs) located along the southwestern and northern land borders of the U.S., as well as at seaports and international airports. The documented presence of corrupt border officials facilitates a wide range of illegal activities along the northern and southern borders. Resource-rich cartels and criminal enterprises employ a variety of methods in order to target and recruit U.S. Border Patrol Agents, Customs and Border Protection Officers, and local police officers who can facilitate the criminal activity. Corrupt officials assist the cartels by providing intelligence and contraband across these borders. To help address this threat, the Border Corruption Initiative (BCI) was established in 2009. The BCI has developed a threat tiering methodology, targeting border corruption in all land, air, and sea ports of entry to mitigate the threat posed to national security. The FBI has established the National Border Corruption Task Force (NBCTF) and 21 Border Corruption Task Forces (BCTFs) in high risk cities along the northern and southern borders.

- Corporate Fraud: As the lead agency investigating corporate fraud, the FBI focuses on cases that involve accounting schemes, self-dealing corporate executives, and obstruction of justice. In these cases, investors, auditors, and analysts are deceived about the true condition of a corporation. Through the manipulation of financial data, the share price of a corporation remains artificially inflated based on fictitious performance indicators provided to the investing public. In addition to significant financial losses to investors,

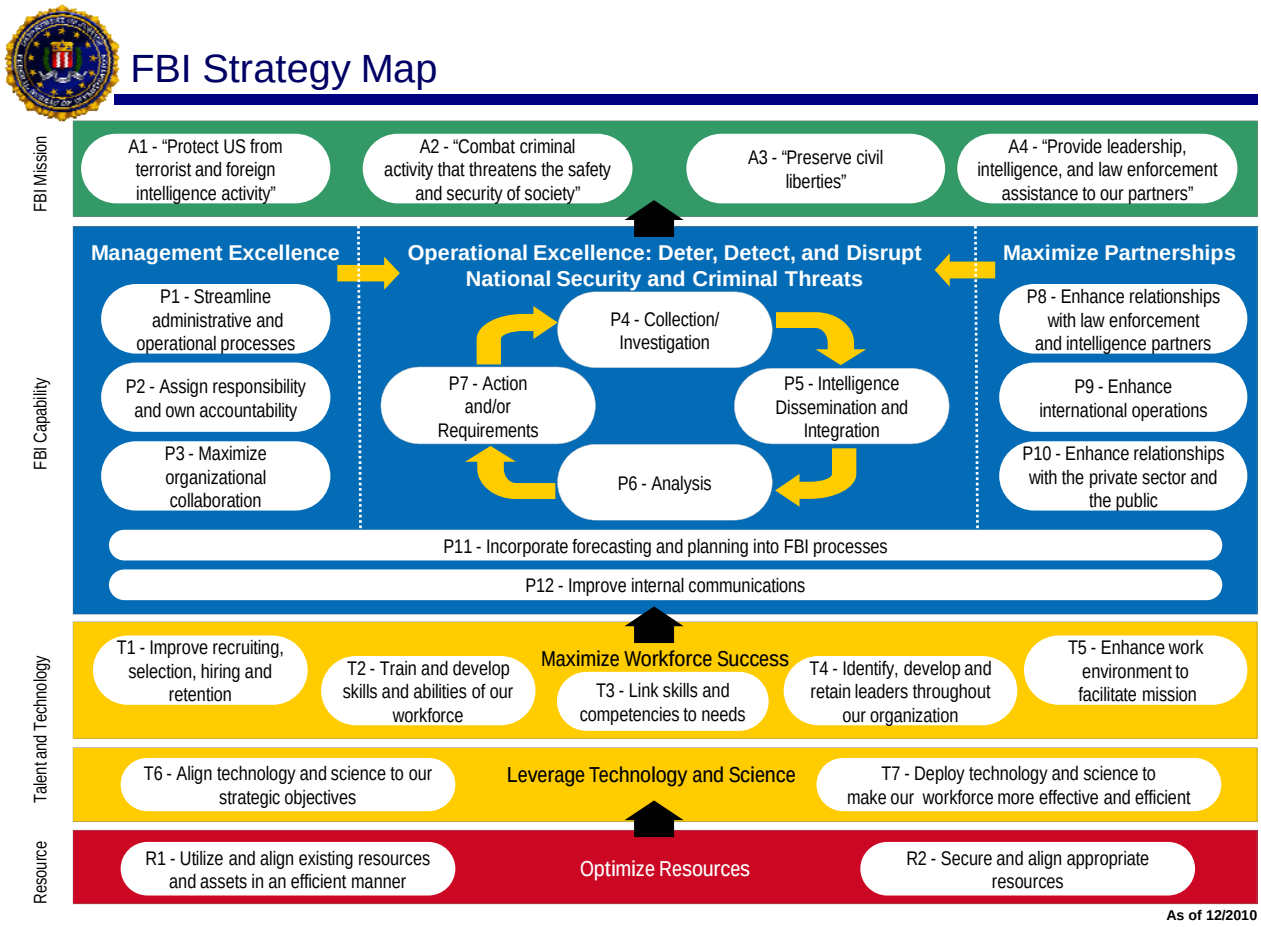
corporate fraud has the potential to cause immeasurable damage to the U.S. economy and investor confidence.

Examples of Corporate Fraud include:

1. Falsification of financial information, including:
    - False accounting entries
    - Bogus trades designed to inflate profit or hide losses
    - False transactions designed to evade regulatory oversight
2. Self-dealing by corporate insiders, including:
    - Insider Trading
    - Kickbacks
    - Backdating of Executive Stock Option
    - Misuse of corporate property for personal gain
    - Individual tax violations related to self-dealing
3. Fraud in connection with an otherwise legitimately-operated mutual or hedge fund, including:
    - Late Trading
    - Certain market timing schemes
    - Falsification of net asset values
    - Other fraudulent or abusive trading practices by, within, or involving a mutual or hedge fund
4. Obstruction of justice designed to conceal any of the above-noted types of criminal conduct, particularly when the obstruction impedes the inquiries of the Securities and Exchange Commission (SEC), other regulatory agencies, and/or law enforcement agencies.

- Securities Fraud: The FBI focuses its efforts in the securities fraud arena to schemes involving high yield investment fraud (to include Ponzi schemes), market manipulation, and commodities fraud. Due to the recent financial crisis, the FBI saw an unprecedented rise in the identification of Ponzi and other high yield investment fraud schemes, many of which involve thousands of victims and staggering losses – some in the billions of dollars. Indeed, the FBI continues to open new Ponzi scheme cases on a weekly basis. With this trend, and the development of new schemes, such as stock market manipulation via cyber intrusion, securities fraud is on the rise. Over the last five years, securities fraud investigations have increased by 47 percent.

  The FBI has adopted an intelligence-led approach to identifying and targeting the most egregious perpetrators of securities fraud, utilizing undercover operations to identify and stop perpetrators before they are able to victimize individuals and damage the financial markets. Securities and Futures Industries Suspicious Activity Reports (SARs) contain some of the best intelligence available to criminal and regulatory law enforcement personnel. In 2009, CID established a new process to better exploit this intelligence to identify new securities fraud schemes and perpetrators. With the coordinated effort of special agents and intelligence analysts, these SARs are analyzed on a national level, leading to the creation of targeting packages which are presented to relevant field offices to open investigations. Among the schemes that were identified through this newly



The Strategy Map provides the ability to portray the FBI's strategy. The story can be told from the "top down:" The FBI will achieve its mission and meet the expectations of the American public by utilizing intelligence and investigations to deter, detect, and disrupt national security threats and criminal activity. It will support these critical operational processes by excelling at managing the organization and by maximizing partnerships with federal, state, local, and international partners. The organization's people and technology provide the capabilities to operate these critical internal processes. Therefore, the FBI must optimize and align its resources in order to maximize workforce success and leverage technology and science.

Alternatively, the story can be told from the "bottom up:" The FBI will optimize its resources in order to hire, train and retain the right people, and implement the necessary technology to support its operations. The Bureau will manage the business effectively and leverage partnerships in order to help deter, detect, and disrupt national security threats and criminal activity. By integrating intelligence with law enforcement, and maintaining traditional standards in other operations, the FBI will execute its mission and meet the expectations of the American people.

SMS Profile

The SMS profile serves as the framework to translate strategy into a list of operational objectives, measures, and initiatives that drive behavior and performance. Each of the objectives identified on the Strategy Map is linked to one or more measures and each measure has a target that defines success. In addition, key strategic initiatives are identified and tracked to ensure that any performance gaps are closed.

The FBI's leadership team uses SMS to manage organizational performance by conducting regular strategy review meetings. At these meetings, leadership reviews SMS profiles, along with information and data on SMS objectives, measures, and initiatives. During these meetings, the leadership team discusses performance and makes decisions on resolving critical performance issues.

Ultimately, the FBI's field offices are central to implementing the organization's strategy. Accordingly, in addition to these strategy review meetings, the FBI uses Strategic Performance Sessions (SPS) to obtain perspectives on key strategic issues from the field offices' perspective. These quarterly sessions are led by the Deputy Director and typically focus on discussions with field managers on a key area of the FBI's strategy.

The SMS is a continuous process for driving evolutionary improvements. Reviews not only track strategic progress; they also examine what is working and not working and what needs to be adjusted. Over time, the Strategy Map and the 25 objectives may change. Initiatives that are not succeeding are provided with the support they need to succeed or will be eliminated, and other initiatives are added to address identified gaps. The SMS provides the flexibility the FBI needs to stay ahead of changing threats and demographic and other trends that impact its mission.

Intelligence-Driven Operations:

Since the events of September 11, 2001, the FBI has transformed from a law enforcement agency to a *national security and law enforcement* agency. The FBI uses intelligence to understand national security threats, and to conduct operations to dismantle or disrupt those threats. Some examples of how the FBI uses intelligence to drive its operations include:

- Field Intelligence Groups (FIGs): The FBI developed a standardized model for field intelligence that can be adjusted to the size and complexity of small, medium, and large offices. There are now 56 FIGs throughout the Nation.
- Central Strategic Coordinating Components (CSCCs): These intelligence components are embedded into the Headquarters' operational divisions in order to ensure intelligence-driven operational strategies and provide a view of national threats.
- The Collection Operations Requirements Environment (CORE): CORE is a technology solution that makes FBI and national intelligence requirements easily accessible to all field office personnel and improves information flow between operational squads and the FIGs.

Multi-year Planning:

An increasing number of the FBI's programs and initiatives are multi-year in nature, and require phased development, deployment, and operations/maintenance funding. A multi-year planning approach allows FBI management to better understand the implications of proposed initiatives.

A new aspect of the multi-year planning effort is the Capital Planning Working Group, which is currently examining the long-term needs of the Quantico facilities. In October 2008, the FBI conducted an Activity-Based Costing (ABC) study of the FBI Academy in Quantico, Virginia. The goal was to create a planning model to help project how increased demand for investigative and intelligence training will affect FBI Academy operations.

In September 2009, with the ABC study completed, the FBI analyzed the effect that increased training will have on demand for capital assets. The challenge of this effort was to bring disparate information together into a cohesive and quantifiable plan with well-defined projects, presented in a manner that considers both the priority of each project and its relationship to other elements of the revitalization effort.

D. Environmental Accountability

The FBI has begun developing an Organizational Environmental Management System (EMS) that will provide corporate-wide environmental protection standards to deploy to the field offices and major facilities (to include CJIS, Quantico, and HQ). The organizational EMS has been developed and implemented through Environmental Protection Programs (EPPs) that establish policy and procedure in major environmental programmatic areas (e.g., hazardous waste management, energy management). The first six EPPs were developed and fully implemented at the end of FY 2010. Individual facility and field office EMSs will follow. An overarching environmental policy is currently being reviewed by FBI top management to serve as the guiding framework for developing, implementing, and continually improving the EMS.

Additionally, the FBI is gathering and maintaining applicable environmental compliance information from its existing audit program and plans to manage this information centrally using a computer-aided facility management program. Managing the information using a software solution provides the advantage of a standardized platform to meet all compliance and sustainability requirements, which functions as single reporting portal for FBI corporate environmental information.

The FBI is revising its safety committee policy and procedures to expand the jurisdiction of our safety committees to include environmental issues. In essence, these safety committees – which are in place within all Bureau Divisions and major facilities – will become “green teams” as well and will provide a forum for discussion of environmental issues and a mechanism for EMS implementation.

The FBI actively participates in DOJ’s overall efforts to implement Executive Order 13514. FBI provided data and input into the Department’s Strategic Sustainability Performance Plan (SSPP) and routinely corresponds with DOJ and the other Bureaus to determine the most efficient, effective methods to protect the environment. Notably, FBI completed its first greenhouse gas inventory for its facilities and operations, and the results of this inventory will provide additional input to decision makers as they determine where to target efficiency measures.

The FBI has developed a sustainable building policy that addresses requirements of Executive Orders 13423 and 13514, the Federal Leadership in High Performance and Sustainable Buildings Memorandum of Understanding of 2006, the Energy Policy Act of 2005, and the Energy Independence and Security Act of 2007. The FBI's policy requires that new FBI-owned facilities be designed and constructed to meet the minimum of a Leadership in Energy and Environmental Design (LEED) Certified Silver Rating in the New Construction category. In addition, the policy - which was signed and implemented in 2008 - requires the installation of advanced metering devices and the use of recycled content or environmentally preferable products in construction of new facilities. Since the policy has been implemented, the FBI has received several LEED Silver Certifications for various buildings and a LEED Platinum Certification for Existing Buildings Operations and Maintenance for one facility.

The FBI's Fleet Management Program integrates environmental accountability into its operations in various ways. The FBI is in the process of incorporating hybrid vehicles, alternative fuel vehicles (E85), and more fuel efficient vehicles (4 cylinders) into our fleet. Additionally, the FBI's Automotive Maintenance and Repair Facilities incorporate environmental accountability through various programs. These facilities use re-refined motor oil for a majority of the vehicles serviced and recycle all used oil. Automotive facilities also use air conditioning and coolant recycling machines in connection with the servicing of vehicles. A battery exchange program is in place to ensure used batteries are returned to the vendor for proper recycling. In addition, many facilities are reviewing the use of environmentally friendly chemicals: degreasers, hand cleaners, and general purpose cleaners, in day to day operations. Finally, some facilities have eliminated hazardous waste entirely through pollution prevention and recycling programs.

II. Summary of Program Changes

Threat Name	Description	Pos.	FTE	Dollars ($000)	Page
Salaries and Expenses Enhancements					
1. Computer Intrusions	To enhance the FBI's investigatory capabilities and protect critical technology network infrastructure from malicious cyber intrusions.	42	20	18,628	5-1
2. National Security	To expand the FBI's surveillance and data collection capabilities to address National Security threats.	73	37	$48,870	5-6
3. Electronic Surveillance Capabilities	To establish a Domestic Communications Assistance Center to support law enforcement's electronic surveillance capabilities.	13	6	12,466	5-7
4. WMD/Render Safe Capability	To complete the acquisition and outfitting of two dedicated mission-tailored Render Safe aircraft to ensure the FBI meets response mandates.	13	6	40,000	5-10
5. Operational Enablers	To provide increased analytical training.	…	…	2,486	5-14
6. Violent Crime in Indian Country	To bolster existing Safe Trails Task Forces and to provide additional investigative resources to address a significant violent crime threat in Indian Country.	40	20	9,000	5-17
Total, Salaries and Expenses Enhancements		**181**	**89**	**$131,450**	

Threat Name	Description	Pos.	FTE	Dollars ($000)	Page
Offsets/Direct to Reimbursable Funding Reallocation					
Administrative Efficiencies	To reduce funding for administrative areas such as travel and transportation supplies and materials, and equipment.	…	…	(5,910)	6-1
Extend Tech Refresh	To reduce Information Technology (IT) operations and maintenance funding.	…	…	(5,651)	6-3
HQ/Field Cost Module Reduction	To reduce funding by eliminating headquarters cost modules for Special Agents and Intelligence Analysts and using only field cost modules.	…	…	(762)	6-5
Lookout Program Efficiencies	To reduce funding by consolidating some permanent platform spaces currently used for fixed surveillance.	…	…	(2,600)	6-7
Network and Intrusion Analysis	To reduce by 50 percent the development of new tools to identify and analyze network intrusions.	(6)	(6)	(5,766)	6-9
Reduce Physical Footprint	To streamline the structure of resident agencies by consolidating and reducing its 385 resident agencies by 12 locations.	…	…	(674)	6-11
Relocation Program	To reduce funding supporting employee relocations.	…	…	(6,250)	6-14
Sentinel	To reduce Sentinel development funding.	…	…	(15,000)	6-16
Task Force Consolidation	To reduce the FBI's criminal task force footprint through consolidating 48 task forces within the same geographic area or by eliminating lower priority task forces.	…	…	(898)	6-18
Total, Offsets		**(6)**	**(6)**	**(43,511)**	

III. Appropriations Language and Analysis of Appropriations Language

Appropriations Language for Salaries and Expenses

For necessary expenses of the Federal Bureau of Investigation for detection, investigation, and prosecution of crimes against the United States, $7,994,991,000; Provided, That not to exceed $150,000,000 shall remain available until expended; Provided further, That not to exceed $205,000 shall be available for official reception and representation expenses.

Note. A full-year 2011 appropriation for this account was not enacted at the time the budget was prepared; therefore, this account is operating under a continuing resolution (P.L. 111-242, as amended). The amounts included for 2011 reflect the annualized level provided by the continuing resolution.

Analysis of Appropriations Language

No substantive changes proposed.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. Decision Unit Justification

A. Intelligence Decision Unit

INTELLIGENCE DECISION UNIT TOTAL	Perm. Pos.	FTE	Amount ($000)
2010 Enacted with Rescissions	6,878	6,455	$1,606,025
2011 Continuing Resolution	6,787	6,394	1,526,146
Adjustments to Base and Technical Adjustments	55	293	48,692
2012 Current Services	6,842	6,687	1,574,838
2012 Program Increases	17	9	25,317
2012 Program Offsets	…	…	(6,766)
2012 Request	6,859	6,696	1,593,389
Total Change 2011-2012	**72**	**302**	**$67,243**

Intelligence Decision Unit—Information Technology Breakout	Perm. Pos.	FTE	Amount* ($000)
2010 Enacted w/Rescissions and Supplementals	713	713	$271,998
2011 Continuing Resolution	243	243	300,327
Adjustments to Base and Technical Adjustments	13	13	(29,949)
2012 Current Services	256	256	270,378
2012 Program Increases	…	…	…
2012 Request	256	256	270,378
Total Change 2011-2012	**13**	**13**	**($29,949)**

*Includes both direct and reimbursable funding

1. Program Description

The FBI's Intelligence Decision Unit (IDU) is comprised of the Directorate of Intelligence (DI), including embedded intelligence functions within Counterterrorism, Counterintelligence, Cyber, Criminal, and Weapons of Mass Destruction Divisions; Field Intelligence Groups (FIGs); Special Technologies and Applications Office (STAO); Terrorist Screening Center (TSC); Infrastructure and Technology; and Intelligence Training. Additionally, to capture all resources that support these programs, a prorated share of resources from the FBI's support divisions (including Training, Laboratory, Facilities and Logistics Services, Information Technology (IT) Operations, and Human Resources) are calculated and scored to the decision unit.

Directorate of Intelligence

The FBI established the DI as a dedicated and integrated intelligence service. This action responds to executive and legislative direction as the logical next step in the evolution of the FBI's intelligence capability. The DI is the FBI's core intelligence element and one of the four major organizations that comprise the National Security Branch (NSB).

The DI is the FBI's dedicated national intelligence workforce with delegated authorities and responsibilities for all FBI intelligence functions, including information sharing policies, from three legal documents: a Presidential Memorandum to the Attorney General dated November 16, 2004; the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004; and the Fiscal Year (FY) 2005 Omnibus Appropriation Bill. The Directorate carries out its functions through embedded intelligence elements at FBI Headquarters (FBIHQ) and in each field office.

Intelligence Analysts
The work performed by Intelligence Analysts (IAs) is essential to the FBI's ability to understand today's threats to national security and to develop a deeper understanding of tomorrow's potential threats. To safeguard national security, the FBI must focus significant analytic resources to analyze the threat, its nature, and potential courses of action, and to then place this analysis in the context of ongoing intelligence and investigative operations. The FBI's intelligence analytic cadre performs functions including understanding emerging threat streams to enhance domain knowledge and exploit collection opportunities, enhancing collection capabilities through the deployment of the collection strategies, reporting raw intelligence in a timely manner, identifying human and technical source collection opportunities, performing domain analysis in the field to articulate the existence of a threat in their area of responsibility, performing strategic analysis at FBIHQ to ascertain the ability to collect against a national threat, serving as a bridge between intelligence and operations, performing confidential human source validation, and recommending collection exploitation opportunities at all levels. The products generated by intelligence analysis drive FBI investigative and operational strategies by ensuring they are based on an enterprise-wide understanding of the current and future threat environments.

Field Intelligence Groups
Field Intelligence Groups (FIGs) are the centralized intelligence components in the field that are crucial to the integration of the intelligence cycle (requirements, collection, analysis and dissemination) into field operations. In accordance with FBI policy and/or guidance to the field, each FIG is responsible for coordinating, guiding, and supporting the office's activities through the five core intelligence functions, which strengthen these efforts into field operations. These functions are: Domain Management; Collection Management; Requirements-based (sometimes non-case) collection – including human intelligence (HUMINT); tactical intelligence; and intelligence production and dissemination. All five of the core intelligence functions require the FIG to work seamlessly with the operational squads in order to be successful.

FIG Agents
FIG Agents are required to perform one or more of the following primary functions: intelligence collection, collection management, Confidential Human Source (CHS) coordination, focused source recruitment, source development and validation, and intelligence and partner relations. FIG Agents' intelligence collection activities include maintaining a CHS base and conducting threat assessments. All Agents assigned to the FIG work closely with analysts on the FIG to report observations indicating new trends in the local environment, collect key intelligence based upon the organization's priority threat or vulnerabilities, and to spot areas and targets for source recruitment. FIG Agents serve to facilitate the handling of cross-programmatic intelligence information obtained from CHS debriefings.

To do this effectively, HUMINT collectors on the FIG must have strong relationships with other collectors and embedded IAs on investigative squads in order to augment their collection abilities beyond reporting on the squad's investigations.

Foreign Language Program
The FBI's success at protecting the U.S. from future terrorist attacks, countering foreign intelligence operations and espionage, and dismantling transnational organized criminal enterprises is increasingly dependent upon a workforce with high quality, robust capabilities in 67 languages. This workforce is managed through the FBI's Foreign Language Program (FLP). Nearly every major FBI investigation now has a foreign language component and the demand for

highly qualified linguists and foreign language and culture training continues to increase. The mission of the FLP is to provide quality language services to the FBI, intelligence, and law enforcement communities, and to maximize the deployment of the linguist workforce, language tools, and technology in line with critical intelligence, investigative, and administrative priorities. The FBI's FLP also promulgates policies and compliance requirements; manages translation and interpreting resources throughout the world; and develops the foreign language skills of employees through on-going training, as well as language testing and assessment.

National Virtual Translation Center

The National Virtual Translation Center (NVTC) was established under the authority of Section 907 of the USA PATRIOT Act to "provide accurate and timely translations of foreign intelligence material to the U.S. Intelligence Community." On February 11, 2003, the Director of Central Intelligence awarded executive agency authority of the NVTC to the FBI. The NVTC is one of the Office of the Director of National Intelligence's (ODNI) controlled multi-agency centers, which was created to provide language services to the 16 agencies in the IC specifically working in national security and intelligence arenas. The NVTC is prohibited from assisting in criminal investigations. The NVTC's mission is to provide translation services and a community portal for accessing language-related tools and a broad range of foreign language materials in translated or vernacular form across security domains; function within the IC System for Information Sharing (ICSIS), which provides a common architecture and promotes interoperability and virtual access to databases across the IC; support continued development and fielding of tools, web-based and other, designed to help process and exploit foreign language text; and develop policies, procedures, and systems for managing NVTC translation requirements and translation services.

Language Analysis

Language Analysis is a critical process in the FBI's effort to acquire accurate, real-time, and actionable intelligence to detect and prevent foreign-originated terrorist attacks against the U.S. The FBI's language analysis capabilities promptly address all of its highest priority CT intelligence translation requirements, often within 24 hours. Language Analysts (LAs) also play a significant role in the FBI's CI and criminal investigative missions.

Intelligence Training

The FBI strives to ensure that its training programs leverage intelligence training expertise not only within the FBI, but also within the IC, academia, and industry to ensure the best intelligence training and educational opportunities are available to the FBI workforce. Such training also facilitates the identification of adjunct faculty, communicates relevant training and educational opportunities available outside the FBI and permits opportunities for research related to intelligence analysis. FBI Agents and IAs receive specialized training designed to better equip them with doctrine and tradecraft necessary to conduct the intelligence-driven mission of the FBI. Improving and expanding the FBI's training capacity will allow the FBI to conduct its intelligence-driven mission and to make a greater contribution to the United States Intelligence Community (USIC). In an effort to train the intelligence workforce and to build a cadre of highly skilled intelligence professionals, the FBI has developed three distinct career paths for Intelligence Analysts and is working to develop a competency-based career path for Special Agents. These career paths will ensure the FBI ICS personnel receive the training, experiences, and joint duty assignments appropriate for their position or stage of development. The FBI is re-designing its training curriculum to map to the career path to ensure that all ICS personnel have the training necessary to analyze and disrupt current and future threats to the U.S. Homeland.

Communications Exploitation Section (CXS)
The mission of the CXS is "to lead law enforcement and intelligence efforts in the U.S. to defeat terrorism by targeting terrorist communications."

Foreign Terrorist Tracking Task Force (FTTTF)
FTTTF assists in finding, tracking, and removing foreign terrorists and their supporters from the U.S. FTTTF utilizes specialized analytical techniques, technologies, and data access to enhance terrorist identification, tracking, and risk assessment operations.

Terrorist Screening Center (TSC)
The Terrorist Screening Center (TSC) is a multi-agency, multi-discipline, globally unique center which supports the FBI, Department of Justice (DOJ), ODNI, and the IC in their ability to detect, deter and disrupt national security threats through their counterterrorism, information and intelligence gathering/analysis/sharing national security missions. TSC accomplishes this through a unique interagency business model which incorporates information technology and information sharing, as well as operational and analytical expertise from interagency operational and IAs, Agents, and data/information technology (IT) analysts/specialists which support law enforcement at the federal, state, local, territorial, tribal, and international levels. The TSC has assisted law enforcement and screening agencies with the positive identification of 18,904 known or suspected terrorists (KST) domestically as well as globally in FY 2009 alone. Additionally, it has allowed FBI field offices to open 238 KST cases against targets which were previously unknown by the IC and law enforcement community to be present in the U.S..

Special Technologies and Applications Office (STAO)
The mission of STAO is to provide the FBI's investigative and intelligence priorities with technical analysis capability through innovative techniques, tools, and systems. STAO develops and maintains systems that store electronic data lawfully obtained or developed by the FBI and provides Agents, IAs, and linguists access to that data for the purpose of developing actionable information through the aid of analytic software applications.

Infrastructure and Technology
The IDU includes funding for several efforts that are critical enablers for FBI Intelligence Career Service (ICS) Agents, IAs, Language Analysts, and Physical Surveillance Specialists (PSSs). These efforts help to manage, process, share, and protect classified and unclassified information critical to national security. Taken together, these efforts form a comprehensive system of security and efficiency. The secure, or classified, side of the comprehensive system includes secure workspaces, or Sensitive Compartmented Information Facilities (SCIFs); a secure information sharing capability through the Sensitive Compartmented Information Operations Network (SCION), the FBI’s TOP SECRET (TS)/Sensitive Compartmented Information (SCI)-certified data network; and Intelligence IT, which are the tools used by FBI intelligence personnel to perform their duties. The unclassified side of the comprehensive system includes the FBI’s ability to share unclassified information with other federal, state, and local governments and other partners through the Criminal Justice Information Services’ Law Enforcement Online (LEO) system and UNet, the FBI’s unclassified connection to the Internet.

Sensitive Compartmented Information Facilities (SCIF)
A SCIF is an accredited, room, group of rooms, floors, or buildings where National Security Professionals (NSPs) collect, process, exploit, analyze, disseminate, and/or store Sensitive Compartmented Information. SCIFs are outfitted with Information Technology,

telecommunications, general office machines, and requisite infrastructure to process unclassified through Top Secret information. SCIFs are afforded intrusion detection and access control systems to prevent the entry of unauthorized personnel.

Sensitive Compartmented Information Operations Network (SCION)
SCION is a compartmented network for Top Secret information which is administered by employing increased security measures, enforcing user accountability, and enhancing information assurance methodology.

PERFORMANCE/RESOURCES TABLE

Decision Unit: Intelligence

DOJ Strategic Goal/Objective: Goal 1: Prevent Terrorism and Promote the Nation's Security (Objectives 1.1, 1.2, & 1.4) and Goal 2: Prevent Crime, Enforce Federal Laws, and Represent the Rights and Interests of the American People (Objectives 2.1-2.6)

WORKLOAD/ RESOURCES		Final Target		Actual		Projected		Changes		Requested (Total)	
		FY 2010		FY 2010		FY 2011 Continuing Resolution		Current Services Adjustments & FY2012 Program Changes		FY 2012 Request	
Total Costs and FTE		**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		6,455	1,606,025	6,025	1,210,237	6,394	1,526,146	302	67,243	6,696	1,593,389
TYPE / GOAL / STRATEGIC OBJECTIVE	**PERFORMANCE**	**FY 2010**		**FY 2010**		**FY 2011 Continuing Resolution**		**Current Services Adjustments & FY2012 Program Changes**		**FY 2012 Request**	
Performance Measure	% of Counterterrorism FISA collection reviewed by the Language Program: • Audio • Text • Electronic File		100% 100% 100%		95% 98% 39%		100% 100% 100%		-- -- --		100% 100% 100%
Performance Measure: *Responsiveness*	% of FBI *Headquarters* finished intelligence reports that are responsive to National Intelligence Priority Framework topics (Internally disseminated)		95%		98%		95%		--		95%
Performance Measure: *Responsiveness*	% of FBI *Field Office* finished intelligence reports that are responsive to National Intelligence Priority Framework topics. (Internally disseminated)		95%		98%		95%		--		95%
Performance Measure: *Responsiveness*	% of FBI finished intelligence reports that are responsive to National Intelligence Priority Framework topics. (Disseminated to Intelligence Community)		95%		99%		95%		--		95%
Performance Measure: *Accuracy*	Number of high priority sources put through an enhanced validation process.	This information is Classified.									
Efficiency Measure	% of FBI Confidential Human Sources (CHS) validated		25%		23%		22%		3%		25%

Data Definition, Validation, Verification, and Limitations:

- All data are provided by records maintained and verified by the FBI's Directorate of Intelligence. No known limitations exist with the available data as currently reported.

Performance Report and Performance Plan Targets		FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010		FY 2011	FY 2012
		Actual	Actual	Actual	Actual	Actual	Actual	Actual	Target	Actual	Target	Target
Performance Measure	% of Counterterrorism FISA collection reviewed by the Language Program: • Audio • Text • Electronic File	 N/A N/A N/A	 N/A N/A N/A	 94% 100% 99%	 88% 99% 94%	 97% 102% 95%	 91% 114% 57%	 85% 100% 87%	 100% 100% 100%	 95% 98% 39%	 100% 100% 100%	 100% 100% 100%
Performance Measure: *Responsiveness*	% of FBI *Headquarters* finished intelligence reports that are responsive to National Intelligence Priority Framework topics (Internally disseminated)	N/A	N/A	57%	86%	94%	100%	97%	95%	98%	95%	95%
Performance Measure: *Responsiveness*	% of FBI *Field Office* finished intelligence reports that are responsive to National Intelligence Priority Framework topics. (Internally disseminated)	N/A	N/A	58%	73%	90%	95%	100%	95%	98%	95%	95%
Performance Measure: *Responsiveness*	% of FBI finished intelligence reports that are responsive to National Intelligence Priority Framework topics. (Disseminated to Intelligence Community)	N/A	N/A	79%	86%	92%	100%	96%	95%	99%	95%	95%
Performance Measure: *Accuracy*	Number of high priority sources put through an enhanced validation process.	This information is Classified.										
Efficiency Measure	% of FBI Confidential Human Sources (CHS) validated	N/A	N/A	N/A	N/A	N/A	N/A	14%	25%	23%	22%	25%

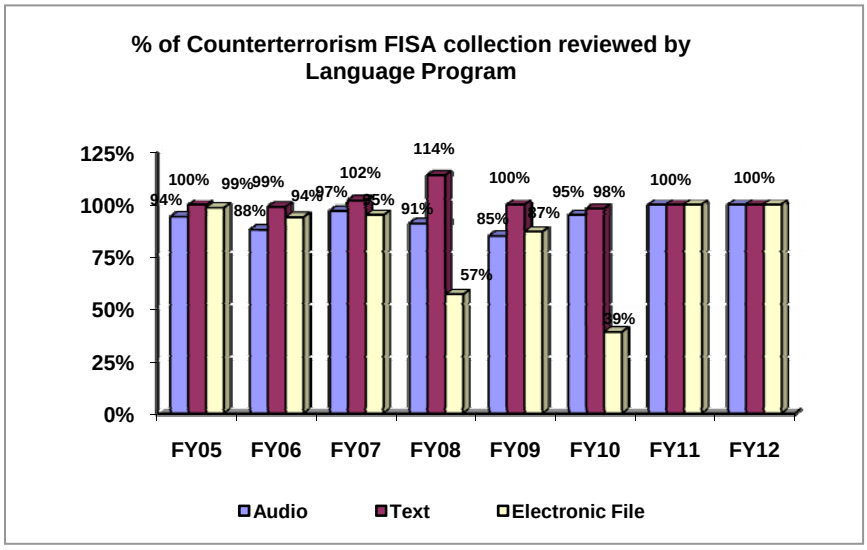
2. Performance, Resources, and Strategies

The IDU contributes to DOJ's first two Strategic Goals: Goal 1, "Prevent Terrorism and Promote the Nation's Security" (Objectives 1.1, 1.2, & 1.4) and Goal 2, "Prevent Crime, Enforce Federal Laws, and Represent the Rights and Interests of the American People" (Objectives 2.1-2.6). In addition, this decision unit ties directly to the FBI's ten priorities: Priority 1 – Protect the United States from terrorist attack; Priority 2 – Protect the United States against foreign intelligence operations and espionage; Priority 3 – protect the United States against cyber-based attacks and high-technology crimes; Priority 4 – Combat public corruption at all levels; Priority 5 – Protect civil rights; Priority 6 – Combat transnational and national criminal organizations and enterprises; Priority 7 – Combat major white-collar crime; Priority 8 – Combat significant violent crime; and Priority 9 – Support federal, state, local and international partners. Priority 10 – Upgrade technology to successfully perform the FBI's mission.

The mission of the Intelligence Program is to optimally position the FBI to meet current and emerging national security and criminal threats by aiming core investigative work proactively against threats to U.S. interests; building and sustaining enterprise-wide intelligence policies and capabilities; and providing useful, appropriate, and timely information and analysis to the national security, homeland security, and law enforcement communities. The DI is responsible for managing all projects and activities that encompass the FBI's Intelligence Program and for prioritizing those functions through the formulation of budgetary requirements. The Directorate carries out its functions through embedded intelligence elements at FBI HQ and in each field division.

a. Performance Plan and Report for Outcomes

Performance Measure: % of Counterterrorism Foreign Intelligence Surveillance Act (FISA) collection reviewed by the language program.



FY 2010 Target:
100% for Audio
100% for Text
100% for Electronic File

FY 2010 Actual:
95% for Audio
98% for Text
39% for Electronic File

Discussion: The Director of the FBI has established a goal of maintaining a review rate of 100% of all CT FISA collection. The FBI's Language Services program is striving to achieve this goal. Although we continually strive to reach the target, the FBI was unable to meet its 2010 targets for the following reasons: (1) There will always be some amount of work collected in languages for which there is a very low density of human resources available or in languages which have yet to be identified. (2) Work collected near the end of the reporting cycle may not be addressed within that cycle and will be carried over

to the next period. (3) Higher priority Non-FISA workload will pull resources away from FISA coverage on a temporary basis. (4) The FBI is developing numerous technological solutions to automatically examine collection content for potential intelligence information. However, until these tools are fully developed, tested, and deployed, the FBI's collection capabilities far exceed the FBI's capacity for review of by human means.

Specifically, a large percentage of the electronic data collected is meta data, spam, or junk and a great deal of effort is required to segregate this material from the material needing review. In addition, the FBI is working to address issues related to the accurate tracking of the level of data reviewed. Once these technical issues are resolved, more accurate review rates can be provided.

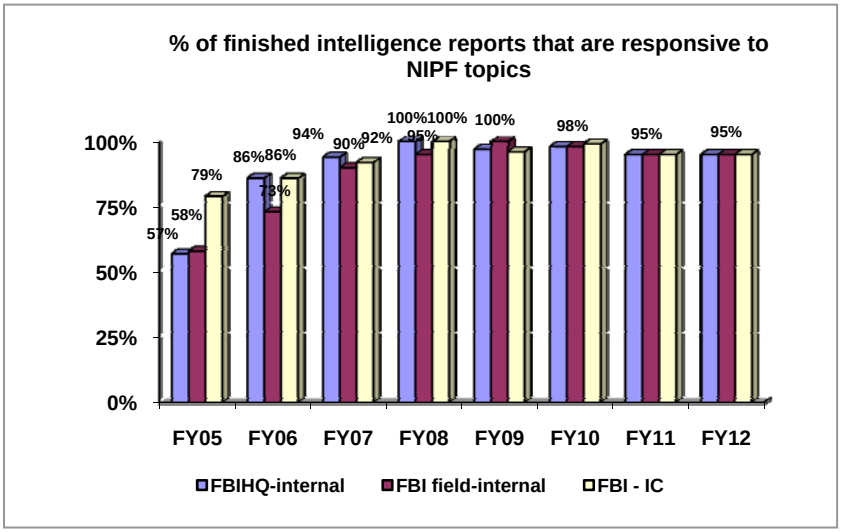
FY 2011 Target: 100% for Audio
100% for Text
100% for Electronic File

FY 2012 Target: 100% for Audio
100% for Text
100% for Electronic File

Performance Measure - Responsiveness: % of FBI Headquarters finished intelligence reports that are responsive to National Intelligence Priority Framework topics (Internally disseminated)

FY 2010 Target: 95%
FY 2010 Actual: 98%

Discussion: Target for FY12 remains the same as it has been analyzed to be a consistent probable goal for this measure. The FBI has a small number of Intel reports that do not respond to the NIPF, those specifically for domestic criminal activities.



FY 2011 Target: 95%
FY 2012 Target: 95%

Performance Measure - Responsiveness: % of FBI Field Office finished intelligence reports that are responsive to National Intelligence Priority Framework topics. (Internally disseminated)

FY 2010 Target: 95%
FY 2010 Actual: 98%

Discussion: See *Discussion* re: Reports responsive to NIPF topics, above.

FY 2011 Target: 95%
FY 2012 Target: 95%

Performance Measure - Responsiveness: % of FBI finished intelligence reports that are responsive to National Intelligence Priority Framework topics. (Disseminated to Intelligence Community)

FY 2010 Target: 95%
FY 2010 Actual: *99%*

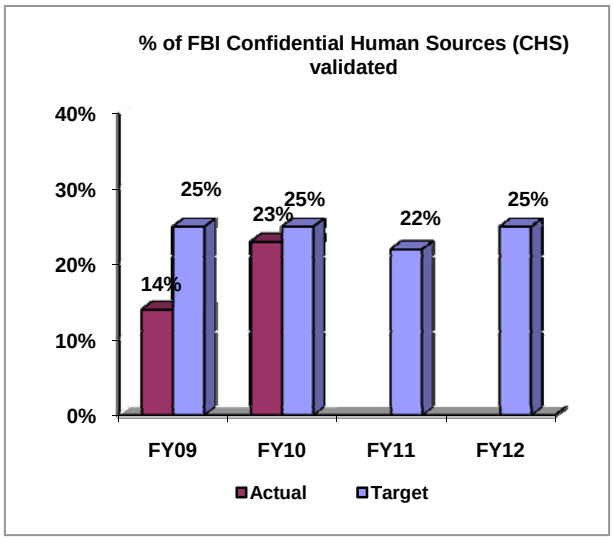
Discussion: See *Discussion* re: Reports responsive to NIPF topics, above.

FY 2011 Target: 95%
FY 2012 Target: 95%

Efficiency Measure: % of FBI Confidential Human Sources (CHS) validated

FY 2010 Target: 25%
FY 2010 Actual: 23%

Discussion: Because the number of CHSs is not static, it will be difficult for the HUMINT Validation Section to ever achieve 100% CHS validation. Higher priority or Special Category CHSs will always take precedence and be more time consuming than routine validations. Accordingly, this target has been adjusted based on trends over the last two years to more appropriately reflect realistic goals.



FY 2011 Target: 22%
FY 2012 Target: 25%

b. Strategies to Accomplish Outcomes

The FBI Intelligence Program was created by Congressional and Presidential mandate to provide centralized management of the Nation's domestic intelligence efforts; no other federal, state or local program shares the FBI's specific authorities and responsibilities for domestic intelligence collection. With respect to broader intelligence collection and analysis authorities, including foreign intelligence and counterintelligence, Executive Order 12333 governs the division of responsibility between FBI and other Intelligence Community members in order to ensure coordination and prevent duplication of effort. Managers of the Intelligence Program also work extensively with external partners to ensure that the FBI's program is not redundant or duplicative of other efforts, both public and private. In some instances, this involves the active co-location of groups so that activities and policies can be better coordinated. For example, many of the FBI's FIGs, which manage the FBI's intelligence functions in each Field Office, include members of state and local law enforcement and other intelligence agencies. The majority of

FIGs participate locally in working groups and analytic exchanges, which provide opportunity for coordination, collaboration and de-confliction. Additionally, FBI's Field Office personnel assigned to the FIGs are members of primary Fusion Centers, and work alongside members of state and local law enforcement and other intelligence community personnel. In other instances, special inter-agency committees have been created to allow senior leaders to monitor and minimize any redundancy between programs. The FBI Director or other senior managers sit on the Justice Intelligence Coordinating Council (JICC), GLOBAL Intelligence Working Group, and the National Intelligence Analysis and Production Board (NIAPB), just to name a few.

B. Counterterrorism/Counterintelligence Decision Unit

COUNTERTERRORISM/ COUNTERINTELLIGENCE DECISION UNIT TOTAL	Perm. Pos.	FTE	Amount ($000)
2010 Enacted with Rescissions	12,646	12,092	$3,156,342
2011 Continuing Resolution	12,682	12,163	3,175,894
Adjustments to Base and Technical Adjustments	4	320	73,551
2012 Current Services	12,686	12,483	3,249,445
2012 Program Increases	97	47	75,525
2012 Program Offsets	(6)	(6)	(21,445)
2012 Request	12,777	12,524	3,303,525
Total Change 2011-2012	**95**	**45**	**$150,132**

Counterterrorism/Counterintelligence Decision Unit —Information Technology Breakout	Perm. Pos.	FTE	Amount ($000)
2010 Enacted w/Rescissions and Supplementals	388	388	$379,768
2011 Continuing Resolution	405	405	381,339
Adjustments to Base and Technical Adjustments	8	8	(52,954)
2012 Current Services	413	413	328,385
2012 Program Increases	…	…	6,675
2012 Request	413	413	335,060
Total Change 2011-2012	**8**	**8**	**($46,279)**

1. Program Description

The FBI's Counterterrorism/Counterintelligence (CT/CI) Decision Unit is comprised of the Counterterrorism Program, the Weapons of Mass Destruction Directorate (WMDD), the Foreign Counterintelligence (FCI) Program, a portion of the Cyber Computer Intrusions Program, a portion of the Critical Incident Response Group, and the portion of the Legal Attaché (Legat) Program that supports the FBI's CT and CI missions. Additionally, to capture all resources that support these programs, a prorated share of resources from the FBI's support divisions (including Training, Laboratory, Security, Information Technology Operations, administrative divisions, and staff offices) is calculated and scored to the decision unit.

Counterterrorism Program

The mission of the FBI's CT program is to prevent, disrupt, and defeat terrorist operations before they occur; to pursue the appropriate sanctions for those who have conducted, aided, and abetted those engaged in terrorist acts; and to provide crisis management following acts of terrorism against the U.S. and U.S. interests. This mission is accomplished by gathering intelligence from all sources and using intelligence and analysis to enhance preventive efforts and exploit links between terrorist groups and their support networks. Threat information is shared with all affected agencies and personnel to create and maintain efficient threat mitigation response procedures and provide timely and accurate analysis to the Intelligence Community (IC) and senior policy makers.

The FBI is committed to stopping terrorism at any stage, from thwarting those intending to conduct an act of terrorism to investigating the financiers of terrorist operations. All CT

investigations are managed at FBI Headquarters, thereby employing and enhancing a national perspective that focuses on the CT strategy of creating an inhospitable terrorist environment.

The FBI aims to protect the U.S. from terrorist attacks by disrupting terrorists' ability to perpetrate harm. Training, finances, recruiting, logistical support, pre-attack planning, and preparation are all required components of terrorist operations. These requirements create vulnerabilities, and the FBI focuses on creating a comprehensive intelligence base to exploit these vulnerabilities.

To develop a comprehensive intelligence base, the FBI employs its Model Counterterrorism Investigative Strategy, focusing each terrorist case on intelligence, specifically on identification of terrorist training, fundraising, recruiting, logistical support, and pre-attack planning.

Under the leadership of Director Mueller, the FBI has moved aggressively to implement a comprehensive plan that has fundamentally transformed the FBI. The FBI has overhauled its counterterrorism operations, expanded its intelligence capabilities, modernized its business practices and technology, and improved coordination with its partners. The FBI is no longer content to concentrate on investigating terrorist crimes after they occur; it is dedicated to disrupting terrorist plots before they are executed. The FBI's CT Program has five priorities:

- To detect, disrupt, and dismantle terrorist sleeper cells in the U.S. before they act;
- To identify and prevent acts of terrorism by individuals with a terrorist agenda acting alone;
- To detect, disrupt, and dismantle terrorist support networks, including financial support networks;
- To enhance its capability to quickly ascertain the reliability, implications and details of terrorist threats and to improve the capacity to disseminate threat-related information to local, state, and federal agencies, and to the private sector as needed; and
- To enhance its overall contribution to the IC and senior policy makers in government by providing timely and accurate in-depth analysis of the terrorist threat and other information of value on an on-going basis.

To implement these priorities, the FBI has increased the number of Special Agents assigned to terrorism matters. The FBI has also established a number of operational units and entities that provide new or improved capabilities to address the terrorist threat. The National Joint Terrorism Task Force (NJTTF) and the around-the-clock Counterterrorism Watch manage and share threat information. The Terrorism Financing Operations Section centralizes efforts to stop terrorist financing. The FBI also utilizes document/media exploitation squads to exploit material found both domestically and overseas for its intelligence value. Deployable "Fly Teams" lend counterterrorism expertise wherever it is needed. The TSC and FTTTF[2] help identify terrorists and keep them out of the U.S.. Finally, the Counterterrorism Analysis Section "connects the dots" and assesses the indicators of terrorist activity against the U.S. from a strategic perspective.

Re-engineering efforts are making the FBI more efficient and more responsive to operational needs. The FBI has revised its approach to strategic planning and refocused recruiting and hiring efforts to attract individuals with skills critical to its counterterrorism and intelligence missions.

[2] Please note that while the TSC and the FTTTF are part of the FBI's CT Program, their resources are scored to the Intelligence Decision Unit.

The FBI has also developed a comprehensive training program and instituted new leadership initiatives to keep its workforce flexible.

The FBI has divided its CT operations into branches, each of which focuses on a different aspect of the current terrorism threat facing the U.S. These components are staffed with Special Agents, Intelligence Analysts, and subject matter experts who work closely with investigators in the field and integrate intelligence across component lines. This integration allows for real-time responses to threat information and quick communication with decision-makers and the field.

The FBI has also established strong working relationships with other members of the IC. From the Director's daily meetings with other IC executives, to the regular exchange of personnel among agencies, to joint efforts in specific investigations and in the National Counterterrorism Center (NCTC), the TSC, and other multi-agency entities, to the co-location of personnel at Liberty Crossing, the FBI and its partners in the IC are now integrated at virtually every level of operations.

With terrorists traveling, communicating, and planning attacks all around the world, coordination with foreign partners has become more critical than ever before. The FBI has steadily increased its overseas presence and now routinely deploys Special Agents and crime scene experts to assist in the investigation of overseas attacks. Their efforts have played a critical role in successful international operations.

FBI Headquarters CT management was responsible for a vital disruption of a plot to bomb U.S.-bound airplanes from the United Kingdom (U.K.) in July 2006. The experience of the CT Field Agents on 18-month temporary (TDY) assignments provided the critical workforce at FBI Headquarters that was needed to accomplish the intelligence-based investigations that detected and prevented recent terrorist acts from occurring against the U.S. and its interests. The disruption and arrests in the U.K. are a testament to the FBI's partnership with British intelligence.

Weapons of Mass Destruction (WMD) Directorate

The FBI realigned and consolidated existing WMD and counterproliferation initiatives, formerly managed in multiple divisions, under a single organizational entity, the WMD Directorate. The strategic focus of this Directorate is to prevent and disrupt the acquisition of WMD capabilities and technologies for use against the U.S. Homeland by terrorists and other adversaries, including nation-states. The WMD Directorate integrates and links all of the necessary counterterrorism, intelligence, counterintelligence, and scientific and technological components to accomplish the FBI's overall WMD mission. The WMD Directorate is organized to provide a mechanism to perform the following essential capabilities:

- Intelligence
- Countermeasures
- Preparedness
- Assessment and Response
- Investigative
- Science and Technology Support
- Policy and Planning

The WMD Directorate provides flexibility for growth and development and represents a flexible structure to leverage federal resources and coordinate with interagency partners. The Directorate addresses the identified essential capabilities through the establishment of three new sections which reside in the Directorate. These include: Countermeasures and Preparedness Section (CPS), Investigations and Operations Section (IOS), and Intelligence and Analysis Section (IAS). The WMD Directorate also has components to address policy, planning, budget, administrative, detailee matters and other functions which serve the entire Directorate. A joint reporting relationship with the Laboratory Division (LD) and the Critical Incident Response Group (CIRG) exists.

Dedicated Technical Program

The FBI's Dedicated Technical Program (DTP) administers resources to provide technical support as well as research and development activities through which the FBI ensures that investigative tools keep pace with evolving investigative requirements and private sector technologies. In compliance with Executive Order 12333 - United States Intelligence Activities and Director of National Intelligence (DNI) requests/guidance, the DTP deploys technical systems in support of foreign intelligence requirements of other IC entities. The DTP provides support enabling achievement of the following strategic goals:

- Identify, prevent, and defeat intelligence operations conducted by any foreign power within the U.S. or against certain U.S. interests abroad that constitute a threat to U.S. national security.
- Prevent, disrupt, and defeat terrorist operations.

Cyber Program

The FBI's Cyber Program consolidates Headquarters and field resources dedicated to combating cyber-crime under a single entity. This allows the Cyber Program to coordinate, supervise, and facilitate the FBI's investigation of those federal violations in which the Internet, computer systems, or networks are exploited as the principal instruments or targets of terrorist organizations, foreign government-sponsored intelligence operations, or criminal activity. Included under the purview of the Cyber Program are counterterrorism, counterintelligence and criminal computer intrusion investigations; intellectual property rights-related investigations involving theft of trade secrets and signals; copyright infringement investigations involving computer software; credit/debit card fraud where there is substantial Internet and online involvement; online fraud and related identity theft investigations; and the Innocent Images National Initiative.

Critical Incident Response Program

The Critical Incident Response Group (CIRG) facilitates the FBI's rapid response to, and management of, crisis incidents. CIRG was established to integrate tactical and investigative resources and expertise for incidents requiring an immediate law enforcement response. CIRG furnishes distinctive operational assistance and training to FBI field personnel as well as state, local, federal, tribal and international law enforcement partners. CIRG personnel are on call around the clock to respond to crisis incidents.

CIRG's continual readiness posture provides the U.S. Government with the ability to counter a myriad of CT/CI threats—from incidents involving WMD to a mass hostage taking. The FBI's crisis response protocols are built upon lessons learned from past incidents. They include a tiered response, streamlined command and control, standardized training, equipment, and

operating procedures, and coordination with other partners. To counter the range of potential crises, an integrated response package that brings command and control, aviation, and technical and tactical assets under a unified structure is essential; CIRG encompasses all of these elements.

CIRG also manages the FBI's mobile surveillance programs – the Special Operations Groups (SOGs) and the Special Surveillance Groups (SSGs) – and its Aviation Surveillance program. SOGs are comprised of armed agents and perform surveillances of targets that might have the propensity for violence; SSGs are comprised of unarmed investigative specialists and, therefore, do not surveil targets that may be violent. SOGs, SSGs, and Aviation Surveillance provide critical support to CT and CI investigations.

Legal Attaché (Legat) Program

Legats are the forward element of the FBI's international law enforcement effort and often provide the first response to crimes against the U.S. and its citizens that have an international nexus. The counterterrorism component of the Legat Program is comprised of Special Agents stationed overseas who work closely with their foreign counterparts to prevent terrorism from reaching into the U.S., help solve crimes, and assist with the apprehension of international terrorists who violate U.S. laws.

PERFORMANCE/RESOURCES TABLE

Decision Unit: Counterterrorism/Counterintelligence

DOJ Strategic Goal/Objective Goal 1: Prevent Terrorism and Promote the Nation's Security (Objectives 1.1, 1.2, & 1.4)

WORKLOAD/ RESOURCES		Final Target		Actual		Projected		Changes		Requested (Total)	
		FY 2010		FY 2010		FY 2011 Continuing Resolution		Current Services Adjustments & FY2012 Program Changes		FY 2012 Request	
Number of Cases: Counterterrorism, Counterintelligence, & Computer Intrusions		†		20,076		†		†		†	
Positive encounters with subjects through screening process		N/A		20,944		N/A		N/A		N/A	
Total Costs and FTE		**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		12,092	3,156,342	12,074	3,293,519	12,163	3,175,894	361	127,631	12,524	3,303,525
TYPE/ STRATEGIC OBJECTIVE	**PERFORMANCE**	**FY 2010**		**FY 2010**		**FY 2011 Continuing Resolution**		**Current Services Adjustments & FY2012 Program Changes**		**FY 2012 Request**	
Program Activity/ 1.1; 1.2	**1. Counterterrorism (CT)**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		7,501	1,957,887	7,486	2,041,982	6,933	1,810,260	80	56,208	7,013	1,866,468
Workload -- # of cases investigated (pending and received)		†		9,228		†		†		†	
Performance Measure (Revised Measure)	Catastrophic Acts of Terrorism	0		0		0		--		0	
Performance Measure	Number of participants in the JTTF	4,520		4,404		4,545		35		4,570	
Performance Measure (Renamed Measure)	Percentage of Counterterrorism Career Path Agents Completing Specialized CT Training	30%		47%		30%		0		30%	
Efficiency Measure (Renamed Measure)	Percentage of Counterterrorism Cases targeting Top Priority Groups	This information is Classified.									
Program Activity/ 1.4	**2. Counterintelligence**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		4,025	1,050,745	3,984	1,086,861	4,257	1,111,563	252	62,103	4,509	1,173,666
Workload -- # of cases investigated (pending and received)		This information is Classified.									
Performance Measure	Percentage of offices that have sufficiently identified Foreign Intelligence Service (FIS) activities	This information is Classified.									
Performance Measure	Percentage of field offices with adequate coverage of known or suspected intelligence officers	This information is Classified.									
Performance Measure	Percentage of field offices satisfactorily engaged in strategic partnerships with other USIC entities	This information is Classified.									

PERFORMANCE/RESOURCES TABLE										
Decision Unit: Counterterrorism/Counterintelligence										
DOJ Strategic Goal/Objective Goal 1: Prevent Terrorism and Promote the Nation's Security (Objectives 1.1, 1.2, & 1.4)										
Performance Measure	Percentage of field offices that have satisfactorily demonstrated knowledge of and liaison with vulnerable entities within their domain	This information is Classified.								
Performance Measure	Percentage of field offices that have identified and documented priority threat country operations	This information is Classified.								
Efficiency Measure	Cost savings through the Interactive Multimedia Instruction and Simulation Program ($000) (discontinued measure)	4,500		5126		N/A		N/A		N/A
Efficiency Measure	Cost savings/ efficiencies through the Lookout Program (new measure)	N/A		N/A		$319,730		($148,998)		$170,732
Program Activity/ 1.1	**3. Cyber Program (Intrusions)**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		This information is Classified.								
Workload -- # of cases investigated (pending and received)		†		2,975		†		†		†
Performance Measure	Number of Priority Criminal Computer Intrusion Investigations Successfully Satisfied	33		34		35		0		35
Efficiency Measure	Cost savings from online Cyber training ($000)	596		819		625		531		1,156
Performance Measure	Computer Intrusion Program Convictions/Pre-trial diversions	††		134		††		††		††

PERFORMANCE/RESOURCES TABLE

Decision Unit: Counterterrorism/Counterintelligence

DOJ Strategic Goal/Objective Goal 1: Prevent Terrorism and Promote the Nation's Security (Objectives 1.1, 1.2, & 1.4)

Data Definition, Validation, Verification, and Limitations:

- "Terrorist "acts," domestic or internationally-based, count 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. The FBI uses the term terrorist incident to describe the overall concerted terrorist attack. A terrorist incident may consist of multiple terrorist acts. For the purposes of these performance data, a catastrophic terrorist act is defined as an act resulting in significant loss of life and/or significant property damage (e.g., each of the individual attacks that took place on September 11, 2001, the attack on the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma on April 19, 1995)."- Other Counterterrorism measures are provided through records kept by the FBI's Counterterrorism Program, including the Terrorist Screening Center. The count of JTTF participants erroneously did not include part-time participants until FY 2008, but will henceforth include them. No other known data limitations exist.- Counterintelligence measures are based on records kept by the FBI's Counterintelligence Program. These records are based upon the results of field reviews of CI squads done on a periodic basis. Since the end of March 2007, all FBI field offices have undergone at least one CI field review. Percentages are updated based upon the most recent field review. IMIS cost savings data are based upon estimates of cost savings per student taking an online course, compared with an in-service training. During FY 2009, contracting delays will affect the extent to which all field offices can reviewed for up-to-date data.- The data source for successful computer intrusion cases and conviction/pre-trial diversion data is the FBI's Integrated Statistical Reporting and Analysis Application (ISRAA) database. The database tracks statistical accomplishments from inception to closure. Before data are entered into the system, they are reviewed and approved by an FBI field manager. They are subsequently verified through FBI's inspection process. Inspections occur on a two to three year cycle. Using statistical sampling methods, data in ISRAA are tracked back to source documents contained in FBI files. FBI field personnel are required to enter accomplishment data within 30 days of the accomplishment or a change in the status of an accomplishment, such as those resulting from appeals. Data for this report are compiled less than 30 days after the end of the fiscal year, and thus may not fully represent the accomplishments during the reporting period. Previous data subject to this limitation were revised during FY 2005.- Data for the cost savings for Cyber training are maintained by the Cyber Education and Development Unit. These data are based on estimated cost savings for each student taking an online course compared to in-service training. No known data limitations exist.
- Data compiled by the TSC for the number of positive encounters with subjects through the screening process are accurate as of the date of this report. However, these data can be revised at a later date as additional information prompts TSC to revise its finding on any individual reviewed.

† Due to the large number of external and uncontrollable factors influencing these data, the FBI does not project numbers of cases.

†† FBI does not set targets for investigative output data.

Performance Report and Performance Plan Targets		FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010		FY 2011	FY 2012
		Actual	Actual	Actual	Actual	Actual	Actual	Actual	Target	Actual	Target	Target
Performance Measure (Revised Measure)	Catastrophic Acts of Terrorism	0	0	0	0	0	0	0	0	0	0	0
Performance Measure	Positive encounters with subjects through screening process	N/A	5,396	15,730	19,967	20,500	19,306	19,043	N/A	20,944	N/A	N/A
Performance Measure	Increase the number of participants in the JTTF	2,394	3,163	3,714	3,540	3,600	4,163	4,597	4,520	4,404	4,545	4,570
Performance Measure (Renamed Measure)	Percentage of Counterterrorism Career Path Agents Completing Specialized CT Training	3%	10%	15%	74%	77%	80%	92%	30%	47%	30%	30%
Efficiency Measure (Renamed Measure)	Percentage of Counterterrorism Cases targeting Top Priority Groups	15%	35%	34%	33%	34%	44%	45%	62.6%	62.3%	65.1%	65.1%
Performance Measure	Percentage of offices that have sufficiently identified Foreign Intelligence Service (FIS) activities	This information is Classified.										
Performance Measure	Percentage of field offices with adequate coverage of known or suspected intelligence officers	This information is Classified.										
Performance Measure	Percentage of field offices satisfactorily engaged in strategic partnerships with other USIC entities	This information is Classified.										
Performance Measure	Percentage of field offices that have satisfactorily demonstrated knowledge of and liaison with vulnerable entities within their domain	This information is Classified.										
Performance Measure	Percentage of field offices that have identified and documented priority threat country operations	This information is Classified.										
Efficiency Measure	Cost savings through the Interactive Multimedia Instruction and Simulation Program ($000)	272	706	1,210	2,746	4,388	3,871	5,786	4,500	5,126	N/A	N/A
Performance Measure	Number of Priority Criminal Computer Intrusion Investigations Successfully Satisfied	N/A	N/A	34	24	27	31	24	33	34	35	35
Efficiency Measure	Cost savings from online Cyber training ($000)	N/A	N/A	N/A	N/A	331	511	809	596	819	625	1,156
Performance Measure	Computer Intrusion Program Convictions/Pre-trial diversions ** Historical data for this measure have been revised – see measure description.*	95*	88*	104*	120*	102*	126*	142	N/A	134	N/A	N/A

2. Performance, Resources, and Strategies

The Counterterrorism/Counterintelligence decision unit contributes to the Department's Strategic Goal 1: Prevent Terrorism and Promote the Nation's Security, Objectives 1.1, 1.2, & 1.4. This decision unit also ties directly to the top three FBI priorities: Priority 1 – Protect the United States from terrorist attacks; Priority 2 – Protect the United States against foreign intelligence operations and espionage; and Priority 3 – Protect the United States against cyber-based attacks and high-technology crimes.

Counterterrorism

a. Performance Plan and Report for Outcomes

The FBI is committed to stopping terrorism at any stage, from thwarting those intending to conduct an act of terrorism to investigating the financiers of terrorist operations. All CT investigations are managed at FBI Headquarters, thereby employing and enhancing a national perspective that focuses on the strategy of creating an inhospitable environment for terrorists. As the leader of the Nation's CT efforts, the FBI must understand all dimensions of the threats facing the Nation and address them with new and innovative investigative and operational strategies. The FBI must be able to effectively respond to the challenges posed by unconventional terrorist methods, such as the use of chemical, biological, radiological, explosive, and nuclear materials. When terrorist acts do occur, the FBI must rapidly identify, locate, and apprehend the perpetrators and their affiliates. As part of its CT mission, the FBI will continue to combat terrorism by investigating those persons and countries that finance terrorist acts.

Under the leadership of Director Mueller, the FBI has moved aggressively to implement a comprehensive plan that has fundamentally transformed the FBI. The FBI has overhauled its CT operations, expanded its intelligence capabilities, modernized its business practices and technology, and improved coordination with its partners. The FBI is no longer content to concentrate on investigating terrorist crimes after they occur; it is dedicated to disrupting terrorist plots before they are executed.

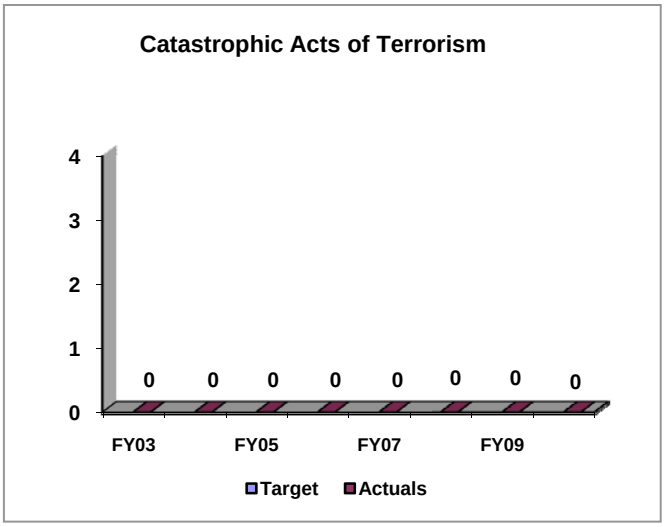
The FBI has also established strong working relationships with other members of the Intelligence Community (IC). From the FBI Director's daily meetings with other IC executives, to regular exchange of personnel among agencies, to joint efforts in specific investigations and in the National Counterterrorism Center, the Terrorist Screening Center, and other multi-agency entities, to the co-location of personnel at Liberty Crossing, the FBI and its partners in the IC are now integrated at virtually every level of operations.

Performance Measure: Catastrophic acts of terrorism

FY 2010 Target: Zero terrorist acts.
FY 2010 Actual: Zero terrorist acts.

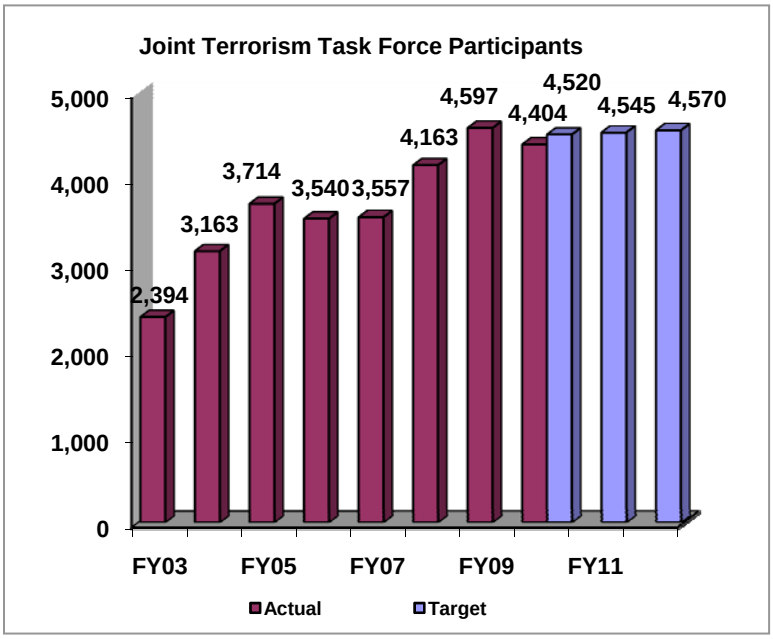
Discussion: This measure includes both international and domestic terrorist acts. This measure is being phased out in conjunction with the HPPG process and the development of new CT-related measures.

FY 2011 Target: N/A
FY 2012 Target: N/A



Performance Measure: Number of participants in the Joint Terrorism Task Force.

FY 2010 Target: 4,520
FY 2010 Actual: 4,404



Discussion: The FBI's Joint Terrorism Task Force participants serve as the "operational arm" of the U.S. Government's domestic Counterterrorism strategy. The partnership between FBI special agents and intelligence analysts with hundreds of investigators from federal, state, and local agencies across the country creates an important force multiplier in the fight against terrorism. The JTTF is focused on maximizing cooperation between these agencies, and consists of cohesive units with full and part-time Federal, state, and local officers who operate in concert with intelligence community assets.

During FY 2010, the number of JTTF participants declined by 4.2 percent, to 4,404. At the end of 1st quarter FY10, there were 4,591 JTTF members. Since then, full-time JTTF participation has declined by 51 Federal, state, and local members; part-time JTTF participation has declined by 218 Federal, state, and local members. Meanwhile, the FBI's participation increased by 82 full- and part-time members. Because JTTF participation comes at a great manpower staffing cost, partner agencies are likely to pull back detailees from JTTFs due to current and future budgetary constraints.

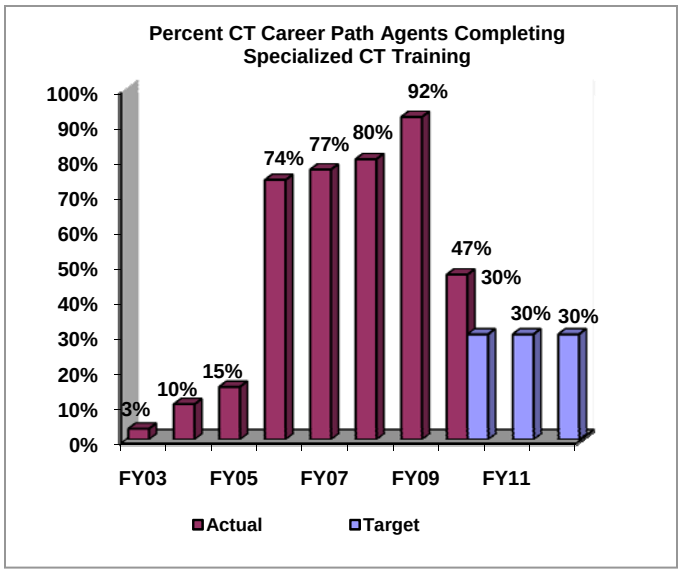
Additionally, during FY 2010 the National Joint Terrorism Task Force (NJTTF) conducted a review of the JTTF national roster and found that liaison members had been captured as part-time members by JTTFs. To eliminate this practice, the NJTTF provided guidance and criteria for Task Force Officer (TFO) membership designation. A new database was introduced to track JTTF members, coupled with a stricter adherence to membership designation guidance, to ensure that only full-time and part-time participation is captured for JTTF statistical reporting.

The JTTF membership estimates for FY 2011 and FY 2012 reflect the current climate, with a modest 0.5 percent increase each fiscal year.

FY 2011 Target: 4,545
FY 2012 Target: 4,570

Performance Measure: RENAMED MEASURE: Percentage of Counterterrorism Career Path Agents completing specialized CT training *(formerly named "Percent of CTD personnel having completed competency profile training").*

FY 2010 Target: 30%
FY 2010 Actual: 47%



Discussion: Based on the change in this measure, the FY 2010 and FY 2011 Targets are being adjusted down from 85% to 30%. The FY 2012 target is also 30%.

Approximately 720 CT Special Agents have received Career Path Training that is necessary for CT Career Path competency and is mandated by the Counterterrorism Division and the Continuing Education and Professional Development Unit (CEPDU). At this time, only the Counterterrorism Investigation and Operations (CTIOPS) courses are mandatory. As CT courses are developed in sufficient frequency and size, additional courses will become mandatory for CT Career Path competency.

Approximately 2,050 Special Agents are currently in the CT Career Path. This includes all non-managerial CT-designated SAs upon graduation from the FBI Academy or after transferring from another career path; up until their advancement into management, their transfer to another career path, or their departure from the FBI. The 720 Career Path-trained SAs represent 30% of the total CT Special Agent population of 2,050.

Data used as a basis for the percentage is not a static number, as new untrained, non-CT-competent Special Agents are added to the CT career path population every two weeks in conjunction with the graduation of each New Agents Class. Another fluctuation of the data occurs after an iteration of a mandatory CT Career Path course. Additionally, these

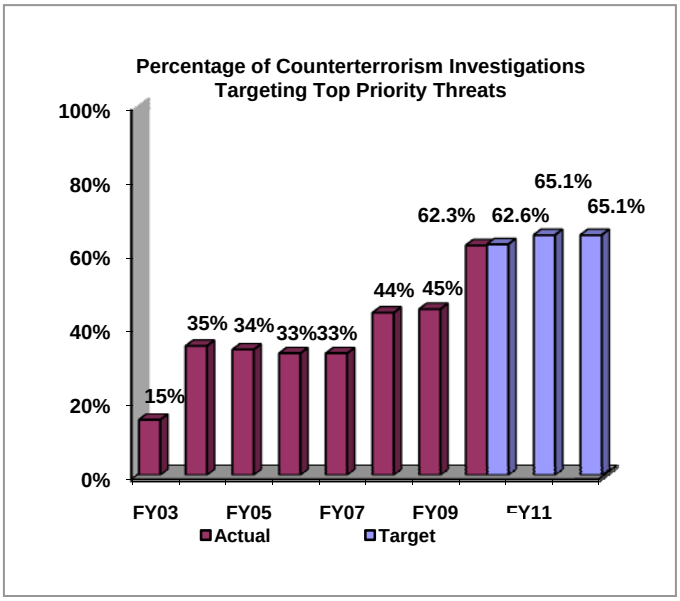
numbers are affected by the ebb and flow of CT-competent and non-CT-competent Special Agents who transfer between Career Paths. Further, career path competency will increase yearly with the continuation of developed and implemented mandatory CT training, and with the loss of senior CT Special Agents who were assigned to the CT Career Path prior to the establishment of a formal CT training program through movement into management and basic attrition.

FY 2011 Target: 30%
FY 2012 Target: 30%

Efficiency Measure: Percentage of Counterterrorism investigations targeting Top Priority Threats

FY 2010 Target: 62.6%
FY 2010 Actual: 62.3%

Discussion: In March 2010, in conjunction with the development of DOJ's National Security High-Priority Performance Goal (HPPG), the FBI's Counterterrorism Division (CTD) refined the methodology for calculating this measure, to align with CTD's new case classifications created at the end of FY 2009 and to better reflect international terrorist threats as defined by the intelligence community.



This measure accounts for top priority terrorist groups for both domestic and international terrorism. "Top Priority Threats" for international terrorism (IT) are defined as all priority one groups from the National Intelligence Priority Framework (NIPF), which is a list maintained by the Interagency Intelligence Committee on Terrorism (IICT). This list establishes the USIC standard for IT targets. For domestic terrorism (DT), "Top Priority Threats" are defined as the top priority groups from the FBI's DT Program National Priorities. Unlike IT, there is no prioritization standard across federal agencies that can be applied to DT cases.

As mandated by DOJ's National Security HPPG, the FBI is working to increase the percentage of counterterrorism investigations targeting top priority threats by five percent by the end of FY 2011. Following the revised methodology for this measure, at the end of FY 2009, 60.1 percent of CT investigations targeted top priority threats. This measure's targets for FY 2010 and FY 2011 have been revised accordingly.

At the end of 3rd quarter FY 2010, 62.7 percent of the FBI's CT investigations targeted top priority threats. Although this figure declined during the fourth quarter, the FBI is on track to meet its target for FY 2011. The FBI investigates all counter-terrorism leads to the fullest extent. Many leads create investigations that may not target top priority threats.

FY 2011 Target: 65.1%
FY 2012 Target: 65.1%

b. Strategies to Accomplish Outcomes

As the leader of the Nation's counterterrorism efforts, the FBI must understand all dimensions of the threats facing the Nation and address them with new and innovative investigative and operational strategies. The FY 2012 budget request will continue to directly address these threats and assists in pursuing the FBI's missions and objectives. The FBI must be able to effectively respond to the challenges posed by unconventional terrorist methods, such as the use of chemical, biological, radiological, explosive, and nuclear materials. When terrorist acts do occur, the FBI must rapidly identify, locate, apprehend, and prosecute those responsible. As part of its counterterrorism mission, the FBI will continue to combat terrorism by investigating those persons and countries that finance terrorist acts. The FBI will aggressively use the money laundering and asset forfeiture statutes to locate and disrupt the financial sources of terrorist organizations. The FBI will also work to effectively and efficiently utilize the tools authorized by Congress. While the ultimate goal is to prevent a terrorist act before it occurs, the FBI must be able to respond should an act occur. The FBI's efforts in this area include improved intelligence gathering and sharing, improved analytical capabilities, and enhanced training and liaison.

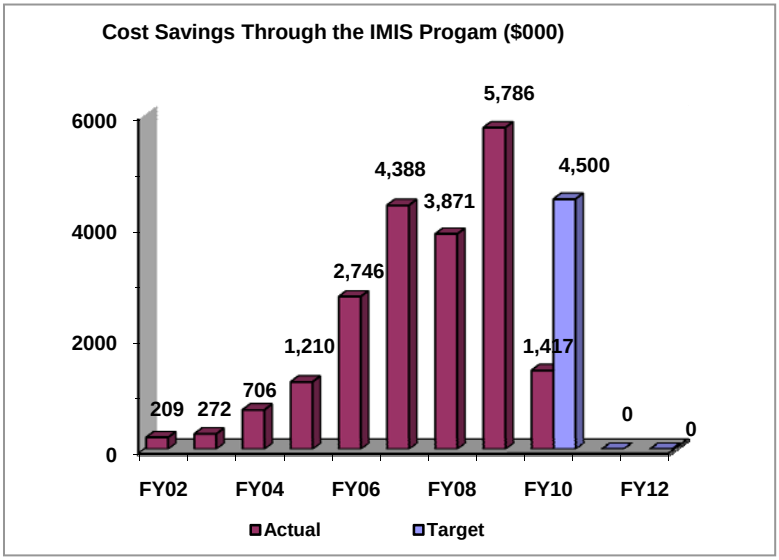
Counterintelligence

a. Performance Plan and Report for Outcomes

In FY 2005, the FBI Counterintelligence (CI) Program initiated an assessment of its performance measurements in conjunction with a program review performed by OMB. As a result of these reviews, the FBI adopted, developed, and implemented several program-level performance measures based on periodic reviews of field operations conducted by the CI Program. As of December 31, 2010, all 56 FBI field offices completed the first phase (Phase I) of CI program reviews, and 50 field offices, 89 percent, completed the second phase (Phase II) of reviews. As each FBI field office finalizes Phase II and some cases Phase III reviews, the CI Program updates performance result data to evaluate overall program efficiency and productivity.

The CI Program conducts on-site reviews of FBI field offices to determine how offices comprehend and manage their domain, identify existing performance gaps, and provide best practices or targeted recommendations that specifically address an individual field office's requirements. These reviews serve as the foundation for compiling various Counterintelligence performance outputs and results. Due to the cyclical nature of the program reviews, performance results and percentages reported in this narrative include ratings from some field offices that completed Phase I program reviews only. Until Phase II reviews are completed for all 56 field offices, Phase I and II results were combined to report performance outcomes across all CI field office programs.

Efficiency Measure: Cost savings through the Interactive Multimedia Instruction and Simulation (IMIS) Program ($000)



FY 2010 Target: 4,500
FY 2010 Actual: 1,417

Discussion: Cost savings based upon number of students completing online course, compared to costs incurred from traveling to attend in-service platform instruction. In FY 2010, the FBI used computer-based training that enabled more personnel to be trained at a reduced cost; and resulting in improved performance across all program strategy measures.

In FY 2011, the FBI intends to terminate this measure and replace it with a new one based on technological efficiencies identified within the Counterintelligence Division's Lookout Program.

FY 2011 Target: N/A (This measure is being replaced with the measure below).
FY 2012 Target: N/A

b. Strategies to Accomplish Outcomes

The FBI's Counterintelligence (CI) Program continues to execute a comprehensive National Strategy for Counterintelligence. This strategy is predicated on the need for centralized national direction that facilitates a focus on common priorities and specific objectives in all areas of the country. It also recognizes the need for collaboration and strategic partnerships both within the U.S. Intelligence Community as well as within the Business and Academic sectors. This strategy enables the program to combat effectively the intelligence threats facing the U.S. The FBI needs to maintain its current resources directed against the CI symmetrical threat, while concurrently obtaining resource enhancements to deploy against the CI asymmetrical threat throughout the CI domain field-wide.

<u>Computer Intrusions</u>

a. Performance Plan and Report for Outcomes

The Computer Intrusion Program (CIP) is the top priority of the FBI's Cyber Division. The mission of the CIP is to identify, assess and neutralize computer intrusion threats emanating from terrorist organizations, state sponsored threat actors, and criminal groups targeting the national information infrastructure.