|  |
| --- |
| **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 1-1**

**II. Summary of Program Changes 2-1**

**III. Appropriations Language and Analysis of Appropriations Language 3-1**

**IV. Decision Unit Justification 4-1**

A. Intelligence Decision Unit 4-1

1. Program Description

2. Performance Tables

3. Performance, Resources, and Strategies

B. Counterterrorism/Counterintelligence Decision Unit 4-12

1. Program Description

2. Performance Tables

3. Performance, Resources, and Strategies

C. Criminal Enterprises Federal Crimes Decision Unit 4-30

1. Program Description

2. Performance Tables

3. Performance, Resources, and Strategies

D. Criminal Justice Services Decision Unit 4-53

1. Program Description

2. Performance Tables

3. Performance, Resources, and Strategies

**V. Program Increases by Item 5-1**

Computer Intrusions 5-1

National Security 5-6

Electronic Surveillance Capabilities 5-7

Weapons of Mass Destruction/Render Safe Capabilities 5-10

Operational Enablers 5-14

Violent Crime in Indian Country 5-17

**VI. Program Offsets by Item 6-1**

Administrative Efficiencies 6-1

Extend Tech Refresh 6-3

Headquarters/Field Cost Module Reduction 6-5

Lookout Program Efficiencies 6-7

Network and Intrusion Analysis 6-9

Reduce Physical Footprint 6-11

Relocation Program 6-14

Sentinel 6-16

Task Force Consolidation 6-18

**VII. Exhibits 7-1**

A. Organizational Chart

B. Summary of Requirements

C. Program Increases/Offsets by Decision Unit

D. Resources by DOJ Strategic Goal/Objective

E. Justification for Base Adjustments

F. Crosswalk of 2010 Availability

G. Crosswalk of 2011 Availability

H. Summary of Reimbursable Resources  
I. Detail of Permanent Positions by Category

J. Financial Analysis of Program Increases/Offsets

K. Summary of Requirements by Grade

L. Summary of Requirements by Object Class

M. (Not Required)

N. (Not Required)

O. (Not Required)

**VIII. Construction 8-1**

**Program Offsets** 8-1

Secure Work Environment Program Reduction 8-1

**Exhibits**

A. Appropriations Language and Analysis of Appropriations Language

B. Summary of Requirements

D. Resources by DOJ Strategic Goal/Objective

E. (Not Required)

F. Crosswalk of 2010 Availability

G. Crosswalk of 2011 Availability

L. Summary of Requirements by Object Class

**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 implemented process is a significant insider trading scheme that is now under investigation.

Corporate fraud, along with securities fraud, remains a high priority of the FBI Financial Crimes Section and the FBI is committed to the dealing with the significant crime problem. Since 2001, FBI special agent resources dedicated to corporate and securities fraud has increased 84 percent (177 to 326 agents) while the caseload has increased at roughly the same pace (1,263 to 2,320 cases) during that time period. The return on investment for these resources is significant: since 2001, the FBI averages 281 arrests, 477 informations and indictments, and 461 convictions per year. These cases have resulted in billions of dollars in recoveries, restitutions, asset forfeitures, and seizures. In FY 2009, the FBI realized $8.2 billion in restitutions and recoveries from corporate/securities fraud matters, an average of $28.6 million per agent utilized. The average FBI jail sentence for corporate/securities fraud has risen every year since 2007 and currently stands at 63 months. Average time to sentencing continues to climb as well, however, due to the increasingly sophisticated nature of these schemes, and currently stands at 43 months per case.

* Mortgage Fraud, and Other Financial Institution Fraud: Mortgage fraud, a subset of financial institution fraud, continues to absorb considerable FBI resources while showing no signs of subsidence. By the 4th Quarter of FY 2010, over 71 percent of the FBI’s 3,029 mortgage fraud cases involved losses exceeding $1 million per case. If first quarter trends continue, the FBI will receive over 75,000 SARs in FY 2011. FBI intelligence and industry sources such as the Mortgage Asset Research Institute (MARI) and recent reports by the Special Inspector General of the Troubled Asset Relief Program (SIGTARP) predict an increase in foreclosures, financial institutions/firms failures, regulatory agency/independent auditor fraud referrals and governmental housing relief fraud.

The majority of FBI Mortgage Fraud cases are broken into three types of schemes:

* + Loan Origination Schemes. Borrowers and real estate insiders provide false financial information and documentation as part of the loan application package and false appraisals.
  + Illegal property-flipping occurs when a property is resold for a profit at an artificially inflated price shortly after being acquired by the seller. The key to this scheme is the fraudulent appraisal.
  + Builders employ bailout schemes to offset losses and circumvent excessive debt and potential bankruptcy as home sales suffer from escalating foreclosures, rising inventory, and declining demand. One type of Builder Bail-Out Scheme is the Condo Conversion. Builders entice individuals into purchasing the excess inventory by offering excessive incentives to buyers, including cash back at close, prepayment of homeowner association dues and other fees, and significant upgrades, all of which are undisclosed to the lender. The perpetrators artificially inflate the value of the condo to offset the cost of these incentives.

Commercial Real Estate (CRE) fraud is another emerging threat:

* + Continued defaults with the declining market are exposing CRE fraud. There are approximately $1.4 trillion CRE loans outstanding. An estimated 50 percent of these loans are projected to be “underwater,” meaning the collateral is worth less than the amount owed on the loan. An estimated nine percent of CRE loans are now delinquent; double the number from a year ago.[[1]](#footnote-1)
  + All economic indicators point to a CRE crisis which would cause billions of dollars in losses to financial institutions, and result in or contribute to the failure of numerous financial institutions.

The FBI is using an intelligence-driven approach to combat mortgage fraud, including:

* + Establishment of the Financial Intelligence Center (FIC), which is issuing targeting packages that focus on the most egregious offenders.
  + Formation of 23 Mortgage Fraud Task Forces in high-risk areas.
  + Proactive Undercover Operations and human source penetration.
  + “Fast Track” approach to identify targets, approach quickly, and obtain cooperation.
  + Analytical tools such as the Property Flip database and an enhanced SAR review process.

Since 2007, the FBI has tripled Special Agent and Intelligence Analyst resources investigating mortgage fraud. The average mortgage fraud case time prior to sentencing was 46 months in FY 2009 and is 43 months so far in FY 2010, indicating that these cases are highly complex and resource intensive. The average jail sentence has increased by 60 percent since FY 2007, from 23 months to 37 months, indicating the FBI is working quality cases and targeting the most egregious offenders. The return on investment (ROI) for each Special Agent utilized in FY 2009 was $8.5 million (based on Recoveries & Restitutions per agent). This figure doesn’t include Asset Forfeitures and Seizures or Fines, which account for millions more in aggregate each year.

* Health Care Fraud: Total health care expenditures in the U.S. will surpass the $4 trillion mark by 2015, representing a 139 percent increase or more than double the $1.67 trillion in expenditures for 2003. This creates an environment prevalent to fraud, as the National Health Care Anti-Fraud Association (NHCAA) estimates conservatively that 3 to 5 percent of total health care expenses are fraudulent, resulting in an estimated $60-$100 billion in health care losses. The independent National Insurance Crime Bureau (NICB) estimates that health care fraud exceeds $130 billion annually.

Today, the FBI seeks to infiltrate illicit operation and terminate scams involving staged auto accidents, online pharmacies, Durable Medical Equipment, outpatient surgery centers, counterfeit pharmaceuticals, nursing homes, hospital chains, and transportation services. Besides the federal health benefit programs of Medicare and Medicaid, private insurance programs lose billions of dollars each year to blatant fraud schemes in every sector of the industry.

Despite a drop of 13 percent in health care fraud cases since 2001 (FY 2001: 2,870; FY 2009: 2,494), the average jail sentence has nearly doubled during that timeframe, from 16 to 30 months, illustrating that the FBI is targeting the worst offenders. Meanwhile, health care fraud cases prove to be extremely resource intensive as average time to sentencing was 49 months per health care fraud case in FY 2009.

* Money Laundering: Money Laundering allows criminals to infuse illegal money into the stream of commerce, thus corrupting financial institutions and the money supply; this provides the criminals with unwarranted economic power. The FBI investigates money laundering cases by identifying the process by which criminals conceal or disguise the proceeds of their crimes or convert those proceeds into goods and services. The major threats in this area stem from emerging technologies, such as stored value devices, pre-paid gift cards, and reloadable debit cards, which are used to move criminal proceeds. Shell corporations are used as well to conceal the ownership of funds being moved through financial institutions and international commerce. This has created a “shadow” banking system, allowing criminals to exploit existing vulnerabilities in the reporting requirements that are imposed on financial institutions and international travelers.

At the end of FY 2009, the FBI had 350 open money laundering investigations, yet money laundering violations occur across all programs – from counterterrorism to organized crime to gangs – and are contained as pieces of higher priority investigations.

Money laundering convictions in FY 2009 were up 22 percent as compared to FY 2001, despite having 50 percent less Special Agent resources.

* Other Complex Financial Crimes (Insurance, Bankruptcy, and Mass Marketing Fraud): According to the Coalition Against Insurance Fraud (CAIF), insurance fraud costs Americans approximately $80 billion a year, or nearly $950 per family. In the first half of 2009, The National Insurance Crime Bureau (NICB) experienced a 16 percent increase in questionable non-health care insurance claims over the same timeframe in 2008. The FBI anticipates insurance fraud to continue to increase, contributing to increases in insurance premiums as well as threatening the financial viability of insurance companies.

Since 2006, the year after bankruptcy laws were changed to make it more difficult for an individual to discharge all debts, bankruptcy filings have significantly increased each year. The potential for fraud within bankruptcy is large. According to the most recent data, there will be over 1.4 million bankruptcy filings in 2009.

According to the Federal Trade Commission, complaints concerning mass marketing fraud have also increased. In 2000, there were 111,255 complaints, while in 2008 the FBI received over 643,195 complaints.

***Gang Violence:*** Violent street gangs operate in communities of all sizes: urban, suburban and rural areas across the country. According to law enforcement officials throughout the Nation, criminal gangs commit as much as 80 percent of the crime in our communities. FBI Violent Gang Safe Streets Task Forces (VGSSTFs) report that violent street gangs, whether they are neighborhood based or national gangs, are a top threat to our communities followed by prison gangs and outlaw motorcycle gangs. The Department of Justice (DOJ) and the National Gang Intelligence Center's (NGIC) 2009 Gang Threat Assessment estimates there were 20,000 U.S. based gangs criminally active with total gang membership at approximately 1,000,000 members. Further, based on National Drug Threat Survey (NDTS) data, the NGIC Assessment indicates that 48 to 60 percent of state and local law enforcement agencies reported that criminal gangs were active in their jurisdictions. This statistic shows that gang activity poses a threat to our domestic security each year.

Gangs continue to proliferate and commit violent crime. NGIC identified a trend whereby gang members are expanding to suburban and rural areas. This migration is believed to be a result of better organized urban gangs expanding their criminal networks into new market areas in suburban and rural locations, where they can absorb local unaffiliated gangs or use violence to intimidate them. As these expanding gangs encounter resistance from local gangs or other drug distributors in these communities, the NGIC reports that an increase in violent crimes such as assaults, drive-by shootings, and murders can be expected. The NGIC estimates the direct economic impact of gang activity in the U.S. at $5 billion and the indirect impact as much greater.

***Transnational Criminal Organizations and Enterprises:*** Transnational organized crime is an immediate and increasing concern of the domestic and international law enforcement and intelligence communities. Geopolitical, economic, social, and technological changes within the last two decades have allowed these criminal enterprises to become increasingly active worldwide, and includes the following distinct groups: Eurasian Organizations that have emerged since the fall of the Soviet Union; Asian Criminal Enterprises; traditional organizations such as the La Cosa Nostra (LCN) and Italian Organized Crime; Balkan Organized Crime; Middle Eastern Criminal Enterprises, and African Criminal Enterprises.

In FY 2010, two Threat Fusion Cells (TFC) were created in order to meet the Organized Crime Program (OCP) plan goal #1: to target, dismantle, disrupt, neutralize, and render impotent transnational criminal organizations and enterprises that pose a threat to National Security. The TFCs are specifically focused on two criminal enterprises, Brothers’ Circle and Semion Mogilevich Organization, and staffed with personnel from various intelligence and law enforcement communities, including the National Security Agency.

The risk of terrorism-related events associated with criminal enterprises is ever-increasing due to the following: Alien smuggling across the southwest border by drug and gang criminal enterprises; Colombian based narco-terrorism groups influencing or associating with traditional drug trafficking organizations; prison gangs being recruited by religious, political, or social extremist groups; and major theft criminal enterprises conducting criminal activities in association with terrorist related groups or to facilitate funding of terrorist-related groups. There also remains the ever present concern that criminal enterprises can facilitate the smuggling of chemical, biological, radioactive, or nuclear weapons and materials.

***Civil Rights:*** The FBI has primary responsibility for investigating all alleged violations of federal civil rights laws. These laws protect the civil rights of all citizens and persons within the U.S., and include the four major areas described below:

* Hate Crimes: Hate crimes are the top investigative priority of the Civil Rights Program because they impact not only the victims, but also the entire community. In October 2009, President Obama signed into law the Matthew Shepard and James Byrd, Jr. Hate Crimes Prevention Act of 2009. For the first time in the history of the Nation, the Federal Government will have the authority to prosecute violent hate crimes, including violence directed at the gay, lesbian, bisexual, and transgender community, to the fullest extent of its jurisdiction. This is the first significant expansion of federal criminal civil rights laws in over a decade. More than 15 percent of the 80,000 hate crime incidents reported over the past decade (16.6 percent in 2007) have involved violence based on sexual orientation. The FBI anticipates that hate crime complaints and predicated investigations will increase in the Field Offices located in states without hate crimes laws (Georgia, Arkansas, Wyoming, South Carolina, and Indiana), and in those fourteen states that have hate crimes laws but which do not include sexual orientation as a protected class (Alabama, Alaska, Idaho, Michigan, Mississippi, Montana, North Carolina, North Dakota, Ohio, Oklahoma, South Dakota, Utah, Virginia, and West Virginia). In these jurisdictions, the FBI will be the sole law enforcement agency with the authority to investigate a violent act as a hate crime.
* Color of Law (COL): COL violations are the deprivation of any rights, privileges, or immunities secured or protected by the U.S. Constitution by someone in his/her official, governmental capacity. The FBI has investigative responsibility for federal COL matters involving local and state law enforcement and concurrent responsibility with the Offices of Inspectors General for other federal agencies.
* Human Trafficking: Human trafficking is a form of modern-day slavery and, although not commonly known, is a significant and persistent problem both domestically and internationally. Victims are often lured with false promises of good jobs and better lives and then forced to work under brutal and inhumane conditions. Many trafficking victims are forced to work in the sex industry, but trafficking can also take place in labor settings involving domestic servitude, prison-like factories, and migrant agricultural work. Human trafficking cases require extensive outreach and cooperation with local, state, and federal agencies, as well as non-governmental organizations, to properly address the problem.
* Freedom of Access: Under the Freedom of Access to Clinic Entrances (FACE) Act, the FBI has the sole investigative responsibility for conducting investigations of potential FACE Act violations. Incidents include murder, death threats, invasions, burglaries, harassing telephone calls, hate mail, assaults, arsons, and other acts of intimidation. The number of FACE Act violations remains relatively low, with occasional spikes during dates which mark significant events in the pro-choice and pro-life movements.

***Violent Crimes:***

* Crimes Against Children: Every day, children are being recruited and forced into the world of child prostitution. Unlike the portrayal of prostitution in popular media, the reality is that child victims are not voluntary participants. Rather, they are modern-day slaves – forced into participating in prostitution and often brutally beaten. Teen runaways– who are often trying to escape abusive homes – frequently fall prey to domestic sex traffickers or "pimps" who lure them in with an offer of food and a seemingly safe place to sleep.
* Innocence Lost investigations address the commercial sexual exploitation of children. Investigations have identified national criminal organizations responsible for the sex trafficking of hundreds of children, some as young as nine years old. To date, the Innocence Lost National Initiative (ILNI) has resulted in 422 pending cases, 381 informations/indictments, and 532 convictions. Furthermore, subjects of these investigations are regularly sentenced to terms of 25 years or more, while four have received life sentences. Since its inception, 893 children have been recovered and removed from the cycle of abuse. In FY 2009 alone, 306 children were recovered, a 25 percent increase from the 245 children located in FY 2008. Between FY 2008 and FY 2009, the ILNI increased from 25 to 34 task forces and working groups, which represents a 36 percent increase.
* Child Sex Tourism (CST) is defined as Americans traveling to a foreign country to engage in sexual activity with a child. Sex tourists travel to specific countries where they can find anonymity, low-cost prostitution, easily accessible children, and immunity from prosecution. The production of child pornography is frequently involved in these cases as are drugs used to solicit or control minors. Travel companies throughout the world promote sex tourism of children by identifying resorts where child prostitution is widespread.
* Indian Country: As of FY 2010, the FBI is addressing more than 2,400 Indian Country (IC) investigations on approximately 200 reservations and over 400 Indian gaming facilities throughout 28 states. The majority of these investigations are in the Minneapolis, Salt Lake City, Phoenix, and Albuquerque Field Offices. Approximately 75 percent of all FBI IC investigations involve murder/death, sexual/physical assault of children, and felony assaults. Furthermore, statistics indicate that more than one-third of all Native American women will be raped at least once during their lifetime and nearly two-thirds will be victims of violent assaults. In addition to the violence, a significant emerging threat for the FBI which has gone largely unaddressed is the level of fraud and other white collar crimes committed on Indian reservations associated with the Indian Gaming industry.

The FBI receives little or no support from other law enforcement agencies in investigating these matters, due to the jurisdictional issues in IC. Furthermore, the Bureau of Indian Affairs has a limited number of investigators, who are not present on every reservation. Compounding this issue is the fact that Tribal authorities can only prosecute misdemeanors of Indians, and state/local law enforcement does not have jurisdiction within the boundaries of the reservation, with the exception of Public Law 280 states and tribes. The IC investigations also make up a large portion of the violent crimes prosecuted by the U.S. Attorney Offices; the current figure is in excess of twenty-five percent. Currently, there are 19 Safe Trails Task Forces who are addressing drug/gang and violent crimes in IC. The gang threat on Indian Reservations has become evident to the tribal community leaders, and gang related violent crime is reported to be increasing. Tribal communities have reported that tribal members are bringing back gang ideology from major cities, and Drug Trafficking Organizations are recruiting tribal members.

* Major Theft crimes caused by transnational, national and regionally based criminal enterprises have a devastating impact on the U.S. economy, not only contributing to the rise of consumer prices, but also to the loss of tax revenues to states and communities. More than 60 percent of the crimes reported to the police are theft/fraud related crimes according to the Uniform Crime Reporting (UCR) system. Major Theft crimes may support terrorism-related funding, and are directly related to organized crime groups, drug trafficking organizations, gang criminal enterprises and illegal alien groups. Major Theft groups actively engage in other criminal activities such as violent crimes, fraud, money laundering, wire and mail fraud, intellectual property crime, and public corruption matters. Estimates from certain Major Theft crimes, such as cargo theft and organized retail crime, are nearly impossible to calculate, but industry experts estimate losses in the tens of billions of dollars. Monetary and product losses from vehicle thefts are estimated at more than $8 billion per year. The Jewelry and Gem Industry estimates losses in excess of $135 million annually and the Art/Cultural Property Community estimate thefts to be about $500 million annually.
* Fugitives remain a concern to law enforcement with approximately 1.5 million active warrants within the National Crime Information Center (NCIC) system. The FBI is conducting investigations on more than 8,000 violent fugitives under the Unlawful Flight to Avoid Prosecution violation. Further, the FBI has more than 6,500 substantive case file fugitives outstanding and approximately 2,143 fugitives from the U.S. are believed to be in foreign countries. The FBI cooperates with the United State Marshals Service to investigate and apprehend domestic fugitives.
* Within the Transportation Crimes area, there were more than 500 crimes reported that occurred aboard an aircraft and another 100 incidents were reported regarding the destruction of aircraft. Personal and property crimes continue to be a concern within Special Jurisdiction Crimes areas such as within federal penal institutions, on other federal government properties, and in special jurisdictional areas, such as on the high seas.

***Southwest Border:*** The volatility among internationally-networked drug trafficking organizations (DTOs) and violent gangs (e.g., Mexican Mafia, Barrio Azteca, Los Zetas) along the Southwest border has resulted in drug-related violence. As rival cartels and gangs battle for control over the lucrative drug markets, numerous kidnappings, homicides and a myriad of other violent acts envelop the U.S.-Mexico border. In addition, these transnational groups are utilizing several “tools” to aid in their objectives, such as public corruption, money laundering, human trafficking, and threats to law enforcement.

* From 2006-08, violent crime dropped 6 percent in San Diego as it rose 28 percent in Tijuana; El Paso had 17 homicides in both 2007 and 2008, while over the same period Ciudad Juarez went from 301 to 1,607 homicides.
  + In 2009, 7,724 drug-related homicides occurred in Mexico, 22,700 since 2006.
  + Through mid-May 2010, 2,553 murders have occurred, on pace for 11,000 this year, averaging 29 per day.
  + 80 percent of these murders have occurred in six Mexican states, two of which border the U.S. – Chihuahua and Baja California

.

To address security along the Southwest border, the FBI has developed an intelligence-led, cross-programmatic strategy to penetrate, disrupt and dismantle the most dangerous organizations and individuals.This strategy begins with the deployment of hybrid squads in certain hotspots. The primary goal of the hybrid squad model is to bring a cross-programmatic domain view of these dynamic, multi-faceted threats and then target, disrupt, and dismantle these organizations. Hybrid squads consist of multi-disciplinary teams of Special Agents, IAs, Staff Operations Specialists (SOS), and other professionals. The agent composition on the squads provides different backgrounds and functional expertise, ranging from violent gangs, public corruption, and violent crimes.

**C. FBI’s 2012 Budget Strategy**

***Required Capabilities to Address National Security and Criminal Threats:*** The FBI’s budget strategy is based on the FBI’s understanding of current and future national security and criminal investigative threats. From this understanding, the FBI has identified critical, enterprise-wide capabilities needed to perform its mission. This capabilities-based approach to planning the FBI’s future resource requirements is necessary since it is not possible to project with certainty who will be the future adversary (e.g., Nation, combination of nations, non-state actor, gangs, criminal enterprises, or individuals). In other words, future capabilities are designed to enable the FBI to address the range of expected national security threats and crime problems regardless of who actually perpetrates the acts.

The FBI based its FY 2012 budget upon addressing six of the key national security and criminal threats noted above as well as critical infrastructure requirements. Please refer to the individual threat summaries and narrative justifications for additional threat discussion and for a detailed description of the resources requested to address the following threats and operational enablers:

* Computer Intrusions – Requested FY 2012 Increases:
  + Direct Funding: 42 positions (14 agents) and $18,628,000 ($6,552,000 non-personnel)
* National Security – Requested FY 2012 Increases:
  + Direct Funding: 73 positions (34 agents, 3 IAs) and $48,870,000 ($34,193,000 non-personnel)
* Electronic Surveillance Capabilities – Requested FY 2012 Increases:
  + Direct Funding: 13 positions (3 agents) and $12,466,000 ($10,247,000 non-personnel)

* Weapons of Mass Destruction / Render Safe – Requested FY 2012 Increases:
  + Direct Funding: 13 positions (6 agents) and $40,000,000 ($35,985,000 non-personnel
* Operational Enablers – Requested FY 2012 Increases:
  + Direct Funding: $2,486,000 non-personnel
* Violent Crime in Indian Country – Requested FY 2012 Increases:
  + Direct Funding: 40 positions (24 agents) and $9,000,000 ($449,000 non-personnel)

The Administration is also requesting funding for construction of the Central Records Complex (CRC). The CRC will make valuable, actionable intelligence, currently contained in FBI records, readily and universally available to analysts and agents throughout the FBI. The CRC will also aid in accurately preserving the administrative and operational records of the FBI, and ensure compliance with internal policy and external requirements, notably, compliance with Federal Records Management Standards. More information about funding for the complex is located in the Congressional Justification from the Public Building Fund administered by the General Services Administration.

***Foundation for Achieving the Desired Capabilities:*** The foundation of the FBI’s budget is supported by four objectives: (1) the application of a Strategy Management System (SMS) to FBI planning; (2) accelerated improvements in program management through intelligence-driven operations; (3) continuation of a multi-year planning process; and (4) a directed-growth strategy aligned to our most critical requirements.

**FBI Strategy Management System:**

The FBI implemented a Strategy Management System (SMS) to guide its strategy development and decision-making. The SMS is a strategic planning process that is maintained throughout the Bureau. Priorities are developed at the Enterprise, Branch, and Division levels; those entities then measure, track, and review performance against achieving their priorities on a quarterly basis.

Through the SMS, the FBI aims to strike the appropriate balance between its national security and criminal missions, and between short-term tactical efforts and longer-term strategic initiatives. Strategic management of the FBI’s two greatest assets, its employees and information, helps address the current mission and position the FBI to meet future challenges.

Led by the Director and facilitated by the Resource Planning Office (RPO), SMS is based on the Balanced Scorecard framework and has a twofold purpose: to implement the FBI’s strategic plan, and to unify strategic planning efforts throughout the FBI. SMS does so by aligning each Division’s resources and activities to the FBI’s top ten priorities and delineating how the priorities will be achieved.

The FBI’s SMS consists of several major, interrelated components:

* Strategic Shifts
* Strategy Map
* Balanced Scorecard/SMS Profile

Strategic Shifts

The FBI’s strategic shifts, shown below, consist of a set of focus areas selected by FBI leadership, along with the perceived present state (on the left) and intended future state (on the right) for each area. While the focus areas are not designed to be all-encompassing, they represent the key dimensions in which the organization needs to change in order to achieve its mission. The areas are often a combination of organizational, cultural, and technological changes that FBI leadership has identified as necessary to address over the next five years in order to realize the Bureau’s vision.



Strategy Map

The FBI Strategy Map is a visual representation of the organization’s strategic objectives. These objectives are organized by four broad themes: American Public Expectations, Internal Processes, Talent and Technology, and Resources.  The FBI is guided by a Strategy Map consisting of 25 strategic objectives, falling under 7 different themes, as shown below.  The Strategy Map describes the “story of the strategy” through a one-page, concise visual representation.



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.

Specifially, 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]](#footnote-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. 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 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 | | †† | | †† | | †† | |
| **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.

**Computer Intrusions**

**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.

***Performance Measure:*** Number of Criminal Computer Intrusion Investigations Successfully Completed

***FY 2010 Target:*** 33

***FY 2010 Actual:*** 34

***Discussion:***

The FBI exceeded its target for this measure for FY 2010. The increase is partially attributable to a shifting paradigm in the neutralization of the cyber threat. Increasingly, cyber threat actors are attacking from abroad and through the FBI’s partnership with international law enforcement, countries are prosecuting their own citizens rather than extraditing them for U.S. prosecution. Reporting metrics will be modified to capture these successes. This measure counts the amount of times where the FBI has achieved a successful result in a case primarily involving a computer intrusion, in violation of 18 U.S.C. §1030. This type of investigation relates to computer intrusions that occur under the following circumstances, using the following methods or having the following characteristics:

*Attack Impact:*

* Destruction of information, alteration of information, theft of information, denial of service.

*Special Circumstances:*

* Computer affecting the administration of justice or national security, threat to public health or safety, causation of physical injury, impaired or modified medical treatment

*Method:*

* Unauthorized access, exceeding authorized access, malicious code, denial of service, botnets, phishing, illegal wiretap, social engineering, physical access, network recon.

Currently, FBI Cyber Division reports automated conviction data for these accomplishments, which will be the basis of the baseline data for this measure. As the FBI implements reporting of these accomplishments through use of the FD-801 form, other criteria for determining the successful completion of a case based on a §1030 violation will be defined. The FBI Cyber Division will target a slightly higher number of successful conclusions, due to the closely developed international partnerships and their willingness to prosecute FBI subjects within their jurisdictions.

***FY 2011 Target:***  35

***FY 2012 Target:***  35

***Efficiency Measure:*** Cost Savings from Online Cyber Training

***FY 2010 Target:*** $596,000

***FY 2010 Actual:*** $819,112

***Discussion:*** The FBI's Cyber Program is progressing towards providing training for conducting cyber investigations via online training courses. The student population for the majority of these classes is quite broad, including FBI Special Agents, support employees and state and local law enforcement or intelligence partners. These classes are primarily introductory-level training classes that provide students with basic cyber concepts and investigative strategies. Introductory-level classes do not involve significant hands-on interaction with hardware, software or networking devices. For Special Agents on the Cyber Career Path, there are core classes which are required before continuing on to take more technically advanced courses. Knowledge of cyber basics, and the mission and priorities of the Cyber Division throughout the FBI, aids the program. In addition to offering online training via the FBI Virtual Academy (the FBI's closed system intranet training system), training is also offered over the Internet, via a CENTRA Server. These online training options allow the FBI to offer courses to employees in remote locations, to state and local investigators with little or no cost, and to FBI employees who would not ordinarily have been selected for attendance at classroom-based training due to prohibitive travel costs or a low selection priority for available seats.

***FY 2011 Target:***  $625,000

***FY 2012 Target:***  $1,155,900

***Performance Measure:*** Computer Intrusion Program Convictions/Pre-Trial Diversions

***FY 2010 Actual:*** 134 Convictions

***Discussion:*** Computer intrusion convictions are expected to rise as a result of increased investigations and level of agent expertise. The FBI anticipates addressing an ever-increasing caseload and hence changes in the amount of subsequent convictions/pre-trial diversions. The strategies to accomplish these outcomes include: continuing and enhancing the alliances with cybersecurity community members, the coordination of intelligence, both criminal and national security in nature, and the most critical – increased international liaison and partnerships. This key factor includes initiatives to develop cyber crime law enforcement strategy, leverage international cooperation between governments, law enforcement, and private industry, share information and training, share and develop new tools, and educate the public. Given the transnational nature of cyber crime, it is imperative to establish effective international cooperation and develop appropriate and consistent legislation. As cyber crimes cross national boundaries, international law enforcement cooperation is crucial. Because most laws and agencies operate within national borders, gaps exist in international legal coverage and harmonization of offences, and agencies seek (or provide) international assistance only when a crime impacts their interests. A lack of staff with sufficient technical skills to effectively assist in investigating cyber crimes compounds this situation.

***FY 2011 Target:*** In accordance with Department guidance, targeted levels of performance are not projected for this indicator.

***FY 2012 Target:*** In accordance with Department guidance, targeted levels of performance are not projected for this indicator.

**C. Criminal Enterprises and Federal Crimes Decision Unit**

|  |  |  |  |
| --- | --- | --- | --- |
| CRIMINAL ENTERPRISES AND FEDERAL CRIMES DECISION UNIT TOTAL | Perm. Pos. | FTE | Amount ($000) |
| 2010 Enacted with Rescissions | 11,484 | 11,090 | $2,471,964 |
| 2011 Continuing Resolution | 11,438 | 10,979 | 2,473,306 |
| Adjustments to Base and Technical Adjustments | 237 | 496 | 117,733 |
| 2012 Current Services | 11,675 | 11,475 | 2,591,039 |
| 2012 Program Increases | 66 | 33 | 28,792 |
| 2012 Program Offsets | … | … | (12,937) |
| 2012 Request | 11,741 | 11,508 | 2,606,894 |
| Total Change 2011-2012 | 303 | 529 | $133,588 |

|  |  |  |  |
| --- | --- | --- | --- |
| Criminal Enterprises and Federal Crimes Decision Unit – Information Technology Breakout | Perm. Pos. | FTE | Amount  ($000) |
| 2010 Enacted with Rescissions | 289 | 289 | $241,456 |
| 2011 Continuing Resolution | 293 | 293 | 253,751 |
| Adjustments to Base and Technical Adjustments | 16 | 16 | (53,572) |
| 2012 Current Services | 309 | 309 | 200,179 |
| 2012 Program Increases | … | … | … |
| 2012 Request | 309 | 309 | 200,179 |
| Total Change 2011-2012 | 16 | 16 | ($53,572) |

1. Program Description

The Criminal Enterprises and Federal Crimes (CEFC) decision unit (DU) comprises all headquarters and field programs that support the FBI's criminal investigative missions. The DU includes:

* The FBI’s Organized Crime, the Gang/Criminal Enterprise (G/CE), and the Criminal Intelligence programs;
* The Financial Crime, Integrity in Government/Civil Rights, and Violent Crime programs;
* The Public Corruption and Government Fraud programs which investigate state, local and federal government acts of impropriety, including the rising level of federal and state legislative corruption;
* The criminal investigative components of the Cyber Division's programs to include, Criminal Computer Intrusions, Intellectual Property Rights violations, the Innocent Images National Initiative (IINI), and the Internet Crime Complaint Center (IC3); and
* A share of the FBI's Legal Attaché (Legat) program.

Additionally, the decision unit includes a prorata share of resources from the FBI's support divisions (including Training, Laboratory, Security, Information Technology Operations, and the administrative divisions and offices).

The structure of the FBI’s Criminal Intelligence Program maximizes the effectiveness of resources, improves investigation and intelligence gathering processes, focuses on threats from criminal enterprises, and promotes the collection, exchange and dissemination of intelligence throughout the FBI and other authorized agencies.

**Financial Crime**

***White Collar Crime:* 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.
* **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, 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 established 13 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. The majority of cases pursued by the Bureau involve accounting schemes—deceiving investors, auditors and analysts 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.
* 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 each involve thousands of victims and staggering losses – some in the billions of dollars. Indeed, the FBI continues to open new Ponzi scheme cases on 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.
* Mortgage Fraud, and Other Financial Institution Fraud: Mortgage fraud, a subset of financial institution fraud, continues to absorb considerable FBI resources. FBI intelligence predicts an increase in foreclosures, financial institutions/firms failures, regulatory agency/independent auditor fraud referrals and governmental housing relief fraud. Currently, Commercial Real Estate (CRE) fraud is the greatest emerging threat that the FBI is addressing.
* Health Care Fraud: Total health care expenditures in the U.S. will surpass the $4 trillion mark by 2015, representing a 139-percent increase or more than double the 2003 $1.67 trillion expenditures. The FBI seeks to infiltrate illicit operation and terminate scams involving staged auto accidents, online pharmacies, Durable Medical Equipment, outpatient surgery centers, counterfeit pharmaceuticals, nursing homes, hospital chains, and transportation services. Besides the federal health benefit programs of Medicare and Medicaid, private insurance programs lose billions of dollars each year to blatant fraud schemes in every sector of the industry.
* Money Laundering: Money Laundering allows criminals to infuse illegal money into the stream of commerce, thus corrupting financial institutions and the money supply; this provides the criminals with unwarranted economic power. The FBI investigates money laundering cases by identifying the process by which criminals conceal or disguise the proceeds of their crimes or convert those proceeds into goods and services. The major threats in this area stem from emerging technologies, such as stored value devices, pre-paid gift cards and reloadable debit cards, in order to move criminal proceeds; as well as shell corporations, which are used to conceal the beneficial ownership of funds being moved through financial institutions and international commerce.
* Other Complex Financial Crimes (Insurance, Bankruptcy, and Mass Marketing Fraud): According to the Coalition Against Insurance Fraud (CAIF), insurance fraud costs Americans approximately $80 billion a year, or nearly $950 per family. The FBI anticipates insurance fraud to continue to increase, contributing to increases in insurance premiums as well as threatening the financial viability of insurance companies. Since 2006, the year after bankruptcy laws were changed to make it more difficult for an individual to discharge all debts, bankruptcy filings have significantly increased each year. The potential for fraud within bankruptcy is large. According to the Federal Trade Commission, complaints concerning mass marketing fraud have also increased.

**Civil Rights**

***Civil Rights:*** The FBI has primary responsibility for investigating all alleged violations of federal civil rights laws. These laws protect the civil rights of all citizens and persons within the U.S., and include the four major areas described below:

* Hate Crimes: Hate crimes are the top investigative priority of the Civil Rights Program because they impact not only the victims, but also the entire community. In October 2009, President Obama signed into law the Matthew Shepard and James Byrd, Jr. Hate Crimes Prevention Act of 2009. For the first time in the history of the Nation, the federal government will have the authority to prosecute violent hate crimes, including violence directed at the gay, lesbian, bisexual, and transgender community, to the fullest extent of its jurisdiction.
* Color of Law (COL): COL violations are the deprivation of any rights, privileges, or immunities secured or protected by the U.S. Constitution by someone in his/her official, governmental capacity. The FBI has investigative responsibility for federal COL matters involving local and state law enforcement and concurrent responsibility with the Office of Inspectors General for other federal agencies.
* Human Trafficking: Human trafficking is a form of modern-day slavery and, although not commonly known, is a significant and persistent problem in America and internationally. Victims are often lured with false promises of good jobs and better lives and then forced to work under brutal and inhumane conditions. Many trafficking victims are forced to work in the sex industry, but trafficking can also take place in labor settings involving domestic servitude, prison-like factories, and migrant agricultural work. Human trafficking cases require extensive outreach and cooperation with local, state, and federal agencies, as well as non-governmental organizations, to properly address the problem.
* Freedom of Access: Under the Freedom of Access to Clinic Entrances (FACE) Act, the FBI has the sole investigative responsibility for conducting investigations of potential FACE Act violations. Incidents include murder, death threats, invasions, burglaries, harassing telephone calls, hate mail, assaults, arsons, and other acts of intimidation. The number of FACE Act violations remains relatively low, with occasional spikes during dates which mark significant events in the pro-choice and pro-life movements.

**Criminal Enterprises**

***Organized Crime:* T**ransnational organized crime is an immediate and increasing concern of the domestic and international law enforcement and intelligence communities. Geopolitical, economic, social, and technological changes within the last two decades have allowed these criminal enterprises to become increasingly active worldwide, and includes the following distinct groups: Eurasian Organizations that have emerged since the fall of the Soviet Union; Asian Criminal Enterprises; traditional organizations such as the La Cosa Nostra (LCN) and Italian Organized Crime; Balkan Organized Crime; Middle Eastern Criminal Enterprises, and African Criminal Enterprises.

In FY 2010, two Threat Fusion Cells (TFC) were created in order to meet the Organized Crime Program (OCP) plan goal #1: to target, dismantle, disrupt, neutralize, and render impotent transnational criminal organizations and enterprises that pose a threat to National Security. The TFCs are specifically focused on two criminal enterprises, Brothers’ Circle and Semion Mogilevich Organization, and is staffed with personnel from various intelligence and law enforcement communities, including the National Security Agency.

The potential for terrorism-related events associated with criminal enterprises is ever-increasing due to the following: Alien smuggling across the southwest border by drug and gang criminal enterprises; Colombian based narco-terrorism groups influencing or associating with traditional drug trafficking organizations; prison gangs being recruited by religious, political, or social extremist groups; and major theft criminal enterprises conducting criminal activities in association with terrorist related groups or to facilitate funding of terrorist-related groups. There also remains the ever present concern that criminal enterprises are, or can, facilitate the smuggling of chemical, biological, radioactive, or nuclear weapons and materials.

***Gang Violence:*** The mission of the Gangs Criminal Enterprise Section (GCES) is to disrupt and dismantle the domestic cells (local, regional, national, and transnational) of criminal enterprises which pose the greatest threats to the economic and national security of the U.S. This is being accomplished through initiatives established in the GCES subprograms of violent gangs, drugs, and major theft.

Violent street gangs operate in communities of all sizes; urban, suburban and rural areas across the country. According to law enforcement officials throughout the Nation, criminal gangs commit as much as 80 percent of the crime in our communities. FBI Violent Gang Safe Streets Task Forces (VGSSTFs) report that violent street gangs, whether they are neighborhood based or national gangs, are a top threat to our communities followed by prison gangs and outlaw motorcycle gangs. The Department of Justice (DOJ) and the National Gang Intelligence Center's (NGIC) 2009 Gang Threat Assessment estimates there were 20,000 U.S. based gangs criminally active with total gang membership at approximately 1,000,000 members. This shows that gang activity poses a dangerous threat to our domestic security each year.

Gangs continue to proliferate and commit violent crime. NGIC further identified a trend whereby gang members are expanding to suburban and rural areas. This migration is believed to be a result of better organized urban gangs expanding their criminal networks into new market areas in suburban and rural locations, where they can absorb local unaffiliated gangs or use violence to intimidate them. As these expanding gangs encounter resistance from local gangs or other drug distributors in these communities, the NGIC reports that an increase in violent crimes such as assaults, drive-by shootings, and murders can be expected. The NGIC estimates the direct economic impact of gang activity in the U.S. at $5 billion and the indirect impact as much greater.

**Violent Crime**

***Violent Crimes:*** The mission of the Violent Crimes Program is to combat significant violent crime in the U.S. and make its streets safer for U.S. citizens. Major violent crime incidents can paralyze whole communities and stretch state and local law enforcement resources to their limits. Significant instances of bank/armored car robberies, extortions, kidnappings, mass shootings, product tampering and crimes against children committed by individuals and criminal groups have a dramatic effect on the safety of citizens and has an unknown economic impact on the U.S.. Increased incidents of violent crime and hostage taking have occurred in foreign countries, and the FBI frequently assists foreign law enforcement agencies in the investigations of those violent acts committed against U.S. citizens or by U.S. citizens in those foreign lands. The FBI Violent Crime Section is responsible in addressing Crime Against Children, Indian Country, and Major Offenders.

* Crimes Against Children: The FBI Crimes Against Children Unit supports the Child Abduction Rapid Deployment Team (CARD Team), Innocence Lost National Initiative and the Child Sex Tourism (CST) Initiative.
  + Child Abductions: In FY 2010, the FBI investigated 190 pending child abduction cases. In an effort to enhance the FBI's response to abductions and the mysterious disappearance of children, the FBI’s Violent Crimes Section in coordination with the Critical Incident Response Group (CIRG)/Behavior Analysis Unit III (BAU III) created regional CARD Teams. The Nation-wide CARD Team cadre consists of sixty field agents. Teams are geographically distributed throughout the five regions of the United States, consistent with the FBI Corporate Management Structure. Each region has two teams comprised of Supervisory Special Agents and Special Agents representing 36 field divisions. To date, the CARD Teams have deployed on 64 occasions resulting in the successful recovery of twenty seven children.
  + Innocence Lost National Initiative: Everyday, children are being recruited and forced into the world of prostitution. Unlike the portrayal of prostitution in popular media, the reality is that child victims are not voluntary participants. Rather, they are modern-day slaves – forced into participating in prostitution and often brutally beaten. Teen runaways – who are often trying to escape abusive homes – frequently fall prey to domestic sex traffickers or "pimps" who lure them in with an offer of food and a seemingly safe place to sleep. In an effort to address this significant crime problem, the FBI has assisted in the establishment of 25 task forces and 16 working groups with our state and local law enforcement partners. In addition, the FBI has developed a national targeted enforcement action entitled Operation Cross Country which is conducted on a regular basis and has resulted in the recovery of 248 juveniles and the arrest of 322 pimps.
  + Child Sex Tourism (CST) is defined as Americans traveling to a foreign country to engage in sexual activity with a child. Sex tourists travel to specific countries where they can find anonymity, low-cost prostitution, easily accessible children, and immunity from prosecution. The production of child pornography is frequently involved in these cases; as are drugs used to solicit or control minors. Travel companies throughout the world promote sex tourism of children by identifying resorts where child prostitution is widespread.
* Indian Country: As of FY 2010, the FBI addresses more than 2,400 Indian Country (IC) investigations on approximately 200 reservations and over 400 Indian gaming facilities throughout 28 states. The greatest majority of these investigations are in the Minneapolis, Salt Lake City, Phoenix, and Albuquerque Field Offices. Approximately 75 percent of all FBI IC investigations involve murder/death, sexual/physical assault of children, and felony assaults. Furthermore, statistics indicate that more than one-third of all Native American women will be raped at least once during their lifetime and nearly two-thirds will be victims of violent assaults. In addition to the violence, a significant emerging threat for the FBI which has gone largely unaddressed is the level of fraud and other white collar crimes committed on Indian reservations associated with the Indian Gaming industry.

The FBI receives little or no support from other law enforcement agencies in investigating these matters, due to the jurisdictional issues in IC. Furthermore, the Bureau of Indian Affairs has a limited number of investigators, who are not present on every reservation. Compounding this issue is the fact Tribal authorities can only prosecute misdemeanors of Indians, and state/local law enforcement does not have jurisdiction within the boundaries of the reservation, with the exception of Public Law 280 states and tribes. The IC investigations also make up a large portion of the violent crimes prosecuted by the U.S. Attorney Offices; the current figure is in excess of twenty-five percent. Currently, there are 19 Safe Trails Task Forces who are addressing drug/gang and violent crimes in IC. The gang threat on Indian Reservations has become evident to the tribal community leaders, and gang related violent crime is reported to be increasing. Tribal communities have reported tribal members are bringing back gang ideology from major cities and Drug Trafficking Organizations are recruiting tribal members.

* Major Offenders: The Violent Crimes/Major Offenders Unit (VC/MOU) is responsible for the program management and oversight of the Violent Incident Crimes, Fugitive, Major Theft and Transportation subprograms.  Particular emphasis is directed toward matters involving significant violence to include Bank Robberies, Armored Car Robberies, Fugitives, Kidnappings for Ransom, Extortions, Police Killings, Assault on Federal Officers (AFO), and Major Theft Cases including Organized Retail, Cargo, and Art Theft.  The VC/MOU also manages various violent crime program initiatives such as Project Pin Point, the Cellular Analysis and Survey Teams (CAST) and Military Extra-Territorial Jurisdiction Act (MEJA) investigations.
  + Major Theft crimes caused by transnational, national and regionally based criminal enterprises have a devastating affect on the U.S. economy, not only contributing to the rise of consumer prices, but also to the loss of tax revenues to states and communities. More than 60 percent of the crimes reported to the police are theft/fraud related crimes according to the Uniform Crime Reporting (UCR) system. Major Theft crimes are directly related to organized crime groups, drug trafficking organizations, gang criminal enterprises and illegal alien groups. Major Theft groups actively engage in other criminal activities such as violent crimes, fraud, money laundering, wire and mail fraud, and public corruption matters. Estimates from certain Major Theft crimes, such as cargo theft and organized retail crime, are nearly impossible to calculate, but industry experts estimate losses in the tens of billions of dollars. Monetary and product losses from vehicle thefts are estimated at more than $8 billion per year. The Jewelry and Gem Industry estimates losses in excess of $135 million annually and the Art/Cultural Property Community estimate thefts to be about $500 million annually
  + Fugitives remain a concern to law enforcement with approximately 1.5 million active warrants within the National Crime Information Center (NCIC) system. The FBI is conducting investigations on more than 8,000 violent fugitives under the Unlawful Flight to Avoid Prosecution violation. Further, the FBI has more than 6,500 substantive case file fugitives outstanding and approximately 2,143 fugitives from the U.S. are believed to be in foreign countries. The FBI cooperates with the United State Marshals Service to investigate and apprehend domestic fugitives.
  + Transportation Crimes include more than 500 crimes reported that occurred aboard an aircraft and another 100 incidents were reported regarding the destruction of aircraft. Personal and property crimes continue to be a concern within Special Jurisdiction Crimes areas such as within federal penal institutions, on other federal government properties and in special jurisdictional areas, such as on the high seas.

***Southwest Border:*** The volatility among internationally-networked drug trafficking organizations (DTOs) and violent gangs (e.g., Mexican Mafia, Barrio Azteca, Los Zetas) along the Southwest border has resulted in drug-related violence. As rival cartels and gangs battle for control over the lucrative drug markets significant spikes in kidnappings, homicides and a myriad of other violent acts envelop the U.S.-Mexico border. In addition, these transnational groups are utilizing several “tools” to aid in their objectives, such as public corruption, money laundering, human trafficking, and threats to law enforcement.

The FBI does not have a single program that addresses the Southwest Border threats and vulnerabilities, but has developed an intelligence-led, cross-programmatic strategy to penetrate, disrupt and dismantle the most dangerous organizations and individuals.This strategy begins with the formation of new hybrid squads in certain hotspots. The primary goal of the hybrid squad model is to bring a cross-programmatic domain view of these dynamic, multi-faceted threats – then target, disrupt, and dismantle these organizations. Hybrid squads will consist of multi-disciplinary teams of special agents, intelligence analysts, Staff Operations Specialists (SOS), and other professionals. The agent composition on the squads will reflect different backgrounds and functional expertise, ranging from violent gangs, public corruption, and violent crimes.

***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 criminal activity. Included under the purview of the Cyber Program within the CEFC DU are 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.

***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. that have an international nexus. The criminal component of the Legat program provides for a prompt and continuous exchange of information with foreign law enforcement and supports the FBI's efforts to meet its investigative responsibilities.

***Management and Support Services***

In addition to the Criminal Investigative, Cyber, and Legat programs that make up the core elements of the CEFC DU, the FBI's various administrative and other security programs provide essential support services.

**Program Objectives**

***White Collar Crime:***

* Initiate undercover operations and employ sophisticated investigative techniques to address fraud related to Federal stimulus funding.
* Facilitate the intelligence and administrative requirements related to complex public corruption investigations to reduce the incidence of government fraud within targeted sectors of local, state, and federal government.
* Reduce the amount of reported economic loss due to fraud and abuse in federally funded procurement, contracts, Electronic Benefits Transfer, and entitlement programs.
* Expand the Border Corruption Initiative (BCI) and threat methodology to better target border corruption in all land, air, and sea ports of entry to mitigate the threat posted to national security.
* Continue Border Corruption Task Force (BCTFs) coordination with other field divisions and agencies on cross-program strategies regarding the threats associated with counter terrorism, weapons of mass destruction, and counter intelligence matters.
* Deploy FBI resources to combat significant complex financial crimes in order to:
  + Minimize the economic loss due to mortgage fraud by identifying, investigating, and disrupting fraudulent activity.
  + Reduce the economic loss associated with the theft of U.S. intellectual property by criminals.
  + Reduce the amount of economic loss and market instability resulting from corporate fraud committed by both individuals and enterprises.
  + Identify, disrupt, and dismantle money laundering industries and confiscate criminal assets associated with said industries.
  + Reduce the economic loss attributable to fraudulent billing practices affecting private and public health care insurers.
  + Minimize economic loss due to crimes such as check fraud, loan fraud, and cyber-banking fraud in federally-insured financial institutions.
  + Reduce the amount of economic loss to the insurance industry due to fraud, both internal and external.
  + Reduce economic loss to investors due to fraud in the investment marketplace, bogus securities, and Internet fraud.
  + Reduce the amount of economic loss caused by fraudulent bankruptcy filings throughout the U.S.

***Cyber:***

* Reduce the amount of economic loss associated with the theft of U.S. intellectual property by criminals.
* Investigate criminal computer intrusions, intellectual property rights violations and theft of trade secrets, internet fraud, etc.
* Reduce the vulnerability of children to acts of sexual exploitation and abuse which are facilitated through the use of computers.
* Develop partnerships between the FBI and private sector, academia, and other public entities to support the FBI’s mission.
* Serve as a vehicle to receive, develop, and refer criminal complaints regarding the cyber crime arena.
* Identify, develop and deliver core and continuing education for Cyber investigators across all levels of the law enforcement, both domestic and international.

***Civil Rights:***

* Deter civil rights violations through aggressive investigation of those crimes wherein the motivation appears to have been based on race, sexuality, color, religion, or ethnic/national origin; reports of abuse of authority under color of law; reports of slavery and involuntary servitude; and reports of the use of force or the threat of force for the purpose of injuring, intimidating, or interfering with a person seeking to obtain or provide reproductive health services and through proactive measures such as the training of local law enforcement in civil rights matters.

***Gang Violence:***

* Infiltrate, disrupt and dismantle violent gang activities by targeting groups of gangs using sensitive investigative and intelligence techniques to initiate long term proactive investigations.

***Organized Crime*:**

* Combat transnational organizations and enterprises and collect resources supporting intelligence and investigation actions to disrupt and dismantle organized criminal activities worldwide.
* Continually assess the international organized crime threat in the country by outlining current state of FBI resources and better position the FBI to strategically direct investigatory resources to the highest threat areas.
* Execute a comprehensive strategy to disrupt and dismantle Simeon Mogilevisch Organization and Brothers’ Circle through two planned Threat Fusion Cells (TFCs).

***Violent Crime:***

* Investigate the most egregious and violent criminal acts across Indian Country to include homicide, child sexual/physical assault, violent assault, drugs/gangs, gaming violations, and property crimes.
* Promote and encourage a level of self-sufficiency for tribal law enforcement on Indian Reservations and allotment territory, thereby allowing the FBI to improve the response and efficiency of Special Agent and support resources in IC; improve the overall quality of law enforcement service in IC through increased coordination with BIA and tribal police, joint training efforts, and joint investigative efforts; establish Safe Trail Task Forces, with objectives focused on specific priority crime problem(s) not effectively addressed by the FBI or other law enforcement agencies in IC; provide training to IC Special Agents, support personnel, and BIA/tribal police; and assist and support DOJ efforts to professionalize law enforcement operations in IC, to include crime statistics reporting, records management, automation, and case management.
* Provide a rapid and effective investigative response to reported federal crimes involving the victimization of children; reduce the vulnerability of children to acts of sexual exploitation and abuse; reduce the negative impact of domestic/international parental rights disputes; and strengthen the capabilities of federal, state and local law enforcement through training programs and investigative assistance.

***Southwest Border:***

* Continue to support the Southwest Border Initiative, which focuses the FBI's efforts on the most significant criminal enterprises operating along the southwest border

| **PERFORMANCE/RESOURCES TABLE** | | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Decision Unit:** Criminal Enterprises/Federal Crimes | | | | | | | | | | | |
| **DOJ Strategic Goal/Objective** Goal 2: Prevent Crime, Enforce Federal Laws, and Represent the Rights and Interests of the American People, Objectives 2.2-2.6. | | | | | | | | | | | |
| **WORKLOAD/ RESOURCES** | | **Final Target** | | **Actual** | | **Projected** | | **Changes** | | **Requested (Total)** | |
| **FY 2010** | | **FY 2010** | | **FY 2011** | | **Current Services Adjustments & FY2012 Program Changes** | | **FY 2012 Request** | |
| **Workload --** # of cases investigated (pending and received) | | † | | 80,955 | | † | | † | | † | |
| **Total Costs and FTE** | | **FTE** | **$000** | **FTE** | **$000** | **FTE** | **$000** | **FTE** | **$000** | **FTE** | **$000** |
| 11,090 | 2,471,964 | 10,688 | 2,471,964 | 10,979 | 2,473,306 | 496 | 117,733 | 11,475 | 2,591,039 |
| **TYPE/ STRATEGIC OBJECTIVE** | **PERFORMANCE** | **FY 2010** | | **FY 2010** | | **FY 2011** | | **Current Services Adjustments & FY2012 Program Changes** | | **FY 2012 Request** | |
| **Program Activity/ 2.3, 2.5** | **1. White-Collar Crime/Cybercrime** | **FTE** | **$000** | **FTE** | **$000** | **FTE** | **$000** | **FTE** | **$000** | **FTE** | **$000** |
| 5,730 | 1,290,735 | 5,522 | 1,277,151 | 5,377 | 1,210,583 | 344 | 96,485 | 5,721 | 1,307,068 |
| **Workload --** # of cases investigated (pending and received) | | † | | 32,488 | | † | | † | | † | |
| **Performance Measure** | Restitutions & Recoveries / Fines ($000)   * Intellectual Property Rights Violations * Public Corruption * White-Collar Crimes (all other) | †† | | 17,100  6,559,531  8,383,458 | | †† | | †† | | †† | |
| **Performance Measure** | Convictions/Pre-Trial Diversions (total)   * Intellectual Property Rights Violations * Public Corruption * White-Collar Crimes (all other) | †† | | 84  954  3,357 | | †† | | †† | | †† | |
| **Performance Measure** | Number of Criminal Enterprises Engaging in White-Collar Crimes Dismantled | 160 | | 236 | | 250 | | 25 | | 275 | |
| Efficiency Measure | % of Major Mortgage Fraud Investigations to all pending | 69% | | 71% | | 70% | | 0 | | 70% | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **TYPE/ STRATEGIC OBJECTIVE** | | **PERFORMANCE** | | **FY 2010** | | | | **FY 2010** | | | **FY 2011** | | | | **Current Services Adjustments & FY2012 Program Changes** | | | | **FY 2012 Request** | | | |
| **Performance Measure (Renamed Measure)** | | Number of Children Depicted in Child Pornography Identified by the FBI | | 130 | | | | 246 | | | 140 | | | | 15 | | | | 155 | | | |
| **Performance Measure** | | Number of high-impact Internet fraud targets neutralized | | 13 | | | | 12 | | | 10 | | | | (1) | | | | 9 | | | |
| **Program Activity/ 2.2, 2.4, 2.6** | | **2. Criminal Enterprises/Civil Rights/Violent Crimes** | | **FTE** | | **$000** | | **FTE** | **$000** | | **FTE** | | **$000** | | **FTE** | | **$000** | | **FTE** | | **$000** | |
| 5,360 | | 1,181,229 | | 5,166 | 1,194,813 | | 5,602 | | 1,262,723 | | 185 | | 37,103 | | 5,787 | | 1,299,826 | |
| **Workload --** # of cases investigated (pending and received) | | | | † | | | | 48,467 | | | † | | | | † | | | | † | | | |
| **Performance Measure** | | Convictions/Pre-trial Diversions   * Organized Criminal Enterprises * Gang/Criminal Enterprises * Crimes Against Children * Civil Rights | | †† | | | | 424  2,163  245  248 | | | †† | | | | †† | | | | †† | | | |
| Efficiency Measure | | % of FBI OCDETF Investigations with links to CPOT-linked DTOs | | 12% | | | | 15.89% | | | 12% | | | | 0 | | | | 12% | | | |
| **Performance Measure** | | CPOT-Linked DTOs   * Disruptions * Dismantlements | | 30  15 | | | | 40  12 | | | 30  15 | | | | 0  0 | | | | 30  15 | | | |
| **Performance Measure** | | Number of Organized Criminal Enterprise Dismantlements | | 36 | | | | 39 | | | 37 | | | | 0 | | | | 37 | | | |
| Performance Measure | | Number of Gang/Criminal Enterprises Dismantlements | | 99 | | | | 124 | | | 99 | | | | 0 | | | | 99 | | | |
| **Data Definition, Validation, Verification, and Limitations:**   * Disruption means impeding the normal and effective operation of the targeted organization, as indicated by changes in organizational leadership and/or changes in methods of operation, including, for example, financing, trafficking patterns, communications or drug production. Dismantlement means destroying the organization’s leadership, financial base, and supply network such that the organization is incapable of operating and/or reconstituting itself. * The Executive Office of OCDETF may sometimes edit CPOT disruptions/dismantlements data after submission of the President’s Budget Submission to Congress. These changes are reflected in the current tables. * Accomplishment and caseload data are obtained from the FBI’s Resource Management Information System (RMIS), which houses the Integrated Statistical Reporting and Analysis Application (ISRAA) and Monthly Administrative Report (MAR) applications that report these data. Data are verified by an FBI field manager before being entered into that system and are subsequently verified through the FBI’s Inspection process. Other non-standardized data are maintained in files by their respective FBIHQ programs.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 when reported close to the end of the fiscal year. * The data source for IINI program data is a database maintained by FBI personnel detailed to the National Center for Missing and Exploited Children, as well as statistics derived by the FBI’s Cyber Division’s program personnel. Limitations on these data are explained in the Discussion of the measure. * Internet Fraud data come from a record system maintained by the IC3. The list of targets is updated each year. Targets are determined by subject matter expert teams at the IC3 and approved by the Unit Chief. IC3 staff maintains the list and determine when a target has been the subject of a take-down. There is some possibility of underreporting of accomplishments resulting from referrals to state, local, and other federal law enforcement organizations. This underreporting is possible where investigations resulting from IC3 referrals do not involve the FBI.   † FBI does not project targets for case workload data.  †† FBI does not set targets for investigative output data. | | | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | | | |
|  | | | **FY 2003** | | **FY 2004** | | **FY 2005** | | | **FY 2006** | | **FY 2007** | | **FY 2008** | | **FY 2009** | | **FY 2010** | | | |
| **Actual** | | **Actual** | | **Actual** | | | **Actual** | | **Actual** | | **Actual** | | **Actual** | | **Target** | | **Actual** | |
| **Performance Measure** | Restitutions/Recoveries/Fines ($000)   * Intellectual Property Fraud * Public Corruption * White-Collar Crimes (all other) | | 205,120 1,631,692  8,433,421 | | 115,967 101,647  7,881,151 | | 432,316 1,116,266  13,056,937 | | | 111,877  321,815 7,799,218 | | 238,832  157,440  19,516,406 | | 260,219  676,889  18,502,635 | | 5,389  220,787  15,956,528 | | N/A  N/A  N/A | | 17,100  6,559,531  8,383,458 | |
| **Performance Measure** | Convictions/Pre-Trial Diversions (total)   * Intellectual Property Fraud * Public Corruption * White-Collar Crimes (all other) | | 110 579  5,022 | | 116  661  4,368 | | 121  812  3,976 | | | 194  929  3,707 | | 136  943  3,347 | | 116  987  3,834 | | 88  981  2,910 | | N/A  N/A  N/A | | 84  954  3,357 | |
| **Performance Measure** | Number of Criminal Enterprises Engaging in White-Collar Crimes Dismantled | | 73 | | 137 | | 163 | | | 231 | | 277 | | 211 | | 250 | | 160 | | 236 | |
| **Efficiency Measure** | % of Major Mortgage Fraud Investigations to all pending | | N/A | | N/A | | N/A | | | N/A | | 56% | | 63% | | 66% | | 69% | | 71% | |
| **Performance Measure (Renamed Measure)** | Number of Children Depicted in Child Pornography Identified by the FBI (*\*only partial year data available for FY06)* | | N/A | | N/A | | N/A | | | 37\* | | 73 | | 187 | | 118 | | 130 | | 246 | |
| **Performance Measure** | Number of high-impact Internet fraud targets neutralized | | 5 | | 7 | | 10 | | | 9 | | 11 | | 11 | | 13 | | 13 | | 12 | |
| **Performance Measure** | Convictions/Pre-Trial Diversions:   * Organized Criminal Enterprises * Gang/Criminal Enterprises * Crimes Against Children * Civil Rights | | 824  4,089  154  163 | | 572  2,923  145  155 | | 897  4,292  164  139 | | | 674  2,070  170  195 | | 693  2,218  207  207 | | 595  2,242  246  208 | | 395  2,136  270  222 | | N/A  N/A  N/A  N/A | | 424  2,163  245  248 | |
| **Efficiency Measure** | % of FBI OCDETF Investigations with links to CPOT-linked DTOs | | N/A | | N/A | | 11% | | | 13% | | 14% | | 15.47% | | 14% | | 12% | | 15.89% | |
| **Performance Measure** | CPOT-Linked DTOs   * Disruptions * Dismantlements | | 41  15 | | 27  12 | | 25  18 | | | 36  17 | | 45  15 | | 50  18 | | 35  20 | | 30  15 | | 40  12 | |
| **Performance Measure** | Number of Organized Criminal Enterprise Dismantlements | | 17 | | 29 | | 34 | | | 36 | | 43 | | 38 | | 43 | | 36 | | 39 | |
| **Performance Measure** | Number of Gang/Criminal Enterprise Dismantlements | | 138 | | 112 | | 138 | | | 119 | | 144 | | 114 | | 135 | | 99 | | 124 | |

**White-Collar Crime**

**a. Performance Plan and Report for Outcomes**

To track its performance, the White-Collar Crime (WCC) program uses performance measures that concentrate on priority programs such as Mortgage Fraud, as well as traditional accomplishment data such as convictions and pre-trial diversions and the level of recoveries, restitutions, and fines generated by the WCC program.

***Performance Measure:***Number of Criminal Enterprises Engaging in White-Collar Crimes Dismantled.

***FY 2010 Target:*** 160

***FY 2010 Actual:*** 236

***Discussion:*** The FBI established the FY 2012 target based on past performance, the increased activity of WCC enterprises, particularly in Healthcare Fraud and Mortgage Fraud, as well as the increase in resources in FY 2011 and FY 2012. Securities, corporate and mortgage fraud investigations are frequently long term and resource intensive. Resources received in FY 2009 and FY 2010 are expected to result in numerous referrals and pre-trial diversions, and subsequent dismantlements, in FY 2012. Further, accomplishments in WCC can reach peaks at times when long term cases initiated in prior years come to conclusion.

***FY 2011 Target:*** 250

***FY 2012 Target:*** 275

***Efficiency Measure:***Percentage of Major Mortgage Fraud Investigations to all Pending

***FY 2010 Target:*** 69%

***FY 2010 Actual:*** 71%

***Discussion:*** The FBI continues to aim for maintaining 70 percent of pending investigations as major cases. The nature of the mortgage fraud threat and recent trends indicate that high loss schemes, schemes involving industry insiders and the sophisticated criminal enterprises will persist into FY 2012. The FBI also notes that the need still exists to investigate cases that have a strong community impact and which are likely to grow into major cases as more information is discovered. The FBI’s long term objective is to lower the incidence of mortgage fraud through detection, deterrence, and investigation so that the FBI can concentrate on neutralizing current and emerging financial threats, as well as financial industry fraud schemes which target our Nation’s financial institutions.

***FY 2011 Target:*** 70%

***FY 2012 Target:*** 70%

**b. Strategies to Accomplish Outcomes**

In FY 2012, the FBI will continue to pursue corporate fraud, securities fraud, mortgage fraud and other types of financial institution fraud, health care fraud, money laundering, and insurance fraud, which threaten to undermine our Nation's financial institutions. The FBI will aggressively utilize the money laundering and asset forfeiture statutes to ensure that fraudulently obtained funds are located and proper restitution is made to the victims of fraud. The enforcement strategy is a coordinated approach whereby the FBI will continue to work with other federal agencies to identify and target fraud schemes by successfully investigating, prosecuting, and obtaining judgments and settlements.

Innocent Images National Initiative

***Background/Program Objectives:*** Facilitation of crimes against children through the use of a computer and the Internet is a national crime problem that is growing dramatically. The Innocent Images National Initiative (IINI), part of the Cyber Division, uses the following performance measure to track its progress in combating the exploitation of children through the Internet. The FBI will continue to make efforts to apprehend those who commit sexual exploitation offenses against children, including those who traffic in child pornography.

The Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act of 2003 (the “PROTECT Act”), Pub. L. No. 108-066, 117 Stat. 650, was signed into law by President Bush in 2003 to enhance federal child exploitation laws in several significant ways. This law updated Title 42 USC §13032 - Reporting of Child Pornography by Electronic Communication Service Providers, which created a mandatory reporting requirement for electronic communication service providers, Internet Service Providers (ISPs), and remote computing service providers, to report violations of federal child pornography laws to any law enforcement agency and/or the National Center for Missing and Exploited Children (NCMEC). This law comes with a penalty of civil fines up to $50,000 per day per infraction that is not reported.

***Performance Measure:***  Number of children depicted in child pornography that are identified by the FBI.

*Note: FY 2006 data in chart are incomplete: data were only collected for part of that year.*

***FY 2010 Target:*** 130

***FY 2010 Actual:*** 246

***Discussion:***  This measure records all children identified through FBI investigations of child pornography, as well as through partnerships with organizations such as its work with NCMEC.

The number of victims identified and recovered by the FBI in FY 2010 is 246. However, this number is difficult to project from year to year depending on the types of cases we have. For example, in FY 2008, the FBI recovered 187 victims; whereas, one year later in FY09, the number of recovered victims decreased to 118.

One possible cause for the spike in FY 2010 is an open investigation in which, as of the close of the 2010 calendar year, approximately 66 victims had been recovered for this case alone; the number is continuing to climb in FY 2011. This is not a typical case, however. The FBI is beginning to see a larger volume in victims being exploited by single offenders (and single cases) due to advanced technology, social networking sites being hacked/manipulated, and the new wave of “sextortion.”

The FBI cannot directly control the number of children identified at any given time through investigative techniques. The FBI continues to take definitive action to negate any data limitations through its continued collaboration with the National Center for Missing & Exploited Children’s (NCMEC) Child Victim Identification Program (CVIP), and CyberTipline. The FBI is setting the FY 2011 target at 140 and the FY 2012 target at 155 because of investigatory techniques and continued collaboration and coordination between all Divisions of the FBI and with the National Center for Missing & Exploited Children (NCMEC)/Child Victim Identification Program (CVIP).

NCMEC/CVIP serves as the national clearinghouse for child pornography cases and the main point of contact to international agencies regarding victims of child pornography.

***FY 2011 Target:*** 140

***FY 2012 Target:***  155

Internet Fraud

***Background/Program Objectives:*** Internet fraud is any scam that uses one or more components of the Internet to present fraudulent solicitations to prospective victims, conduct fraudulent transactions, or transmit the proceeds of fraud to financial institutions or others that are connected with the scheme. Identity theft and Internet auction fraud are problems that plague millions of U.S. victims, and the threat of illegitimate online pharmacies exposes the American public to unregulated, often dangerous drugs.

The FBI and National White Collar Crime Center partnered in May 2000 to create the Internet Crime Complaint Center (IC3), a national repository for receipt and exchange of consumer, federal, and industry Internet crimes data. The IC3 allows for an enhanced capability for intelligence development to assist in these multi-divisional investigations. The FBI uses the IC3 data to develop law enforcement referrals focusing on Internet crimes with significant financial impact, large numbers of victims and/or social impact on Internet users. Periodically, the FBI synchronizes Nation-wide takedowns (i.e., arrests, seizures, search warrants, indictments) to target the most significant perpetrators of on-line schemes and draw attention to an identified crime problems.

***Performance Measure:***  Number of high-impact Internet fraud targets neutralized

***FY 2010 Target:*** 13

***FY 2010 Actual:*** 12

***Discussion:***  The FBI ranks cyber financial threats by the level of impact to the financial sector and the economy. The most significant cyber financial threats are highly sophisticated schemes involving intrusions into the computers of financial institutions; commercial and retail businesses; and, the computers, cell phones and other internet connected devices of consumers to collect and monetize personal identification and bank account information. The impact of these intrusions is rising dramatically; however, the FBI does not classify these cases as internet frauds. Internet frauds do not include the insertion of malware, phishing, spoofing or require complex computer hacking skills. Internet frauds are the utilization of the internet as a communications platform to execute traditional frauds. Examples would include emails soliciting funds for a fraudulent non-profit association or the solicitation of a law firm to assist in the collection of a debt in order to launder counterfeit checks through the law firm’s escrow account. While the FBI continues to address Internet fraud as part of its Cyber Program; as a stand-alone issue, Internet fraud rates as the Cyber Program’s lowest priority. Non-intrusion Internet fraud investigations decreased in number from FY 2009, consistent with FBI’s Cyber Program national strategy.

Victim complaints of non-intrusion Internet fraud reported directly to the FBI, or to the Internet Crime Complaint Center (IC3), which are able to be addressed by state and local authorities, are not routinely opened as FBI investigations.

In FY 2010, statistical accomplishments were claimed in 41 non-intrusion Internet fraud cases throughout the FBI. This included all types of accomplishments, such as individuals charged, arrested, convicted, sentenced, restitution imposed, recoveries, and fines. Of these, 24 cases involved the arrest of a total of 27 subjects. While the term “high-impact” is subjective, Cyber Division judges that 12 meet that description.

An example of a high-impact case that resulted from the consolidation of investigations in several field offices is Operation Pacific Wire. This case targeted a group of fraudsters that victimized 70 law firms throughout the U.S., United Kingdom, and Canada with a combined loss of $31 million. This case involved a bank in South Korea and subject in Nigeria. The subject was arrested by Nigerian authorities in late 2010. Extradition is pending.

***FY 2011 Target:*** 10

***FY 2012 Target:***  9

**b. Strategies to Accomplish Outcomes**

In its effort to thwart the online exploitation of children, the FBI will prioritize those investigations involving organizations, e-groups, or enterprises that exploit children for profit. The second priority will be cases involving U.S. travelers abroad. The third priority will be the producers, distributors, and possessors of child pornography. These priorities will be addressed by expanding current UCOs and undercover techniques to target and identify sexual predators and enterprises. The FBI also will develop and implement proactive initiatives designed to identify child victims and prevent exploitation before it can occur.

The FBI has formed the Innocent Images International Task Force (IIITF), where investigators from more than five countries are assigned to the Innocent Images program within the U.S. These international investigators are helping the FBI address this global crime problem. The current focus on several large international cases draws upon extensive resources, thus potentially diminishing the attention to shutting down individual websites.

The FBI will continue to aggressively pursue criminals that pose a threat to the national information infrastructure and, in the course of such endeavors, commit fraud. In cases that the Internet is but an instrumentality of a traditional fraud scheme, the FBI’s Cyber Program will continue to pursue only the most egregious, high-impact, and sophisticated non-intrusion schemes with an international nexus. Therefore, the FBI projects a modest, but sustained, reduction in its portfolio of traditional Internet fraud cases.

**Gang/Criminal Enterprises - Consolidated Priority Organization Targets (CPOT)**

With respect to criminal enterprises engaged in drug trafficking, the DOJ has developed a single national list of major drug trafficking and money laundering organizations. This list of targets, known as the CPOT list, reflects the most significant international narcotic supply and related money laundering organizations, poly-drug traffickers, clandestine drug manufacturers and producers, and major drug transporters supplying the U.S. The FBI tracked its own priority list, the National Priority Threat List (NPTL), before DOJ established the CPOT list in FY 2003.

The FBI has developed a comprehensive counter-drug strategy that is designed to investigate and prosecute illegal drug traffickers and distributors, reduce drug related crime and violence, provide assistance to other law enforcement agencies, and strengthen international cooperation. The strategy focuses the FBI's counter-drug resources on 69 identified CPOTs associated primarily with Colombian, Mexican, and Caribbean drug trafficking organizations that have the most adverse impact on U.S. national interests.

***Performance Measure:*** Percentage of FBI OCDETF Investigations with Links to CPOT-linked DTOs

***FY 2010 Target:***  12%

***FY 2010 Actual:*** 15.89%

***Discussion:*** Through involved complex and coordinated intelligence, analyzing drug investigative data and related financial data, CPOT-linked DTOs were identified. Resources focused on CPOT-linked membership who traffic in narcotics and launder illicit proceeds. Resources, expertise and unique investigative capabilities were utilized to target their infrastructure. The FBI participates in investigations of CPOT-linked DTOs through the OCEDTF program, and is investigating all 69 CPOTs. The target remains low as the FBI has additional capacity to investigate other drug groups that are not CPOTs.

***FY 2011 Target:*** 12%

***FY 2012 Target:*** 12%

***Performance Measure:*** CPOT-linked Drug Trafficking Organizations (DTOs) Disrupted

***FY 2010 Target:*** 30

***FY 2010 Actual:*** 40

***Discussion:***  CPOT-linked DTOs were disrupted through involved complex and coordinated intelligence driven investigations, analyzing drug investigative data and related financial data to effectively alter the operations of major trafficking organizations. Comprehensive strategic initiatives were developed to effectively exploit the DTO’s most vulnerable points, thus attacking their infrastructure. Our enforcement actions resulted in keeping multi-ton quantities of illegal drugs such as cocaine, heroin, marijuana and methamphetamine from ever entering the U.S..

***FY 2011 Target:*** 30

***FY 2012 Target:*** 30

***Performance Measure:*** CPOT-linked Drug Trafficking Organizations (DTOs) Dismantled

***FY 2010 Target:*** 15

***FY 2010 Actual:*** 12

***Discussion:***  Performance measure was not met for multiple reasons. 1) Investigations of CPOT-level organizations are complex and time-consuming, and the impact of dismantling such a network may not be apparent immediately. DTOs are typically assessed in the months that follow law enforcement actions to determine if they were truly dismantled, this assessment causes a reporting lag time. 2) Additionally we cannot rush law enforcement actions that would dismantle a criminal organization simply in pursuit of a performance statistic. Each investigation must reach a logical juncture whereat a dismantling law enforcement action is appropriate and warranted. Premature takedowns are detrimental to an investigation. 3) Furthermore, it is labor intensive to perform research and analysis associated with validating the CPOT linkage status of a criminal organization, delays in CPOT linkage verification impact our statistical claims.

***FY 2011 Target:*** 15

***FY 2012 Target:*** 15

**b. Strategies to Accomplish Outcomes**

Asian criminal enterprises (ACEs) are involved in criminal violations that include organized crime activities, such as murder, alien smuggling, extortion, loansharking, illegal gambling, counterfeit currency and credit cards, prostitution, money laundering, drug distribution, and various acts of violence. Loosely knit, flexible and highly mobile, ACEs have become more sophisticated, diverse, and aggressive in directing their activities, and profiting through legitimate and illegitimate businesses to avoid law enforcement attention and scrutiny. Russian/Eastern European/Eurasian criminal enterprise groups (ECEs) in the U.S. are engaged in traditional racketeering activity such as extortion, murder, prostitution, and drugs. Both ECEs and Middle Eastern criminal enterprise organizations are also deeply involved in large-scale white-collar crimes, such as gasoline excise tax scams, fraudulent insurance claims, stock fraud, and bank fraud. The strategy for the FBI’s Criminal Enterprise Program, encompassing both the Organized and the Gang/Criminal Enterprise Programs, emphasizes the development and focusing of resources on national targets, the use of the Enterprise Theory of Investigations, the enhanced use of intelligence, and the exploitation and development of FBI technical capabilities.

To address the threat that violent urban gangs pose on a local, regional, national and even international level, the FBI established a National Gang Strategy to identify the gangs posing the greatest danger to American communities, to combine and coordinate the efforts of the 163 local, state, and federal law enforcement in Violent Gang Safe Streets Task Forces throughout the U.S., and to utilize the same techniques previously used against organized criminal enterprises. The increasingly violent activity of MS-13, has prompted an FBI initiative that will assure extensive coordination between all field offices involved in the investigation of MS-13 matters. Additionally, due to a significant number of MS-13 gang members residing in Central America and Mexico, liaison with international law enforcement partners abroad will be a key part of the FBI’s strategy against this gang threat. In FY 2005, Congress approved funding for a National Gang Intelligence Center, which is being used as a mechanism for gathering data on violent gangs. In FY 2006, DOJ and DHS established the National Gang Tracking Enforcement Coordination Center (GangTECC), now known as Special Operations Division/Operational Section: Gangs (SOD/OSG), a multi-agencyinitiativeanti-gang enforcement, deconfliction, coordination and targeting center headed by a Director from the DEA and a Deputy Director from the FBI, and staffed with representatives from ATF, BOP, DEA, FBI, ICE and the USMS.

In order to make the most progress with the resources available, the FBI concentrates counter-narcotics resources against DTOs with the most extensive drug networks in the U.S. As entire drug trafficking networks, from sources of supply through the transporters/distributors are disrupted or dismantled, the availability of drugs within the U.S. will be reduced. To assess its performance in combating criminal enterprises that engage in drug trafficking, the Gang/Criminal Enterprise Program works in tandem with DEA and the Executive Office for OCDETF to track the number of organizations linked to targets on DOJ’s CPOT list.

**Organized Criminal Enterprises & Gangs/Criminal Enterprises**

**a. Performance Plan and Report for Outcomes**

Organized Criminal Enterprises

Investigative subprograms that focus on criminal enterprises involved in sustained racketeering activities and that are mainly comprised of ethnic groups with ties to Asia, Africa, the Middle East, and Europe are consolidated into the Organized Criminal Enterprise program. Organized criminal enterprise investigations, through the use of the Racketeering Influenced Corrupt Organization statute, target the entire entity responsible for the crime problem. With respect to groups involved in racketeering activities, the FBI focuses on: the Russian/Eastern European/Eurasian organized crime groups, Asian criminal enterprises, La Cosa Nostra and Italian organized crime groups, Balkan/Albanian Organized crime groups, Middle Eastern criminal enterprises and African criminal enterprises. Each of these groups is engaged in a myriad of criminal activities.

***Performance Measure:***Organized Criminal Enterprises Dismantled

***FY 2010 Target:*** 36

***FY 2010 Actual:*** 39

***Discussion:*** Based on the findings of the recently released National Intelligence Estimate (NIE) on International Organized Crime (IOC) that establishes that IOC activities are a threat to U.S. national security, the OCP has targeted The Brother’s Circle and Semion Mogilevich Organizations, which are the two highest priority IOC organizations that represent this national security threat. The OCP anticipates additional collection, the establishment of an additional 78 additional cases, the development of 52 additional CHS(s), and a 50 percent increase in IIR production. This will also include the initial targeting and operational activities against 10 percent of criminal bosses that support the associated Thieves and members of the Brother’s Circle, and will target the financial and communications avenues of the criminal enterprise already identified as potential vulnerabilities.

***FY 2011 Target:*** 37

***FY 2012 Target:*** 37

**Gang/Criminal Enterprises**

The mission of the FBI’s Gang/Criminal Enterprise Program is to disrupt and dismantle the domestic cells (local, regional, national, and transnational) of criminal enterprises, which pose the greatest threat to the economic and national security of the U.S. Many of these criminal enterprises have ties to North, Central and South America. This will be accomplished through the FBI’s Violent Gang and Drug Programs, increased involvement in the Organized Crime Drug Enforcement Task Force Program (OCDETF), and support and leadership of HIDTA initiatives. The majority of the FBI’s anti-gang efforts are directed towards the following identified priority threats: neighborhood based gangs, prison gangs, Mara Salvatrucha (MS-13), and outlaw motorcycle gangs. The FBI works closely with local, state, federal, and international law enforcement agencies to accomplish this mission.

The National Gang Intelligence Center (NGIC) is DOJ’s primary vehicle for collecting, collating, analyzing, evaluating and disseminating gang related information and intelligence. NGIC supports this mission by sharing, and coordinating information with both state and local law enforcement, as well as other federal law enforcement agencies. The NGIC analyzes gang intelligence from a broad spectrum to identify migration patterns and current trends involving gangs.

The Gang Targeting and Coordination Center (GangTECC) focuses on enhancing gang investigations of all federal agencies by acting as a deconfliction and case coordination center. GangTECC facilitates operations across agency lines and seeks to dismantle national and trans-national violent gangs. Tactical and strategic intelligence is shared between law enforcement agencies in conjunction with the NGIC and the Safe Streets and Gang Unit.

***Performance Measure:*** Gang/Criminal Enterprises Dismantled

Note: This measure does not include CPOT-linked dismantlements, which are recorded below.

***FY 2010 Target***: 99

***FY 2010 Actual:*** 124

***Discussion:***  DTOs were dismantled through involved complex and coordinated intelligence driven investigations, analyzing drug investigative data and related financial data to effectively alter the operations of major trafficking organizations and ultimately destroy them. Resources focused on coordinated, nationwide investigations targeting the entire infrastructure of major DTOs. DTO membership who traffic in narcotics and launder illicit proceeds were targeted. Strategic initiatives were developed to effectively exploit the DTO’s most vulnerable points, thus attacking their infrastructure. Our enforcement actions resulted in keeping multi-ton quantities of illegal drugs such as cocaine, heroin, marijuana and methamphetamine from ever entering the U.S.

xpendituresHCF program managersfor***FY 2011 Target:*** 99

***FY 2012 Target*:** 99

**D. Criminal Justice Services Decision Unit**

|  |  |  |  |
| --- | --- | --- | --- |
| **CRIMINAL JUSTICE SERVICES DECISION UNIT TOTAL** | **Perm. Pos.** | **FTE** | **Amount ($000)** |
| 2010 Enacted with Rescissions | 1,990 | 1,941 | $424,291 |
| 2011 Continuing Resolution | 2,091 | 2,042 | 483,276 |
| Adjustments to Base and Technical Adjustments | … | 7 | 8,454 |
| 2012 Current Services | 2,091 | 2,049 | 491,730 |
| 2012 Program Increases | … | … | 1,816 |
| 2012 Program Offsets | … | … | (2,363) |
| 2012 Request | 2,092 | 2,049 | 491,183 |
| **Total Change 2011-2012** | **1** | **7** | **$7,907** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Criminal Justice Services Decision Unit —Information Technology Breakout** | **Perm. Pos.** | **FTE** | **Amount**  **($000)** |
| 2010 Enacted w/Rescissions and Supplementals | 287 | 287 | $334,063 |
| 2011 Continuing Resolution | 284 | 284 | 482,707 |
| Adjustments to Base and Technical Adjustments | (33) | (33) | (99,240) |
| 2012 Current Services | 251 | 251 | 383,467 |
| 2012 Program Increases | … | … | … |
| 2012 Request | 251 | 251 | 383,467 |
| **Total Change 2011-2012** | **(35)** | **(35)** | **($99,240)** |

**1. Program Description**

The Criminal Justice Services (CJS) Decision Unit is comprised of all programs of the Criminal Justice Information Services (CJIS) Division, the portion of the Laboratory Division that provides criminal justice information and forensic services to the FBI's state and local law enforcement partners, and the state and local training programs of the Training Division. Additionally, to capture all resources that support the CJS program, a prorated share of resources from the FBI's support divisions (Security, Information Technology Operations, and the administrative divisions and offices) are calculated and scored to this decision unit.

***CJIS Division***

The mission of the CJIS Division is to equip our law enforcement, national security, and intelligence community partners with the criminal justice information they need to protect the U.S. while preserving civil liberties. The CJIS Division includes several major program activities that support this mission, all of which are described below.

Integrated Automated Fingerprint Identification System (IAFIS)/Next Generation Identification (NGI): IAFIS provides timely and accurate identification services in a paperless environment 24 hours a day, 7 days a week. The system identifies individuals through name, date-of-birth, other descriptors, and/or fingerprint image comparisons, and provides criminal history records on individuals for law enforcement and civil purposes. IAFIS is designed to process criminal fingerprint submissions in two hours or less and civil submissions in 24 hours or less. In Fiscal Year (FY) 2009, the FBI conducted over 52.7 million fingerprint background checks. In FY 2010, the FBI conducted over 61.2 million fingerprint background checks.

In FY 2008, the CJIS Division awarded a contract for the development and integration of the NGI system. NGI is a major upgrade and replacement to the current IAFIS. The FBI initiated the NGI Program in response to advances in technology, FBI customer requirements, growing demand for IAFIS services, and growing obsolescence of the IAFIS information technology infrastructure.  NGI advances the FBI’s biometric identification and investigation services, providing an incremental replacement of current IAFIS technical capabilities, while introducing new biometric functionality.  The NGI system will offer state-of-the-art biometric services and capabilities that will serve as a platform for multiple modes of biometric functionality.

NGI will be the cornerstone that enables the FBI to meet its criminal justice service mission and support the intelligence community, as well as, continue to build its reputation as a global leader in biometrics.  The FBI will dramatically improve all of the major features of the current IAFIS including system flexibility, storage capacity, accuracy and timeliness of responses, and interoperability with other systems - including DHS and DOD biometric matching systems.

National Crime Information Center (NCIC): The NCIC is a nationwide information system that supports local, state, tribal, federal, and international law enforcement agencies in their mission to uphold the law and protect the public. The NCIC allows for the compilation, dissemination, and exchange of timely and critical criminal justice and law enforcement information, such as wanted person information, stolen property information, sex offenders, immigration violators, terrorists, and other data. In FY 2009, the NCIC processed nearly 6.8 million transactions per day. On July 24, 2009, NCIC set a record by processing 7.9 million transactions in one day. In FY 2010, NCIC processed over 7.2 million transactions per day. On August 4, 2010, NCIC set a record by processing more than 9.1 million transactions in one day, as well as a record monthly daily average transaction volume of 8.0 million for the month of July.

National Instant Criminal Background Check System (NICS): The NICS is a national system established to enforce the provisions of the Brady Handgun Violence Prevention Act of 1993. The NICS allows Federal Firearms Licensees to determine whether receipt of a firearm by a prospective purchaser would violate state or federal law. The system ensures the timely transfer of firearms to individuals who are not specifically prohibited and denies transfer to prohibited persons. In FY 2009, the NICS processed over 14.4 million inquiries. The FBI conducted approximately 6.4 million of these checks, resulting in 70,656 denials to prohibited persons. The remaining 8 million checks were conducted by individual states. For FY 2010, the NICS processed over 14.1 million inquiries. The FBI conducted approximately 5.9 million of these checks, resulting in 70,972 denials to prohibited persons. The remaining 8.2 million checks were conducted by individual states.

Uniform Crime Reporting (UCR): The FBI’s UCR Program has served as the national clearinghouse for the collection of crimes reported to law enforcement since 1930. It is the CJIS Division of the FBI that collects, analyzes, reviews, and publishes the data collected from participating local, state, tribal, and federal law enforcement agencies. Information derived from the data collected within the UCR Program is the basis for the annual publications *Crime in the United States*, *Law Enforcement Officers Killed and Assaulted* (LEOKA), and *Hate Crime Statistics* that fulfill the FBI’s obligations under Title 28 United States Code Section 534. The publications provide statistical compilations of crimes such as murder, forcible rape, robbery, aggravated assault, burglary, larceny-theft, motor vehicle theft, and arson; officers killed and assaulted in the line of duty; and hate crime statistics. The UCR Program also conducts officer safety awareness training for the Nation’s law enforcement community based on the statistics and research collected in the UCR LEOKA Program.

Law Enforcement National Data Exchange (N-DEx): N-DEx offers services and capabilities to law enforcement through secure collection and processing of criminal justice data to combat crime, including violent crime and gang activity, as well as terrorism rooted in criminal activity. The N-DEx system is the result of collaboration among local, county, state, tribal and federal law enforcement communities to establish a secure, national, criminal justice information sharing capability. N-DEx interfaces with and enables queries of NCIC, the Interstate Identification Index (III), and OneDOJ. The integration of OneDOJ into N-DEx establishes an information sharing network currently containing over 100,000,000 searchable records. N-DEx Increment 1 became available in March 2008 and provided the ability to search nationwide incident and case reports. Deployed in July 2009, Increment 2 provided N-DEx users with additional capabilities including subscription, notification, collaboration, geographic search, and automated processing. Increment 3 will be delivered in February 2011 and will provide "Google-like" search capability with the same refined results and much less effort by the user, continue advancement of integration of N-DEx and OneDOJ, and add probation and parole data and an expansion of web services.

Law Enforcement On-line (LEO): LEO is a 24-hour-a-day, 7-day-a-week, on-line (real time), information-sharing system that is accredited and approved by the FBI for the transmission of sensitive but unclassified information throughout the world to the local, state, and federal law enforcement, criminal justice, and public safety communities. The LEO system provides a vehicle for these communities to exchange information, conduct online education programs, and participate in professional special interest and topically focused dialog. LEO provides law enforcement and criminal justice communities a secure “anytime and anywhere” national and international method to support antiterrorism, intelligence, investigative operations, sends notifications and alerts, and provides an avenue to remotely access other law enforcement and intelligence systems and resources. LEO also provides a “badge blind” incident management system, the LEO Virtual Command Center (VCC), which allows all levels of law enforcement to securely share critically needed information in real time across any Internet connection in order to provide safety and security at all major events and natural disaster areas. LEO currently supports a user base of over 177,000 vetted members that can access LEO through any connection to the Internet such as cable modem, Digital Subscriber Line, Local Area Network, or dial-up Internet service provider. LEO operates as a sensitive but unclassified network under the Federal Information Security Management Act and Privacy Act. LEO provides a common communications link to all levels of law enforcement and criminal justice by supporting broad, immediate dissemination and exchange of information.

***Laboratory Division***

A portion of the Laboratory Division programs that provide forensic services to the FBI's state and local law enforcement partners is scored in the CJS Decision Unit.

The successful investigation and prosecution of crimes require the collection, examination, and scientific analysis of evidence recovered at the scene of the incident and obtained during the course of the investigation. Without such evidence, many crimes would go unsolved and unpunished. At the same time, forensic examination of evidence exonerates individuals wrongly accused of crimes.

The FBI Laboratory, established in 1932, is the only full-service civilian federal forensic laboratory in the U.S. The FBI Laboratory was accredited in August 2008 by the American Society of Crime Laboratory Directors – Laboratory Accreditation Board (ASCLD-LAB) for meeting or exceeding the requirements for *international* accreditation (ISO/IEC 17025). Examinations support investigations that cross all FBI investigative programs, international, federal, state, and local boundaries. Examinations of evidence for duly constituted U.S. law enforcement agencies, whether federal, state or local, and foreign law enforcement unable to perform the examinations at their own facilities are performed, free of charge. In addition to the actual processing and analysis of physical evidence, the FBI Laboratory provides comprehensive technical reports, training, and expert testimony to federal, state, and local agencies.

In addition to providing forensic analysis services, the FBI Laboratory also provides operational response capabilities with respect to chemical, biological, nuclear, radiological and explosive devices/incidents and evidence collection. Biometric identification services are provided through the Combined DNA Index System (CODIS) and the Federal Convicted Offender Program (FCOP). The FBI Laboratory is the executive agent for the Terrorist Explosive Devices Analytic Center (TEDAC), a multi-agency center that forensically and technically exploits terrorist improvised explosive devices and related materials and generates actionable investigative and intelligence information for use by the U.S. law enforcement, the Intelligence Community, the U.S. military, and other partners.

In FY 2010, the FBI conducted approximately 635,000 forensic examinations (FBI, other Federal, state, and local). The Laboratory estimates it will conduct approximately 633,000 forensic examinations in FY 2011 and in FY 2012, respectively.

***Training Division***

The FBI provides instruction for state and local criminal justice practitioners, both at the FBI Academy and throughout the U.S. at state, regional, and local training facilities. The principal course for state and local law enforcement officers is the FBI National Academy, a 10-week multi-disciplinary program for officers who are considered to have potential for further advancement in their careers. In FY 2010, there were 1,059 state and local law enforcement officers that participated in the National Academy program at the FBI Academy in Quantico, Virginia. The FY 2011 estimate for National Academy participants is 1,000.

In addition to sessions offered at the FBI Academy, the FBI conducts and participates in courses and seminars at state, regional, and local training facilities. These training sessions cover the full range of law enforcement training topics such as hostage negotiation, computer-related crimes, death investigations, violent crimes, criminal psychology, forensic science, and arson. In FY 2010, an estimated 97,000 criminal justice personnel received training from FBI instructors at state, regional, and local training facilities. TD estimates that the FBI will train 97,000 criminal justice personnel in FY 2011.

Due to the increasingly global nature of many of the FBI's investigative initiatives, the FBI has in recent years emphasized the need to train its foreign law enforcement partners through the International Training and Assistance Program. In FY 2010, the FBI provided training to 5,853 international police officers and executives representing 118 countries. It is expected that there will be 5,000 international police officers trained in FY 2011.

**Program Objectives**

* Reduce criminal activity by providing timely and quality criminal justice information to federal, state, and local law enforcement agencies.
* Provide new technologies and address critical shortfalls in forensic investigative capabilities including latent fingerprint, firearms/toolmark, explosive, trace evidence, DNA, and training of personnel.
* Lead and inspire, through excellence in training and research, the education and development of the criminal justice community.

| **PERFORMANCE /RESOURCES TABLE** | | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Decision Unit:** Criminal Justice Services | | | | | | | | | | | |
| **DOJ Strategic Goal/Objective** Goal 2: Prevent Crime, Enforce Federal Laws, and Represent the Rights and Interests of the American People (Objective 2.1: Strengthen partnerships for safer communities and enhance the Nation’s capacity to prevent, solve, and control crime) | | | | | | | | | | | |
| **WORKLOAD/ RESOURCES** | | **Final Target** | | **Actual** | | **Projected** | | **Changes** | | **Requested (Total)** | |
| **FY 2010** | | **FY 2010 Enacted** | | **FY 2011** | | **Current Services Adjustments & FY2012 Program Changes** | | **FY 2012 Request** | |
| IAFIS fingerprint background checks | | 89,019,199 | | 61,244,186 | | 68,050,000 | | 4,085,000 | | 72,135,000 | |
| NCIC transactions | | 2,728,841,676 | | 2,645,868,617 | | 2,920,280,283 | | 67,754,863 | | 2,988,035,146 | |
| Total number of federal, state, and local investigations aided by the Combined DNA Index System (CODIS) | | † | | 23,789 | | † | | † | | † | |
| Total number of forensic and offender matches identified at CODIS | | † | | 26,349 | | † | | † | | † | |
| **Total Costs and FTE** | | **FTE** | **$000** | **FTE** | **$000** | **FTE** | **$000** | **FTE** | **$000** | **FTE** | **$000** |
| 1,941 | 424,291 | 1,904 | 621,864 | 2,042 | 483,276 | 7 | 8,454 | 2,049 | 491,730 |
| **TYPE/**  **STRATEGIC OBJECTIVE** | **PERFORMANCE** | **FY 2010** | | **FY 2010** | | **FY 2011** | | **Current Services Adjustments & FY2012 Program Changes** | | **FY 2012 Request** | |
| **Efficiency Measures** | **IAFIS: (*Discontinued Measure)***  % of electronically submitted fingerprint identification requests:  Criminal:   * General checks completed w/in 2 hours * DHS checks completed w/in 72 hours   Civil:   * General checks completed w/in 24 hours * DOS checks completed w/in 15 minutes | 95.0%  95.0%  99.0%  97.0% | | 99.32%  99.51%  99.70%  99.11% | | 95.0%  95.0%  99.0%  97.0% | | --  --  -- | | N/A  N/A  N/A  N/A | |
| **Performance Measure** | **IAFIS/NGI:** *(New Measures)*   * Average daily identification searches (excluding CBP searches) * Average daily latent searches * Response time for routine criminal submissions * Response time for routine civil submissions | 177,000  568  2 hours  24 hours | | Avg=132,064  (One day Max=243K)  682  8 min 42 sec  55 min 24 sec | | 191,000  624  2 hours  24 hours | | 20,000  62  1 hour  12 hours | | 211,000  686  1 hour  12 hours | |
| **Performance Measure** | **NCIC:**   * System availability * Downtime in minutes | 99.7%  1,440 | | 99.79%  1,152 | | 99.7%  1,440 | | 0%  0 | | 99.7%  1,440 | |
| **Performance Measure** | **NICS:**  % of NICS checks with an Immediate Determination | 90.0% | | 91.36% | | 90.0% | | 0 | | 90.0% | |
| **Performance Measure** | Student-weeks of Instruction at the Hazardous Devices School (HDS) | 2,668 | | 2,326 | | 2,668 | | 0 | | 2,668 | |
| **Performance Measure: *Customer Satisfaction*** | LEO:% of users who visit the Law Enforcement Online (LEO) service (which provides intelligence dissemination) more than one month out of each year. | 44% | | 45% | | 44% | | 2% | | 46% | |
| **Data Definition, Validation, Verification, and Limitations:**   * IAFIS Response Times are captured automatically from in-house developed software code residing on the Electronic Fingerprint Transaction Standard (EFTS) Fingerprint Conversion (EFCON) System. The software that captures this information, time stamps all incoming and out-going transactions and produces a report that calculates transaction response times. The developed code for this requirement was rigorously tested through System Integration and Test (SIT) prior to being put into operations. The information produced by EFCON was validated using Transaction Status (TS), a contractor developed statistical capture program that runs on the Integrated Automated Fingerprint Identification System. The data collected from EFCON is imported into a spreadsheet to calculate the average response time and percentage for electronic criminal and electronic civil responses. CJIS Division staff review this information prior to release. * NCIC Transaction Volumes are captured similarly to the IAFIS Response Time statistics in that they are also capture automatically from developed code. This program was developed as a requirement by a contractor during the development of the NCIC 2000 system. The developed code for this requirement was also rigorously tested through System Integration and Test (SIT) prior to being put into operations. The information produced in the NCIC reports is also validated by CJIS Division staff prior to release. * System Availability data are collected manually from System Management Center (SMC) logs. System Availability is based on the time that a system is out of service until it is returned to service as recorded by SMC personnel. CJIS Division staff input the information into spreadsheets that calculate percent averages. The algorithms used within the spreadsheets were validated prior to being used by in-house personnel. The System Availability figures are tracked closely on a weekly basis by Systems Managers and the Section Chief in charge of the operations and maintenance of the CJIS Division's systems. * HDS data are maintained in central files and databases located at the HDS. The HDS Program Administrator reviews and approves all statistical accomplishment data for dissemination.   † DOJ is no longer requesting estimates for these data. Actual data will be reported as current workload only during the Budget Submission to the Congress. | | | | | | | | | | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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** |
| **Efficiency Measures** | **IAFIS:**  % of electronically submitted fingerprint identification requests:  Criminal:   * General checks completed w/in 2 hours * DHS checks completed w/in 72 hours   Civil:   * General checks completed w/in 24 hours * DOS checks completed w/in 15 minutes | 91.6%  N/A  97.5%  N/A | 94.8%  N/A  99.2%  N/A | 96.5%  N/A  99.2%  N/A | 97%  N/A  98%  N/A | 98.0%  N/A  98.8%  N/A | 97.9%  N/A  98.5%  N/A | 98.2%  100%  98.8%  99.7% | 95.0%  95.0%  99.0%  97.0% | 99.32%  99.51%  99.70%  99.11% | 95.0%  95.0%  99.0%  97.0% | N/A  N/A  N/A  N/A |
| **Performance Measure** | **IAFIS/NGI:** *(New Measures)*   * Average daily identification searches (excluding CBP searches) * Average daily latent searches * Response time for routine criminal submissions * Response time for routine civil submissions | N/A  N/A  N/A  N/A | N/A  N/A  N/A  N/A | N/A  N/A  N/A  N/A | N/A  N/A  N/A  N/A | N/A  N/A  N/A  N/A | N/A  N/A  N/A  N/A | N/A  N/A  N/A  N/A | 177,000  568  2 hours  24 hours | 132,064  682  8m 42s  55m24s | 191,000  624  2 hours  24 hours | 211,000  686  1 hour  12 hours |
| **Performance Measure** | **NICS:**  % of NICS checks with an Immediate Determination | 91.23% | 91.85% | 91.45% | 91.46% | 91.63% | 91.66% | 91.9% | 90% | 91.36% | 90% | 90% |
| **Performance Measure** | **NCIC:**   * System availability * Downtime in minutes | 99.7%  1,788 | 99.7%  1,606 | 99.7%  1,602 | 99.8%  1,277 | 99.8%  1,267 | 99.8%  1,138 | 99.8%  1,028 | 99.7%  1,440 | 99.79%  1,152 | 99.7%  1,440 | 99.7%  1440 |
| **Performance Measure: *Customer Satisfaction*** | LEO:% of users who visit the Law Enforcement Online (LEO) service (which provides intelligence dissemination) more than one month out of each year. | N/A | N/A | 45% | 39% | 26% | 41% | 42% | 44% | 45% | 44% | 46% |
| **Performance Measure** | Student-weeks of Instruction at the Hazardous Devices School (HDS) | 2,245 | 2,304 | 2,593 | 2,614 | 2,159 | 2,605 | 2,437 | 2,668 | 2,326 | 2,668 | 2,668 |

**2. Performance, Resources, and Strategies**

The Criminal Justice Services decision unit contributes to the Department of Justice’s Strategic Goal 2, “Prevent Crime, Enforce Federal Laws, and Represent the Rights and Interests of the American People.” Within this goal, the resources specifically support Strategic Objective 2.1, “Strengthen partnerships for safer communities and enhance the Nation’s capacity to prevent, solve, and control crime.” This decision unit ties directly to the FBI’s ninth priority: Support federal, state, local, and international partners.

**a. Performance Plan and Report for Outcomes**

**Integrated Automated Fingerprint Identification System/Next Generation Identification**

Fingerprint identification, which includes the processing of fingerprint submissions and criminal history records, has been a responsibility of the FBI since 1924. With an ever-increasing demand for fingerprint services, the FBI set out to automate its fingerprint identification operations, and on July 28, 1999, it launched the Integrated Automated Fingerprint Identification System (IAFIS). Since its inception, the IAFIS has dramatically improved the processing of fingerprint submissions, reducing typical response times for electronic criminal and civil submissions to two hours and twenty-four hours, respectively. In 2010, the Criminal Justice Information Services (CJIS) Division averaged 167,000 fingerprint submissions daily.

The FBI’s CJIS Division in Clarksburg, West Virginia manages the IAFIS. The IAFIS is a national fingerprint and criminal history system. The IAFIS provides automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses, 24 hours a day, 365 days a year.

In FY 2008, the CJIS Division awarded a contract for the development and integration of the Next Generation Identification (NGI) system. The FBI initiated the NGI Program in response to advances in technology, FBI customer requirements, growing demand for IAFIS services, and growing obsolescence of the IAFIS information technology infrastructure.  NGI advances the FBI’s biometric identification and investigation services, providing an incremental replacement of current IAFIS technical capabilities, while introducing new biometric functionality.  The NGI system will offer state-of-the-art biometric services and capabilities that will serve as a platform for multiple modes of biometric functionality.

NGI will be the cornerstone that enables the FBI to meet its criminal justice service mission and support the intelligence community, as well as, continue to build its reputation as a global leader in biometrics.  The FBI will dramatically improve all of the major features of the current IAFIS including system flexibility, storage capacity, accuracy and timeliness of responses, and interoperability with other systems - including DHS and DOD biometric matching systems.

The NGI Program Office manages this development effort and continues to keep FBI, DOJ, and OMB aware of their progress. Meetings are held regularly with these entities to discuss cost, schedule, and contract performance.  One of the follow-up action items received from the Federal CIO specifically requested that NGI update milestones and performance measures.

The measures listed below are based on historical system data, current system improvements, as well as the deployment of NGI Initial Operating Capability in March 2011. The target projections change due to the incremental deployment of new functionality and the anticipated increase in usage.

***Performance Measure:*** NEW MEASURE: Average daily identification searches (excluding CBP searches)

***FY 2010 Target:*** 177,000

***FY 2010 Actual:*** 132,064

***Discussion:*** Measures the number of identification searches being conducted by the CJIS Division. The targets are based on historical system data, current system improvements, as well as the deployment of NGI Initial Operating Capability in March 2011. The target projections increase due to the incremental deployment of new functionality and the anticipated increase in usage. Actual FY 2010 outcome was an average of 132,064 daily identification searches, with a maximum of 243,000 processed in one day. The FY 2010 Target was not met due to the fact that the FY 2010 Target included a higher projected number of transactions for projected new business workloads than was actually received.

***FY 2011 Target:*** 191,000

***FY 2012 Target:*** 211,000

***Performance Measure:*** NEW MEASURE: Average daily latent searches

***FY 2010 Target:*** 568

***FY 2010 Actual:*** 682

***Discussion:***  Measures the average daily number of latent investigative searches processed by the CJIS Division. The targets are based on historical system data, current system improvements, as well as the deployment of NGI Initial Operating Capability in March 2011. The target projections increase due to the incremental deployment of new functionality and the anticipated increase in usage.

***FY 2011 Target:*** 624

***FY 2012 Target:*** 686

***Performance Measure:*** NEW MEASURE: Response time for routine criminal submissions

***FY 2010 Target:*** 2 hour

***FY 2010 Actual:*** 8 minutes 42 seconds

***Discussion:*** Measures how quickly the CJIS Division responds to routine criminal submissions from state, local, and federal criminal justice entities. The targets are based on historical system data, current system improvements, as well as the deployment of NGI Initial Operating Capability in March 2011. The target projections decrease due to the incremental deployment of new functionality and the anticipated increase in usage.

***FY 2011 Target:*** 2 hour

***FY 2012 Target:*** 1 hour

***Performance Measure:*** NEW MEASURE: Response time for routine civil submissions

***FY 2010 Target:*** 24 hours

***FY 2010 Actual:*** 55 minutes 24 seconds

***Discussion:*** Measures how quickly the CJIS Division responds to routine civil submissions for positions of trust, employment, and licensing purposes. The targets are based on historical system data, current system improvements, as well as the deployment of NGI Initial Operating Capability in March 2011. The target projections decrease due to the incremental deployment of new functionality and the anticipated increase in usage.

***FY 2011 Target:*** 24 hours

***FY 2012 Target:*** 12 hours

***Performance Measure:*** DISCONTINUED MEASURE: Percentage of criminal electronic fingerprint identification checks submitted by the Department of Homeland Security completed within 72 hours

***FY 2010 Target:*** 95%

***FY 2010 Actual:*** 99.51%

***Discussion:*** In December 2007, the Department of Homeland Security (DHS) and the FBI agreed that criminal fingerprint submissions from ports of entry would be processed within 72 hours.

***FY 2011 Target:*** 95%

***Performance Measure:*** DISCONTINUED MEASURE: Percentage of civil electronic fingerprint identification checks submitted by the Department of State completed within 15 minutes.

***FY 2010 Target:*** 97%

***FY 2010 Actual:*** 99.11%

***Discussion:*** In November 2007, the Department of State and the FBI agreed that civil submissions from consulates would be processed within 15 minutes.

***FY 2011 Target:*** 97%

### *Performance Measure -- Customer Satisfaction:* % of users who visit the Law Enforcement Online (LEO) service (which provides intelligence dissemination) more than one month out of each year out of the total user base of over 177,000 vetted members.

***FY 2010 Target:*** 44%

***FY 2010 Actual:***  45%

***Discussion:***  This measure serves as a proxy for customer satisfaction. Repeated use of LEO is a strong indication that customers (other intelligence agencies, state and local law enforcement, etc.) find the information they are obtaining on the site useful. FY 2005 actual performance was uncharacteristically high-usage numbers were artificially driven up by the occurrence of the London subway bombings and a domestic emergency response training exercise in 2005. Later targets do not assume any repeat event-based surges in user levels, but, if future performance continues to trend high, the targets will be adjusted accordingly.

The FBI has developed new customer satisfaction surveys for its finished and raw intelligence products, which will ultimately provide data to replace the current customer satisfaction measure. Complete automation of the surveys is expected by the end of FY 2011. Currently, the FBI is upgrading the information sharing websites upon which the survey will be made available to customers. FBI will track initial data collections to see if sufficient feedback is captured. When the FBI feels that the administration of the surveys gets a sufficient volume of feedback, the FBI will use the data provided to replace the current customer satisfaction measure. Until then, the current measure based on LEO data will be used for reports to DOJ and ODNI.

In addition to the new customer satisfaction surveys to be used in the near future, LEO is in the process of creating a reporting tool. This reporting tool will provide these performance measures more accurately and is scheduled to be available for use by the end of the 3rd quarter FY 2011.

### *FY 2011 Target:* 44%

### *FY 2012 Target:* 46%

**Hazardous Devices School (HDS)**

Two key elements of domestic preparedness are expertise in hazardous devices and emergency response capabilities to address threats such as weapons of mass destruction (WMD). The HDS is the only formal domestic training school for state and local law enforcement to learn safe and effective bomb disposal operations. The HDS prepares bomb technicians to locate, identify, render safe, and dispose of improvised hazardous devices, including those containing explosives, incendiary materials, and materials classified as WMD.

***Performance Measure:*** State and Local Bomb Technicians Trained (# of student-weeks) at the HDS

***FY 2010 Target:*** 2,668

***FY 2010 Actual:*** 2,326

***Discussion:***  FY 2010 target was not met. The target number was based on the assumption that the Electronic Measures (ECM) and other advanced courses would be conducted. During the FY, these courses were not conducted. The amount of projected training in FY 2012 is based upon funding which drives the frequency of training courses available, duration of training courses, and the number of courses that can be offered per FY. For FY 2011 and FY 2012, if the ECM courses, and advanced classes in the Stabilization Program are conducted, the targets can be met. The HDS program is a reimbursable inter-service support agreement between the FBI and the U.S. Army.

***FY 2011 Target:*** 2,668

***FY 2012 Target:*** 2,668

**b. Strategies to Accomplish Outcomes**

Through its Laboratory Division, the FBI strives to provide timely, high-quality forensic science services (i.e., examinations, reports, testimony, and support to law enforcement partners across all levels of government) to its customers consistent with the FBI’s priorities. As the presence of terrorist cases persists, the Laboratory Division’s workload increases not only in terms of the examination of the volume of evidence, but in the administrative aspects associated with the volume of physical evidence. The FBI Federal Convicted Offender Program (FCOP) was expanded to comply with the DNA Fingerprint Act of 2005, which requires persons arrested, charged with or convicted of any federal felony to be included in the National DNA Index System (NDIS). In addition, NDIS includes an index for DNA profiles from relatives of missing persons and known reference DNA profiles of missing children.

The FBI’s Criminal Justice Information Services Division (CJIS) provides law enforcement and civil identification and information services with timely and critical information that matches individuals with their criminal history records, criminal activity (e.g., stolen property, gang or terrorist affiliation, fugitive status, etc.), and latent fingerprints, and provides information used for employment, licensing, or gun purchase consideration. To meet future demand, such as civil fingerprint-based background checks for employment, licensing, and border entry, CJIS needs to significantly increase its systems capacity. Automation and computer technology inherently require constant upgrading and enhancement if such systems are to remain viable and flexible to accommodate changing customer requirements.

CJIS’ National Instant Criminal Background Check System (NICS) is tracked against two performance standards: the Attorney General’s (AG) mandate of an Immediate Determination Rate (IDR) of 90 percent, and the Brady Act’s three business day deadline for a final determination. Current plans are to request the necessary funded staffing level to process increased workloads to ensure the NICS is able to meet both performance goals.

The FBI HDS provides state-of-the-art technical intelligence to state, local, and federal first responders in five separate courses regarding the criminal and terrorist use of improvised explosive devices (IEDs) and the tactics, techniques, and procedures to render these hazardous devices safe. As the U.S. Government's only civilian bomb disposal training facility, HDS provides training on emerging threats targeting the U.S. and its interests. This training includes countermeasures targeting suicide bombers, vehicle borne IEDs, stand-off weapons, WMD devices, and radio-controlled IEDs. To meet future demand for the training of first responders, HDS needs to add additional courses and increase student capacity to significantly impact the preparedness of our first-responder public safety bomb squads throughout the country. HDS is meeting the FBI's number one priority of terrorism prevention.

**Threat Name: Computer Intrusions**

Budget Decision Unit(s): All

Strategic Goal(s) & Objective(s): 1.1, 1.2, 1.4, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6

FBI SMS Objective(s): A-01, A-02, A-04, P-04, P-05, P-06, P-07, P-08

Organizational Program: Cyber, Operational Technology

Program Increase: Positions 42 Agt 14 FTE 20 Dollars $18,628,000 ($6,552,000 non-personnel)

Description of Item

The FBI requests 42 positions (14 Agents) and $18,628,000 ($6,552,000 non-personnel) to enhance its investigatory capabilities and protect critical technology network infrastructure from malicious cyber intrusions. This request includes two parts - the Comprehensive National Cybersecurity Initiative and digital forensics.

Justification

*Threat Summary*

Attacks against the U.S. information infrastructure are a grave threat to our national and economic security. All key sectors and critical infrastructures rely heavily on computers and computer networks, many of which are connected to the Internet. Terrorist groups, hostile foreign intelligence services, and transnational criminal actors target these computer networks to disrupt critical infrastructures, steal secrets and intellectual property, manipulate critical data, and perpetrate fraud and other crimes.

Despite numerous efforts across the government and private sector, the volume of the activity conducted by these actors continues to increase. In 2010, through the Internet Crime Complaint Center (IC3) website, the FBI received over 300,000 complaints from victims with reported losses of nearly $1.4 billion, resulting in more than double the loss reported in 2009. Globally, the 2008 losses due to data theft and cybercrime have been estimated in excess of $1 trillion.[[3]](#footnote-3) As alarming as these trends may be, the most recent National Computer Security Survey conducted by the Department of Justice reported that only 15 percent of all cyber crime incidents are reported to Law Enforcement[[4]](#footnote-4), suggesting that the scale of the problem is likely far worse than reported.

The sophistication of organized actors has also increased as the exploitation of computer networks proves to be both lucrative and low risk. As an example, in one well publicized case, the FBI and U.S. Secret Service (USSS) uncovered a criminal enterprise that spent over a year compromising and subverting financial computer networks and attacked more than 350 financial institutions before being detected. Through these well-planned attacks, the criminals orchestrated a heist, withdrawing over $9 million from ATMs in 28 countries, all within a 24 hour period. Because the financial computer network was manipulated in this attack, safeguards failed and at least one bank lost more money than it had in assets and ultimately went bankrupt.

**The Role of the FBI**

The FBI is in a unique position to counter cyber threats as the only agency with the statutory authority, expertise, and ability to combine intelligence, counterterrorism, counterintelligence, and criminal pursuit resources in support of the Comprehensive National Cybersecurity Initiative (CNCI) and other national cyber goals. The FBI Cyber Division leads a robust and mature cyber program focused on investigating computer intrusion activity. This program leverages a number of other FBI programs, which provide a comprehensive portfolio of cyber-related services, ranging from investigative tool research and development to media forensics, malicious code analysis, lawful electronic surveillance collection, and tactical and strategic intelligence analysis and production. A significant portion of the CNCI investment in the FBI focuses on strengthening these supporting elements, increasing their capacity, speed, and agility. Although the FBI coordinates extensively with United States Intelligence Community (USIC) partners, the implications of domestic laws and differences in domestic technologies introduce many challenges unique to the FBI.

Within the evolving cybersecurity landscape, investments have traditionally focused on securing and hardening networks to eliminate computer vulnerabilities exploited by criminals and national security threat actors. Investments have also concentrated on detecting and stopping threats active on the network, before they can cause significant harm.

The investments in the FBI and other cyber threat investigation (CTI) efforts focus on the attribution, pursuit, and mitigation of threat organizations and threat actors. Simultaneously, the FBI disseminates information about our adversaries’ targets and techniques to better assist network defenders.

**Major Strategy Components**

The National Cyber Investigative Joint Task Force (NCIJTF) is a Presidentially mandated and well recognized alliance of peer government organizations with complementary missions to protect national cyber interests. The NCIJTF identifies, mitigates, and neutralizes cyber threats by coordinating and integrating the counterintelligence, counterterrorism, intelligence, and law enforcement activities of member organizations. The NCIJTF enables unified, strategic actions to be taken across all partner agencies to reach desired outcomes. The FBI is both the executive agent for the NCIJTF and a key member of the NCIJTF forum.

This enhancement will enable the FBI to further leverage the FBI-led NCIJTF as a focal point to coordinate CTI activity, discover and communicate pertinent investigative data, and leverage analytic tools and techniques from across the USIC and CTI community. Through the NCIJTF and its member agencies, the FBI will integrate and share the gains of CTI with the rest of the USIC to enable stronger situational awareness and a broader portfolio of opportunities.

The additional funding and positions will also strengthen the FBI intelligence gathering and investigative missions as they pertain to cyber to exploit opportunities at hand, operate more strategically, increase efficiency, and better serve the Nation. This includes bolstering existing cyber agent, analyst and support resources and making investments in the research and development of new investigative tools to enable lawful surveillance, correlated forensic, technical and intelligence analysis, and proactive investigative operations.

The FBI cyber investment strategy builds upon a threat-centric approach. In the cyber domain, the elements that make up an investigation can be scattered across the country or around the globe. The borderless nature of CTI makes coordination and workload management across geographically structured agencies, such as the FBI and other NCIJTF partners, particularly challenging. This differs from traditional crimes where physical evidence, victim, threat actor, and criminal enterprise are commonly within the same geographical region. This difference has challenged traditional investigative processes and cross-field office coordination efforts. To overcome these challenges, the NCIJTF and FBI developed the “*Five Pillar*” approach for conducting CTI, as first presented in the FY 2011 FBI CNCI enhancement request.

The *Five Pillar* model divides the elements of the investigation into interdependent, but independently assignable efforts.

The pillar approach is threat adversary-centric, not technology-centric. Similar strategies apply to organized crime, terrorist, and nation-state threats outside of the cyber domain as well. Managing cyber threats under this model is a continual and iterative process, and although each pillar builds on the previous, the FBI and its partners cannot stop activity in one pillar when investigative efforts mature to the next. Similarly, understanding the portfolio of community activities across all pillars provides a strategic perspective of the impact the FBI is having and helps to measure the maturity of the program. Over time, the FBI must continue to invest in a strong foundation in pillars I-III in order to enable high impact outcomes in pillars IV and V. With this enduring strategy in mind, the *Five Pillar* model remains the basis for the Computer Intrusions Program (CIP) strategy and enhancement request.

*Justification for Program Increases*

**Comprehensive National Cybersecurity Initiative – 19 positions (14 Agents) and $11,199,000 ($6,552,000 non-personnel)**

*Increase coverage of Cyber-Terrorist threats – 8 positions (8 Agents) and $4,464,000 ($2,200,000 non-personnel)*

Terrorist actors are increasingly using the Internet as a forum to recruit and plan actions. To date, the use of the Internet as a means of attack has been limited to website defacements, denial of service events, and other activities of limited consequence. However, terrorist actors have growing access to skilled hackers that are capable of planning and developing more complex and devastating attacks. Based on previous activities, likely targets may include domestic critical infrastructures and financial networks. Because of the expanding nature of the threat, additional agents and ELSURS are required to address the increasing workload and ensure the FBI’s efforts are proactive rather than reactive.

*Establish NCIJTF 24x7 Operations – 5 positions (5 Agent) and $3,415,000 ($2,000,000 non-personnel)*

The FBI seeks to move the NCIJTF from an 8x5 operation to a 24x7 operation. This request includes the additional government (5 Agents) and contract staff needed to provide minimal after-hours coverage for essential analysis of ELSUR feeds of interest, coordinating member agency efforts, and maintaining contact with other cybersecurity centers.

As one of the six cybersecurity centers identified under the CNCI, the NCIJTF plays an important role in coordinated national cybersecurity operations. With threat actors operating globally, a significant volume of cyber threat activity occurs outside of normal business hours. To date, the NCIJTF has leveraged alternate work schedules and overtime to meet after-hours requirements. However, with the ever increasing need for real-time analysis to support operations and provide program management for multi-agency efforts, as well as to match the operational tempo of other cybersecurity centers, the NCIJTF now requires an after-hours presence. The 24x7 capabilities have been identified as an anticipated, but unfunded requirement as part of the FBI’s CNCI quarterly reporting, also driven by the CNCI *Connect the Centers* initiative, and the need for continual coordination with the DHS National Cybersecurity Center (NCSC).

Without this enhancement, the FBI will not be able to maintain effective coordination of after-hours efforts, maintain after-hours situational awareness, or maintain operational engagement with other 24x7 centers.

*Advance Electronic Surveillance capabilities – 6 positions (1 Agent) and $3,320,000 and ($2,352,000 non-personnel)*

Digital Forensics – 23 positions (all support) and $7,429,000 (all personnel)

Description of Item

The FBI requests 23 positions (all support) and $7,429,000 (all personnel) to improve analysis of digital evidence. The FBI’s Digital Forensics program supports the analysis of digital evidence through the Computer Analysis Response Team (CART). This program lacks the resources to keep pace with the use of technology by computer hackers, nation-state actors, terrorists, and white collar criminals. The volume of digital evidence that requires forensic examination to support investigations continues to grow at an alarming rate. For example, the amount of data examined by the Digital Forensics program in 1999 was 18 Terabytes (Tb). In 2010, the Digital Forensics program examined 6,628 Tb. The additional personnel will allow the program to address the growth in workload.

Justification

Digital Forensics – 23 positions (all support) and $7,429,000 (all personnel)

The 20 additional CART examiners will address the growing number of requests for digital forensics. These positions will be strategically deployed to FBI Field Offices with the largest percentage of backlogged requests or specialty operations. In addition, three CART examiners are required at the FBIHQ Laboratory to assist in reducing the field’s backlog, as well as enhance the Digital Forensics Training Program’s capacity to deliver CART TECH training to over 100 Special Agents.

As of January 20, 2011 there were 1,443 backlogged cases throughout the CART program. The bulk of the backlogged cases are related to Cyber Crime, Violent Crime, White Collar Crime, and Computer Intrusions. A certified CART examiner can complete approximately 24 examinations annually. The deployment of 20 new CART examiners in the field would produce approximately 480 examinations annually and address a significant portion of the backlog. The addition of three certified CART examiners at FBI HQ will also improve the training of Special Agents as CART TECHs. CART TECHs can review evidence, thus reducing the amount of evidence requiring forensic examination, and who can also improve the turn-around time for examinations by imaging original evidence without the assistance of a CART examiner. These additional CART examiners will enable the FBI to increase intelligence sharing with other members of the Intelligence Community by expanding the amount of data collected from digital forensic analysis and the speed with which that analysis is produced.

Impact on Performance

Please refer to the classified addendum for additional information on this request.

**Funding**

Base Funding

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | FY 2010 Enacted | | | | FY 2011 Continuing Resolution | | | | FY 2012 Current Services | | | |
| Initiative | Pos | Agt | FTE | ($000) | Pos | Agt | FTE | ($000) | Pos | Agt | FTE | ($000) |
| CNCI | 560 | 175 | 430 | $135,828 | 560 | 175 | 430 | $114,138 | 560 | 175 | 430 | $117,646 |
| Digital Forensics | 62 | 5 | 62 | 30,212 | 62 | 5 | 62 | 29,663 | 62 | 5 | 62 | 30,212 |
| Total | 622 | 180 | 492 | $166,040 | 622 | 180 | 492 | $143,801 | 622 | 180 | 492 | $147,858 |

Personnel Increase Cost Summary

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Initiative Name | Type of Position | Modular Cost Per Position ($000) | Number of Positions Requested | FY 2012 Request ($000) | FY 2013 Net Annualization (change from FY 2012)  ($000) |
| *Increase Coverage of Cyber-Terrorist Threats* | |  |  |  |  |
| CNCI | Special Agent, HQ | $283 | 8 | $2,264 | $(744) |
| *Establish NCIJTF 24x7 Operations* | |  |  |  |  |
| CNCI | Special Agent, HQ | 283 | 5 | 1,415 | (465) |
| *Advance Electronic Surveillance Capabilities* | |  |  |  |  |
| CNCI | Special Agent, HQ | 283 | 1 | 283 | (93) |
| CNCI | Engineer | 181 | 1 | 181 | 30 |
| CNCI | Information Technology | 136 | 2 | 272 | 78 |
| CNCI | Professional Support | 116 | 2 | 232 | 20 |
| *Digital Evidence Forensic Support* | |  |  |  |  |
| Digital Forensics | CART Examiner, HQ | 323 | 3 | 969 | (162) |
| Digital Forensics | CART Examiner, Field | 323 | 20 | 6,460 | (1,080) |
|  | Total Personnel |  | 42 | $12,076 | ($5,330) |

Total Request for this Item

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Pos | Agt | FTE | Personnel  ($000) | Non-Personnel  ($000) | Total  ($000) | FY 2013 Net  Annualization  (Change from 2012)  ($000) |
| Current Services | 622 | 180 | 492 | $80,536 | $67,322 | $147,858 | $… |
| Increases | 42 | 14 | 22 | 12,076 | 6,552 | 18,628 | (5,330) |
| Grand Total | 664 | 194 | 514 | $92,612 | $73,874 | $166,486 | ($5,330) |

Threat Name: **National Security**

Budget Decision Unit(s): All

Strategic Goal(s) & Objective(s): 1.1, 1.2, 1.4, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6

FBI SMS Objective: A-01, A-03, A-04, P-03, P-04, P-05, P-06, P-07, P-09,

T-02, T-05, T-06, T-07

Organizational Program: National Security, Critical Incident Response, General Counsel, Information Technology, Intelligence, Records Management, Security, Special Technologies and Applications, Terrorist Screening

Program Increase: Positions ­73 Agt 34 FTE 37 Dollars $48,870,000 ($34,193,000 non-personnel)

Description of Item

The FBI requests 73 positions (34 Agents, 3 Intelligence Analysts (IAs), 36 Professional Staff) and $48,870,000 ($34,193,000 non-personnel) to address national security threats. This comprehensive request will enhance the Data Integration and Visualization System (DIVS), increase vital surveillance resources to combat International Terrorism, enable the implementation of the High-Value Detainee Interrogation Group, augment the operations of the Terrorist Screening Center, address ODNI analytic goals for counterterrorism strategy, and advance the FBI’s information sharing capability.

Justification

*Threat Summary*

The FBI is committed to preventing threats to national security of any kind at any stage, from thwarting those intending to conduct an act of terrorism to investigating the financiers of terrorist operations. As the leader of the Nation’s counterterrorism (CT) efforts, the FBI must understand all dimensions of the threats facing the country and address them with innovative investigative and operational strategies. The FBI must be positioned to proactively overcome the challenges posed by unconventional terrorist methods.

Impact on Performance

Please refer to the classified addendum for additional information on this request.

**Funding**

Total Request for this Item

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Pos | Agt | FTE | Personnel  ($000) | Non-Personnel  ($000) | Total  ($000) | FY 2013 Net  Annualization  (Change from 2012)  ($000) |
| Current Services | 837 | 531 | 837 | $123,016 | $143,886 | $266,902 | $... |
| Increases | 73 | 34 | 37 | 14,677 | 34,193 | 48,870 | (2,999) |
| Grand Total | 910 | 565 | 874 | $137,693 | $178,079 | $315,772 | $(2,999) |

Item Name: **Electronic Surveillance Capabilities**

Budget Decision Unit(s): All

Strategic Goal(s) & Objective(s): 1.1, 1.2, 1.4, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6

FBI SMS Objective: A-01, A-03, A-04, P-03, P-04, P-05, P-07, P-08, P-09, T-02, T-05, T-06, T-07

Organizational Program: Operational Technology, Office of General Counsel

Program Increase: Positions 13 Agt 3 FTE 6 Dollars $12,466,000 ($10,247,000 non-personnel)

Description of Item

The ability of federal, state, and local law enforcement authorities to successfully conduct lawfully-authorized electronic surveillance, in a manner that preserves both a secure, robust, and innovative communications infrastructure and protects privacy and civil liberties, is essential to combating crime and protecting public safety. Electronic surveillance not only provides otherwise unobtainable evidence of criminal activity, but also helps law enforcement authorities to prevent crimes and save lives. However, due to changes in the volume and complexity of today’s communications services and technologies, law enforcement agencies face growing challenges to their ability to access, intercept, collect and process wire or electronic communications to which they are lawfully authorized.

The Department has been working to identify the challenges and propose solutions related to law enforcement’s electronic surveillance capabilities. One way to help address some of these challenges is to establish a Domestic Communications Assistance Center (DCAC). The DCAC would leverage the research and development efforts of federal law enforcement, facilitate the sharing of technology between agencies, strengthen compliance with the Communications Assistance for Law Enforcement Act (CALEA); and seek to build more effective relations with the communications industry.

Within the total Department initiative, $12,466,000 and 13 positions (3 agents) is proposed for the FBI including $10,463,000 to support the Domestic Communications Assistance Center and $2,003,000 to support advanced electronic surveillance.

Justification

**Domestic Communications Assistance Center (DCAC) – 13 positions (3 Agents) and $10,463,000 ($8,244,000 non-personnel)**

The Domestic Communications Assistance Center would strengthen and centralize Law Enforcement Coordination, Technology Sharing, CALEA Implementation, and Industry Relations. The DCAC will serve as a hub for the management of knowledge and technical expertise regarding lawful electronic surveillance, facilitate the sharing of solutions and know-how among federal, state and local law enforcement agencies, and improve relations with industry. The four operational units are:

Law Enforcement Coordination – This unit would identify law enforcement needs related to a specific communications service or provider and direct DCAC resources to address those needs. With input from federal, state, and local law enforcement, the DCAC would be directed toward addressing the more pressing needs for all of law enforcement.

Technology Sharing – This unit would serve as a resource center that can identify technical capabilities for use by federal, state and local law enforcement. In addition, the unit would assist the customer agency by making referrals to agencies with the requisite technical tools or expertise.

CALEA Implementation – This unit would be detailed from the FBI, which is currently responsible for implementing CALEA, to the DCAC. The unit would be expanded to more effectively test and evaluate CALEA-mandated solutions and identify deficiencies in industry-developed technical standards.

Industry Relations – Through this unit, the DCAC would be capable of representing consensus law enforcement positions and would focus and prioritize requests made to industry by law enforcement.

**Advanced Electronic Surveillance – Data Intercept Technology Unit (DITU) – $2,003,000 (all non-personnel)**

Please refer to classified addendum for additional information on this request.

**Funding**

Base Funding

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | FY 2010 Enacted | | | | FY 2011 Continuing Resolution | | | | FY 2012 Current Services | | | |
| Initiative | Pos | Agt | FTE | ($000) | Pos | Agt | FTE | ($000) | Pos | Agt | FTE | ($000) |
| Data Intercept | 45 | 5 | 45 | 42,005 | 45 | 5 | 45 | 41,712 | 45 | 5 | 45 | 41,712 |
| DCAC | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| Total | 45 | 5 | 45 | 42,005 | 45 | 5 | 45 | 41,712 | 45 | 5 | 45 | 41,712 |

Personnel Increase Cost Summary

| Type of Position | Modular Cost  per Position ($000) | Number of  Positions  Requested | FY 2012  Request ($000) | FY 2013  Net Annualization  (change from 2012)  ($000) |
| --- | --- | --- | --- | --- |
| Special Agent | $283 | 3 | $849 | ($279) |
| Attorney | 160 | 3 | 480 | 135 |
| Clerical | 105 | 2 | 210 | (30) |
| Information Technology | $136 | 5 | 680 | 195 |
| Total Personnel |  | 13 | $2,219 | $21 |

Non-Personnel Increase Cost Summary

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Non-Personnel Item | Unit Cost | Quantity | FY 2012 Request ($000) | FY 2013 Net Annualization (Change from 2012)  ($000) |
| Engineering Services – DITU | n/a | n/a | $2,003 | $ … |
| DCAC | n/a | n/a | 8,244 |  |
| Total Non-Personnel |  |  | $10,247 | $ … |

Total Request for this Item

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Pos | Agt | FTE | Personnel  ($000) | Non-Personnel  ($000) | Total  ($000) | FY 2013 Net  Annualization  (Change from 2012)  ($000) |
| Current Services | 45 | 5 | 45 | $6,410 | $35,302 | $41,712 | $... |
| Increases | 13 | 3 | 6 | 2,219 | 10,247 | 12,466 | 21 |
| Grand Total | 58 | 8 | 51 | $8,629 | $45,549 | $54,178 | $21 |

**Item Name: WMD Render Safe Capability**

Budget Decision Unit(s): All

Strategic Goal(s) & Objective(s): 1.1

FBI SMS Objective: A-01, A-02, A-04, T-02, P-03, P-07, P-08

Organizational Program: Critical Incident Response Group, Laboratory

End-State Capability: Domain & Operations

Program Increase: Positions 13 Agt 6 FTE 6 Dollars $40,000,000 ($35,756,000 non-personnel)

Justification

*Threat Summary*

The WMD threat continues to grow and pose significant danger to the U.S. The U.S. Government has taken decisive and urgent actions needed, however these actions have not kept pace with the increasing capabilities and agility of those who would do harm to the U.S. and the world. In an effort to mitigate the WMD threat, the FBI has identified four threat areas that constitute the greatest vulnerabilities: Biological Weapons, Proliferation of WMD Materials, Foreign Interest in Acquiring CBRN Materials, and Reduced Controls over Nuclear Materials. As cited in the Director of National Intelligence March 2009 report,“ the ongoing efforts of nation-states to develop and/or acquire weapons of mass destruction and delivery systems constitute a major threat to the U.S. The U.S. is most concerned about the threat and destabilizing effect of nuclear proliferation-but also about the proliferation of materials and technologies that could contribute to both existing and prospective biological and chemical weapons programs.” U.S. Intelligence Community (IC) agencies assess with confidence that, in the next five years, at least one terrorist group will conduct an attack against U.S. interest overseas-and possibly against the U.S. Homeland-using a biological, chemical, or nuclear weapon that seriously injures or kills hundreds of people.

*Emerging Threat: Biological Weapons*

*Emerging Threat: Foreign Interest in acquiring CBRN Materials*

*Emerging Threat: Reduced Controls over Nuclear Materials*

The ambitious nuclear weapons programs of North Korea and Iran continue to advance with North Korea’s second nuclear test in May and the revelation of a hidden uranium enrichment facility in Iran, presenting increasing immediate and urgent threats to the nonproliferation regime as stated by the 2009 “Clock is Ticking” report. Experts agree that trafficking in nuclear materials and technology is a serious, relentless, and multidimensional problem. This is due in part to the growth in the amount of safeguarded nuclear bomb-making material by a factor of 6 to 10 over the past 20 years and the decline in the number of International Atomic Energy Agency (IAEA) inspections per facility. According to IAEA, there are 439 nuclear power reactors in 30 countries as well as 36 more plants under construction. There are 4,275 identified critical infrastructure and CBRN facilities in total. More than 100 of those, in more than 40 countries, use the highly enriched uranium, which constitutes weapons-grade material. The Commission Report noted that the number of incidents reported to IAEA involving the theft or loss of nuclear or radioactive material is “disturbingly high” and that “much of the material is not recovered, increasing the risk and potential for disaster.”

Graham Allison, author of *Nuclear Terrorism: the Ultimate Preventable Catastrophe* and member of the Commission, provided several examples of the devastation that would result from a nuclear bomb explosion. Below are two examples that illustrate the span of destruction without consideration of the radiological fall-out and resulting devastation.

Washington, DC - A nuclear bomb detonation at the Smithsonian Institution would destroy everything from the White House to the Capitol lawn. The Supreme Court would be rubble and the Pentagon, across the Potomac River, would be engulfed in flames.

Chicago, IL – A nuclear bomb detonation at the Sears Tower would cause everything from Navy Pier to the Eisenhower Expressway to disappear. The United Center and Grant Park would be destroyed and a firestorm would sweep from the White Sox’s U.S. Cellular Field on the South Side to the Cubs’ Wrigley Field on the North Side.

*Justification for Program Increases*

Currently, the FBI Render Safe teams are deployed via a specially-configured leased aircraft whose lease is set to expire in FY 2013. Continuation of the current lease past FY2013 would not be cost-efficient. This request provides funding for a multi-year phased approach to the acquisition and outfitting of two planes to replace the current lease and maintain this valuable capability. The phased acquisition requires multi-year investment commitment to complete the project and provide a viable capability and represents a more cost effective way to meet the mission requirements than the existing lease.

Justification

DOJ is requesting a multi-year phased approach for the acquisition of two planes to replace the current lease and maintain the WMD Render Safe capability. Maintaining the National Security Staff’s mandated Render Safe mission response requires two aircraft with secure and redundant communications systems; a primary aircraft and a backup to cover and support unexpected primary aircraft mechanical failure, and scheduled maintenance down time. The aircraft must be equipped and fitted with secure voice and data equipment required to link the responding assets with the FBI and National leadership and the Department of Energy National Laboratory complex. The connectivity is mandated by the National Security Staff to allow the President and Attorney General to receive updates from the responding assets and issue corresponding directives, reserved only for the President and Attorney General, to the response force.

The FY 2012 request is step one of a three step process:

* Purchase Aircraft. The FY 2012 request of $35.8 million will purchase and refurbish two aircraft within one year.
* Outfit Aircraft. Funding for specialized aircraft outfitting will be necessary in the subsequent year to meet the connectivity between the response force, President and Attorney General, as mandated by the NSC.
* Provide yearly turn-key air operations support. Funding will also be required annually beginning in the third year, to provide around-the-clock crew and maintenance support.

Failure to execute any of the three steps outlined above will prevent the FBI from meeting the directed domestic emergency Render Safe response time.

The positions requested provide six additional Special Agent Bomb Technicians who will conduct Render Safe technical operations, forensics collection and attribution activities, three Physical Security Specialist Hazmat personnel for the National Assets Response Unit to conduct paramedic advanced trauma and life support care and CBRN prophylaxis administration at the incident site, and four support personnel for the Laboratory Division for crime scene processing, including the collection, cataloging and processing, of contaminated and non-contaminated evidence.

Please refer to classified addendum for additional information on this request.

**Funding**

Base Funding

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | FY 2010 Enacted | | | | FY 2011 Continuing Resolution | | | | FY 2012 Current Services | | | |
| Initiative | Pos | Agt | FTE | ($000) | Pos | Agt | FTE | ($000) | Pos | Agt | FTE | ($000) |
| Render Safe Capability | 106 | 28 | 99 | $48,783 | 106 | 28 | 106 | $48,783 | 106 | 28 | 106 | $48,783 |
| Total | 106 | 28 | 99 | $48,783 | 106 | 28 | 106 | $48,783 | 106 | 28 | 106 | $48,783 |

Personnel Increase Cost Summary

| Item | Type of Position | Modular Cost  per Position ($000) | Number of  Positions  Requested | FY 2011  Request ($000) | FY 2012  Net Annualization  (change from 2011)  ($000) |
| --- | --- | --- | --- | --- | --- |
| Hazardous Devices Response Unit | HQ Agent | $327 | 4 | $1,308 | ($24) |
| Explosives Unit | HQ Agent | 327 | 2 | 654 | (12) |
| National Assets Response Unit | Non-Agent Responder | 326 | 3 | 978 | (237) |
| Hazardous Materials Response Unit | Non-Agent Responder | $326 | 4 | 1,304 | (316) |
|  | Total Personnel |  | 13 | $4,244 | ($589) |

Non-Personnel Increase Cost Summary

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Non-Personnel Item | Unit Cost | Quantity | FY 2011 Request  ($000) | FY 2012 Net  Annualization  (Change from 2011)  ($000) |
| Aircraft | n/a | 2 | $35,756 | $... |
| Total Non-Personnel |  |  | $35,756 | $... |

Total Request for this Item

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Pos | Agt | FTE | Personnel  ($000) | Non-Personnel  ($000) | Total  ($000) | FY 2012 Net  Annualization  (Change from 2011)  ($000) |
| Current Services | 106 | 28 | 106 | $14,202 | $34,581 | $48,783 | $… |
| Increases | 13 | 6 | 6 | 4,244 | 35,756 | 40,000 | (589) |
| Grand Total | 119 | 34 | 112 | $18,446 | $70,337 | $88,783 | ($589) |

**Threat Name: Operational Enablers**

Budget Decision Unit(s): Intelligence

Strategic Goal(s) & Objective(s): 1.1, 1.4, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6

FBI SMS Objective: P-08, T-02, T-05

Organizational Program: Intelligence, Training

Program Increase: Positions 0 Agt 0 FTE 0 Dollars $2,486,000 (all non-personnel)

Description of Item

The FBI requests $2,486,000 (all non-personnel) to provide increased analytical career path training.

Justification

*Threat Summary*

The FBI continues to face technical, physical, and personnel constraints that cause gaps in intelligence collection, analysis, and information sharing abilities. The growth in the FBI’s programs and resources in recent years has not been accompanied by a commensurate increase in critical information sharing capabilities, analytic training, and essential personnel. These are key elements of a foundation necessary for enabling the FBI ability to effectively address law enforcement and national security threats.

Effective enterprise-wide infrastructure is critical to ensuring the FBI possesses the capabilities to carry out its national security and criminal investigative missions. Without the following enhancement, the FBI runs the risk of losing critical support for overall functionality and program effectiveness.

*Justification of Program Increases*

**Analytic Career Path Training – $2,486,000 (all non-personnel)**

The FBI requests $2,486,000 (all non-personnel) to support the FBI’s Analytic Career Path Training for intelligence personnel. Resources will fund analytic training courses consistent with the FBI’s five-year intelligence training strategy.

As part of the five-year intelligence training strategy, the FBI plans to develop training courses where SAs and IAs will learn in the same classroom. During the development and implementation of the FBI’s Strategic Execution Team (SET) initiative, a high priority was placed on the training of intelligence personnel. The following courses are essential to preparing the FBI’s workforce to determine what we do not yet know, what threats we have not yet anticipated, and what vulnerabilities we have not yet recognized.

*Intelligence Analyst Training: 3 New Work-Role courses – $1,978,000*

The FBI requests resources to fund six iterations of the new work-role courses for IAs. Derived from the FBI’s evolution of a generalist to a subject-matter-expert workforce, the FBI is developing a three-tiered career path model for IAs to respond to the increased complexity and global scope of threats. This model reflects different skill sets within the tactical analysis, collection/reporting and strategic analysis disciplines. The FBI will develop specialized training in each discipline, which will be delivered as part of an enhanced Intelligence Basic Course. As the IA Career paths develop, new and expanded job tasks will need to be researched, developed, analyzed and integrated into training that IAs need at different levels of development. The FBI is planning to use this money to conduct evaluations of current training, develop the job task analysis tied to the three career paths and work roles, and develop new curriculum and implement the new classes to provide Bureau IAs with the training they need to counter known and asymmetrical threats to the Homeland. This curriculum effort will be tied into the Intelligence Basic Course and provide material support for future class development as part of the Five Year Plan.

*Intermediate Analytic Tradecraft (IAT) Course – $508,000*

There is a major training gap for the intermediate analytic population, which comprises the largest portion of the total analytic population. The requested resources will fund three iterations of the 15-day IAT course, with 24 students per iteration. This course was developed in conjunction with the FBI Directorate of Intelligence (DI) staff to support the Intelligence Analysts Career Path as listed in the Bureau’s Intelligence Workforce Strategy. This course will be mandatory training and required for promotion. For growth at the intermediate level, this course fulfills training and experiential learning requirements. The curricula will help participants hone their skills specific to the FBI, common throughout the IC, and needed for future promotion. Instruction topics include: critical thinking, ethics in analysis, and the legal principles and practices related to intelligence analysis.

Impact on Performance

Without the requested funding, the FBI will be unable to fully meet mission requirements and Office of the Director of National Intelligence imposed analytic tradecraft standards may not be achieved. Additionally, the FBI will be unable to properly train its workforce to produce high-quality analysis and actionable intelligence.

**Funding**

Base Funding

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | FY 2010 Enacted | | | | FY 2011 Continuing Resolution | | | | FY 2012 Current Services | | | |
| Initiative | Pos | Agt | FTE | ($000) | Pos | Agt | FTE | ($000) | Pos | Agt | FTE | ($000) |
| Analytic Career Path Training | 63 | 22 | 57 | $54,102 | 68 | 22 | 64 | $40,869 | 75 | 22 | 72 | $44,102 |
| Total | 63 | 22 | 57 | $54,102 | 68 | 22 | 64 | $40,869 | 75 | 22 | 72 | $44,102 |

Non-Personnel Increase Cost Summary

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Non-Personnel Item | Unit Cost | Quantity | FY 2012 Request  ($000) | FY 2013 Net  Annualization  (Change from 2012)  ($000) |
| Analytic Career Path Training | n/a | n/a | $2,486 | $… |
| Total Non-Personnel |  |  | $2,486 | $… |

Total Request for this Item

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Pos | Agt | FTE | Personnel  ($000) | Non-Personnel  ($000) | Total  ($000) | FY 2013 Net  Annualization  (Change from 2012)  ($000) |
| Current Services | 75 | 22 | 72 | $11,690 | $32,412 | $44,102 | $… |
| Increases | … | … | … | … | 2,486 | 2,486 | … |
| Grand Total | 75 | 22 | 72 | $11,690 | $34,898 | $46,588 | $... |

**Item Name: Violent Crime in Indian Country**

Budget Decision Unit(s): All

Strategic Goal(s) & Objective(s): 2.2, 2.6

FBI SMS Objective(s): A1, A2, A4, P4, P5, P6, P7, P8

Organizational Program: Criminal

Program Increase: Positions 40 Agt 24 FTE 20 Dollars $9,000,000 ($449,000 non-personnel)

Description of Item

The FBI requests 40 positions (24 Agents, 16 Support) and $9,000,000 ($449,000 non- personnel) to bolster existing Safe Trails Task Forces and to provide additional investigative resources to address a significant violent crime threat in Indian Country. These resources will support the Attorney General’s Department-wide initiative on public safety in tribal communities.

Justification

*Threat Summary*

The U.S. Government recognizes more than 560 American Indian tribes and Native Alaskan groups comprised of more than 4.3 million members. A little more than half of all members live on land owned by these tribes or groups, which includes more than 50 million acres of land spread across more than 30 continental states. Although there are some densely populated areas on reservations, many Native Americans live in geographically isolated areas.

There is significant variation among tribal group nations and Alaska native groups in terms of social, economic and cultural characteristics. According to 2000 Census data and later reporting, many groups experience social and economic problems. Native American and Alaska Native communities are sometimes characterized by high rates of alcoholism and substance abuse, high suicide rates and high crime rates.[[5]](#footnote-5)

Violent crime in Indian Country is at unacceptable levels and has a devastating impact on the basic quality of life there. Many tribes experience rates of violent crime far higher than most other Americans; indeed, some face murder rates against Native American women more than ten times the national average. Tribal law enforcement resources are typically scarce, a problem exacerbated by geographic isolation and/or vast size of many reservations. Federal and state resources devoted to Indian Country have also typically been insufficient to address law enforcement needs.

According to a Bureau of Justice Statistics (BJS) profile from 1992-2002, 25 percent of all violent crimes prosecuted by U.S. Attorneys occur on Indian Reservations. As of January, 2010, the FBI has over 2,500 pending Indian Country cases, of which 75 percent are comprised of death investigation, sexual/physical abuse of children, rape, and aggravated assault cases. Domestic violence cases in Indian Country are virtually unaddressed unless they involve the above crimes.

According to the Executive Office for United States Attorneys (EOUSA), in FY 2009 over 2,500 federal domestic violence cases in Indian Country were prosecuted and an overwhelming number were in violation of The Gun Control Act. Following the Violence Against Women Act of 2005, a new statute (18 USC 117, Domestic Assault by a Habitual Offender) took effect to address domestic violence. Subjects may be charged under this statute if the subject has two prior domestic violence convictions.

Other domestic violence statues include:

* Interstate Domestic Violence (18 USC 2261)
* Stalking (18 USC 2261A)
* Interstate Violation of a Protection Order (18 USC 2262)

According to the BJS study, the rate of victimization among Native American women (age 12 or older) was more than double that of all women. Also, statistics indicate that more than one-third of all Native American women will be raped at least once during their lifetime and nearly two-thirds will be victims of violent assaults.

According to a Bureau of Indian Affairs (BIA) gap analysis conducted in 2006, Indian Country is served by just half as many police officers as similarly situated rural areas. Police emergency response in Indian Country can be up to one and a half hours, compared to a national average of six minutes.

In addition to the violence, fraud and other such crimes committed on Indian reservations associated with the Indian Gaming industry represent an emerging threat for the FBI which is currently largely unaddressed. There are over 400 Indian gaming facilities spread throughout 28 states. The National Indian Gaming Commission (NIGC) has stated that Indian Gaming grossed $26.7 billion in revenues during 2008 and is regulated by approximately 25 NIGC investigators. These NIGC investigators perform a regulatory function as opposed to conducting criminal investigations for prosecution. Currently, the NIGC estimates that over 90 percent of all gaming theft and embezzlement violations are committed by employees associated with the gaming industry. Crime trends in Indian Gaming indicate traditional organized crime elements are targeting the Indian Gaming industry. Funds generated by gaming related theft and embezzlement can fuel more violent crime and could lead to expanding criminal networks.

*Justification for Program Increases*

**Indian Country Investigations – 40 positions and $9,000,000 ($449,000 non-personnel)**

The FBI has primary Federal jurisdiction over more than 200 reservations, with approximately 106 agents available to investigate crimes that occur in Indian Country. This is less than one percent of the FBI’s total agent workforce. The agents often operate out of remote FBI Resident Agencies (RAs).

Although the FBI has established 19 Safe Trails Task Forces (STTFs) in an effort to proactively address the growing violent crime problem on reservations, domestic violence cases are virtually unaddressed as no other law enforcement entity besides the FBI can investigate these crimes.

Additional personnel resources in Indian Country will:

* investigate sexual assault and domestic violence;
* address violence against women and children; and
* allow for a proactive FBI response to public corruption and Indian gaming issues.

Impact on Performance

Without the requested resources, domestic violence cases in Indian Country will continue to be under-addressed. Furthermore, if FBI resources are not enhanced in Indian Country, the full scope of the violent crime problem will be unknown and only limited resources will be available to address the threat.

Enhancements in Indian Country will allow a proactive FBI response focused on criminal enterprise investigations in drugs, gangs, public corruption, and Indian gaming issues in active Indian Country territories. Further, the additional positions in Indian Country will provide specific STTF SA designees who focus on the mission of the taskforce.

**Funding**

Base Funding

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | FY 2010 Enacted | | | | FY 2011 Continuing Resolution | | | | FY 2012 Current Services | | | |
| Initiative | Pos. | Agt. | FTE | ($000) | Pos. | Agt. | FTE | ($000) | Pos. | Agt. | FTE | ($000) |
| Indian Country | 121 | 111 | 117 | $22,258 | 121 | 111 | 121 | $22,801 | 121 | 111 | 121 | $22,801 |
| Total | 121 | 111 | 117 | $22,258 | 121 | 111 | 121 | $22,801 | 121 | 111 | 121 | $22,801 |

Personnel Increase Cost Summary

| Type of Position | Modular Cost Per Position ($000) | Number of Positions Requested | FY 2012 Request ($000) | FY 2013 Net Annualization (change from 2012)  ($000) |
| --- | --- | --- | --- | --- |
| Special Agent | $283 | 24 | $6,792 | $(2,232) |
| Clerical | 105 | 9 | 945 | (135) |
| Investigative Support | 113 | 6 | 678 | (24) |
| Information Technology | 136 | 1 | 136 | 39 |
| Total Personnel |  | 40 | $8,551 | $(2,352) |

Non-personnel Increase Cost Summary

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Non-Personnel Item | Unit Cost | Quantity | FY 2012 Request  ($000) | FY 2013 Net  Annualization  (Change from 2012)  ($000) |
|  | n/a | n/a | $449 | $... |
| Total Non-Personnel |  |  | $449 | $... |

Total Request for this Item

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Pos | Agt | FTE | Personnel ($000) | Non-Personnel ($000) | Total | FY 2013 Net Annualization  (Change from 2012) ($000) |
| Current Services | 121 | 111 | 121 | $20,042 | $2,759 | $22,801 | $… |
| Increases | 40 | 24 | 20 | 8,551 | 449 | 9,000 | (2,352) |
| Grand Total | 161 | 135 | 141 | $28,593 | $3,208 | $31,801 | $(2,352) |

**Item Name: Administrative Efficiencies**

Budget Decision Unit(s): All

Strategic Goal(s) & Objective(s): 1.1, 1.2, 1.4, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6

FMS SMS Objective: T-05, R-02

Organizational Program: Administrative

Program Reduction to Direct S&E Appropriation: ($5,910,000) (all non-personnel)

Description of Item

Recognizing the constrained resource environment, the FBI has proposed several reductions. This proposal would reduce funding for administrative areas such as travel, conferences, supplies, and equipment by $5,910,000.

Impact on Performance

This offset reflects anticipated savings that will be achieved by reducing spending in administrative areas and the FBI will work to minimize the impact from additional reductions.

**Funding**

Base Funding

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| FY 2010 Enacted | | | | FY 2011 Continuing Resolution | | | | FY 2012 Current Services | | | |
| Pos | Agt | FTE | ($000) | Pos | Agt | FTE | ($000) | Pos | Agt | FTE | ($000) |
| … | … | … | 975,720 | … | … | … | 800,425 | … | … | … | 871,812 |

Non-Personnel Decrease Cost Summary

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Non-Personnel Item | Unit Cost | Quantity | FY 2012 Request  ($000) | FY 2013 Net  Annualization  (Change from 2012)  ($000) |
| Administrative Services | n/a | n/a | ($5,910) | $… |
| Total Non-Personnel |  |  | ($5,910) | $… |

Total Request for this Item

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Pos | Agt | FTE | Personnel  ($000) | Non-Personnel  ($000) | Total  ($000) | FY 2013 Net  Annualization  (Change from 2012)  ($000) |
| Current Services | … | … | … | $… | $871,812 | $871,812 | $… |
| Decreases | … | … | … | … | (5,910) | (5,910) | … |
| Grand Total | … | … | … | $… | $865,902 | $865,902 | $... |

**Item Name: Extend Tech Refresh**

Budget Decision Unit(s): All

Strategic Goal(s) & Objective(s): 1.1, 1.4, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6

FMS SMS Objective: T-05, T-07

Organizational Program: Information Technology

Program Reduction to Direct S&E Appropriation: ($5,651,000) (all non-personnel)

Description of Item

Recognizing the constrained resource environment, the FBI has proposed several reductions. This proposal would extend the FBI’s refresh cycle of its desktops and laptops from four to five years, in some cases more.

Impact on Performance

Staying current with IT infrastructure is an important operational enabler. However, as desktops and laptops are used primarily for basic office automation applications (e.g. spreadsheets and word processing), replacing this inventory at a slower rate will put an additional, minimal burden on the workforce.

**Funding**

Base Funding

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| FY 2010 Enacted | | | | FY 2011 Continuing Resolution | | | | FY 2012 Current Services | | | |
| Pos | Agt | FTE | ($000) | Pos | Agt | FTE | ($000) | Pos | Agt | FTE | ($000) |
| … | … | … | $35,530 | … | … | … | $35,530 | … | … | … | $35,530 |

Non-Personnel Decrease Cost Summary

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Non-Personnel Item | Unit Cost | Quantity | FY 2012 Request  ($000) | FY 2013 Net  Annualization  (Change from 2012)  ($000) |
| Technical Refresh | n/a | n/a | ($5,651) | $… |
| Total Non-Personnel |  |  | ($5,651) | $… |

Total Request for this Item

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Pos | Agt | FTE | Personnel  ($000) | Non-Personnel  ($000) | Total  ($000) | FY 2013 Net  Annualization  (Change from 2012)  ($000) |
| Current Services | … | … | … | $… | $35,530 | $35,530 | $… |
| Decreases | … | … | … | … | (5,651) | (5,651) | … |
| Grand Total | … | … | … | $… | $29,879 | $29,879 | $... |

**Item Name: Headquarters/Field Cost Module Reduction**

Budget Decision Unit(s): All

Strategic Goal(s) & Objective(s): 1.1, 1.4, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6

FMS SMS Objective: P-01

Organizational Program: Resource Planning

Program Reduction: Positions 0 Agt 0 FTE 0 Dollars ($762,000) (all personnel)

Description of Item

Recognizing the constrained resource environment, the FBI has proposed several program reductions. This proposal would reduce FBI field and headquarters (HQ) Intelligence Analyst (IA) and Special Agent (SA) prior year cost modules by $762,000.

Summary Justification

Position cost modules are developed to capture the full cost incurred to hire and support a new position on board. Costs include pay, benefits, computers, furniture, and vehicles, among other items to support each position’s full performance level. The FBI proposes to streamline the SA and IA cost modules by eliminating the HQ cost module. While HQ positions are paid at a higher level than field positions, the field cost module fully supports the journeyman level, which represents the average of all FBI positions. The FBI proposes to eliminate the HQ cost module and reduce its base by the difference between the HQ and field cost modules.

**Funding**

Base Funding

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| FY 2010 Enacted | | | | FY 2011 Continuing Resolution | | | | FY 2012 Current Services | | | |
| Pos | Agt | FTE | ($000) | Pos | Agt | FTE | ($000) | Pos | Agt | FTE | ($000) |
| 32,998 | 12,781 | 31,578 | $4,177,919 | 32,998 | 12,781 | 32,398 | $4,441,459 | 33,469 | 12,993 | 32,777 | $4,588,173 |

Personnel Decrease Cost Summary

| Type of Position | Modular Cost Per Position ($000) | Number of Positions Requested | FY 2012 Request ($000) | FY 2013 Net Annualization (change from 2012)  ($000) |
| --- | --- | --- | --- | --- |
| n/a | n/a | n/a | ($762) | $ … |
| Total Personnel |  |  | ($762) | $ … |

Total Request for this Item

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Pos | Agt | FTE | Personnel ($000) | Non-Personnel ($000) | Total | FY 2013 Net Annualization  (Change from 2012) ($000) |
| Current Services | 33,469 | 12,993 | 32,777 | $4,588,173 | $… | $4,588,173 | $… |
| Decreases | … | … | … | (762) | … | (762) | … |
| Grand Total | 33,469 | 12,993 | 32,777 | $4,587,411 | $... | $4,587,411 | $… |

**Item Name: Lookout Program Efficiencies**

Budget Decision Unit(s): Counterterrorism/Counterintelligence

Strategic Goals & Objectives(s): 1.4

FMS SMS Objective: P3, P4, P5, P7

Organizational Program: Counterintelligence

Program Reduction to Direct S&E Appropriation: Positions … Agt … FTE …

Dollars ($2,600,000) (All non-personnel) (see companion Lookout Program enhancement)

Description of Item

Please refer to the classified addendum for additional information on this request.

**Funding**

Base Funding

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| FY 2010 Enacted | | | | FY 2011 Continuing Resolution | | | | FY 2012 Current Services | | | |
| Pos | Agt | FTE | ($000) | Pos | Agt | FTE | ($000) | Pos | Agt | FTE | ($000) |
| 188 | … | 188 | $26,340 | 188 | … | 188 | $26,340 | 188 | … | 188 | $27,655 |

Non-Personnel Decrease Cost Summary

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Non-Personnel Item | Unit Cost | Quantity | FY 2012 Request  ($000) | FY 2013 Net  Annualization  (Change from 2012)  ($000) |
| Lookout Program | n/a | n/a | ($2,600) | $… |
| Total Non-Personnel |  |  | ($2,600) | $… |

Total Request for this Item

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Pos | Agt | FTE | Personnel  ($000) | Non-Personnel  ($000) | Total  ($000) | FY 2013 Net  Annualization  (Change from 2012)  ($000) |
| Current Services | 188 | … | 188 | $17,734 | $9,931 | $27,665 | $… |
| Decreases | … | … | … | … | (2,600) | (2,600) | … |
| Grand Total | 188 | … | 188 | $17,734 | $7,331 | $25,065 | $... |

**Item Name:** **Network and Intrusion Analysis**

Budget Decision Unit(s): All

Strategic Goals & Objectives(s): 1.1, 1.4, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6

FMS SMS Objective: P-01, P-06, T-06

Organizational Program: Operational Technology

Program Reduction to Direct S&E Appropriation: Positions (6) Agt (1) FTE (6)

Dollars ($5,766,000) ($5,162,000 non-personnel)

Description of Item

Recognizing the constrained resource environment, the FBI proposes to reduce program funding by 50 percent for the development of new tools to identify and analyze network intrusions.

Impact on Performance

Intrusion Analysis currently supports the Bureau’s Comprehensive National Cybersecurity Initiative (CNCI) and employs personnel with the skills to understand and analyze the different ways terrorists and criminals exploit technology to their benefit as a means to committing crimes and eventual harm to society.

FBI will attempt to leverage other government agencies’ development activities to minimize the impact this reduction will have on the FBI’s ability to conduct complex digital analysis through the application of advanced innovative techniques and technologies in support FBI investigations and intelligence operations.

**Funding**

Base Funding

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| FY 2010 Enacted | | | | FY 2011 Continuing Resolution | | | | FY 2012 Current Services | | | |
| Pos | Agt | FTE | ($000) | Pos | Agt | FTE | ($000) | Pos | Agt | FTE | ($000) |
| 13 | 3 | 13 | $11,532 | 13 | 3 | 13 | $11,274 | 13 | 3 | 13 | $11,532 |

Personnel Decrease Cost Summary

| Type of Position | Modular Cost  per Position ($000) | Number of  Positions  Requested | FY 2012  Request ($000) | FY 2013  Net Annualization  (change from 2012)  ($000) |
| --- | --- | --- | --- | --- |
| Special Agent | $169 | (1) | ($169) | $… |
| Clerical | $87 | (5) | (435) | … |
| Total Personnel |  | (6) | ($604) | $… |

Non-Personnel Decrease Cost Summary

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Non-Personnel Item | Unit Cost | Quantity | FY 2012 Request ($000) | FY 2013 Net Annualization (Change from 2012)  ($000) |
| Intrusion Analysis Unit | n/a | n/a | ($5,162) | $ … |
| Total Non-Personnel |  |  | ($5,162) | $... |

Total Request for this Item

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Pos | Agt | FTE | Personnel  ($000) | Non-Personnel  ($000) | Total  ($000) | FY 2013 Net  Annualization  (Change from 2012)  ($000) |
| Current Services | 13 | 3 | 13 | $1,377 | $10,155 | $11,532 | $... |
| Decreases | (6) | (1) | (6) | (604) | (5,162) | (5,766) | … |
| Grand Total | 7 | 2 | 7 | $773 | $4,993 | $5,766 | $... |

**Item Name: Reduce Physical Footprint**

Budget Decision Unit(s): All

Strategic Goals & Objectives(s): 1.1, 1.4, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6

FMS SMS Objective: P-01, R-01, R-02

Organizational Program: All

Program Reduction to Direct S&E Appropriation: Positions … Agt … FTE …

Dollars ($674,000) (all non-personnel)

Description of Item:

The FBI proposes to consolidate and reduce 12 of its 385 resident agencies (RAs). This reduction reflects GSA rent savings; staff at consolidated facilities would be relocated to nearby locations. The FBI recently completed a comprehensive analysis of the strategic placement of its facilities using both quantitative and qualitative methods. As part of the quantitative analysis, each RA was evaluated on the basis of five criteria:

1. Facility Density (the number of FOs and/or RAs within a 25- and 50-mile radius);
2. Facility Utilization (the number of seats being utilized relative to total the number of seats available);
3. Personnel (the number of FBI employees, Task Force Officers (TFOs) & other personnel);
4. Professional Staff-to-Special Agent Ratio (the number of Professional Staff members relative to the number of Special Agents); and
5. Distance to the Nearest U.S. Attorney’s Office within the applicable Judicial District.

RAs that met the threshold detailed above were subjected to a qualitative analysis by each Field Division’s Assistant Director in Charge (ADIC) or Special Agent in Charge (SAC), whereby each RA was evaluated on the basis of seven criteria:

1. Partnerships (local, state, tribal, federal, etc.);
2. Primary Responsibilities and Exclusive Jurisdictions (counterterrorism, counterintelligence, public corruption, Indian Country);
3. Current and Emerging Risks;
4. Personnel Considerations (first-office assignments, retirement eligibility, participation in the Special Agent Relief Program);
5. Facility Considerations (lease terms, associated facilities, sensitive compartmented information facilities);
6. Financial Considerations (operating costs, relocation bonuses, hard to staff policies); and,
7. Geographic Considerations.

Upon completion of this analysis, the following offices were proposed for closure:

1. Dublin, Georgia
2. Effingham, Illinois
3. Elizabeth City, North Carolina
4. Enid, Oklahoma
5. Frankfort, Kentucky
6. Lorain, Ohio
7. Niagara Falls, New York
8. St. Peters, Missouri
9. Staten Island, New York
10. Vinita, Oklahoma
11. Wenatchee, Washington
12. Wesley Chapel, Florida

Impact on Performance

While recent high-profile counterterrorism, counterintelligence, and criminal cases demonstrate that RAs are vital operational platforms, the FBI will ensure that its resources are strategically allocated. This realignment will allow the FBI to increase its mission effectiveness by focusing resources on higher priority matters as well as increase operation efficiency by leveraging cost savings and creating more manageable spans of control.

**Funding**

Base Funding

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| FY 2010 Enacted | | | | FY 2011 Continuing Resolution | | | | FY 2012 Current Services | | | |
| Pos | Agt | FTE | ($000) | Pos | Agt | FTE | ($000) | Pos | Agt | FTE | ($000) |
| … | … | … | $564,930 | … | … | … | $564,930 | … | … | … | $564,930 |

Non-Personnel Decrease Cost Summary

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Non-Personnel Item | Unit Cost | Quantity | FY 2012 Request ($000) | FY 2013 Net Annualization (Change from 2012)  ($000) |
| Rent | n/a | n/a | ($674) | $ … |
| Total Non-Personnel |  |  | ($674) | $... |

Total Request for this Item

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Pos | Agt | FTE | Personnel  ($000) | Non-Personnel  ($000) | Total  ($000) | FY 2013 Net  Annualization  (Change from 2012)  ($000) |
| Current Services | … | … | … | $… | $564,930 | $564,930 | $... |
| Decreases | … | … | … | … | (674) | (674) | … |
| Grand Total | … | … | … | $… | $564,256 | $564,256 | $... |

**Item Name: Relocation Program**

Budget Decision Unit(s): All

Strategic Goal(s) & Objective(s): 1.1, 1.2, 1.4, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6

FMS SMS Objective: T-05, R-02

Organizational Program: Human Resources

Program Reduction to Direct S&E Appropriation: ($6,250,000) (all non-personnel)

Description of Item

Recognizing the constrained resource environment, the FBI proposes to reduce funding supporting its Relocation Program. The Employee Relocation Program strategically relocates staff to meet the organizational needs of the FBI by ensuring FBI field offices and programs are optimally staffed to carry out the FBI’s mission requirements.

Impact on Performance

The FBI will attempt to minimize the impact by prioritizing agent relocations for mission critical programs.

**Funding**

Base Funding

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| FY 2010 Enacted | | | | FY 2011 Continuing Resolution | | | | FY 2012 Current Services | | | |
| Pos | Agt | FTE | ($000) | Pos | Agt | FTE | ($000) | Pos | Agt | FTE | ($000) |
| 18 | 2 | 18 | $122,326 | 18 | 2 | 18 | $121,915 | 18 | 2 | 18 | $147,804 |

Non-Personnel Decrease Cost Summary

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Non-Personnel Item | Unit Cost | Quantity | FY 2012 Request  ($000) | FY 2013 Net  Annualization  (Change from 2012)  ($000) |
| Relocation Program | n/a | n/a | ($6,250) | $… |
| Total Non-Personnel |  |  | ($6,250) | $… |

Total Request for this Item

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Pos | Agt | FTE | Personnel  ($000) | Non-Personnel  ($000) | Total  ($000) | FY 2013 Net  Annualization  (Change from 2012)  ($000) |
| Current Services | 18 | 2 | 18 | $61,785 | $86,019 | $147,804 | $… |
| Decreases | … | … | … | … | ($6,250) | ($6,250) | … |
| Grand Total | 18 | 2 | 18 | $61,785 | $79,769 | $141,554 | $... |

**Item Name: Sentinel**

Budget Decision Unit(s): All

Strategic Goal(s) & Objective(s): 1.1, 1.4, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6

FMS SMS Objective: T-05, T-07

Organizational Program: Information Technology

Program Reduction to Direct S&E Appropriation: ($15,000,000) (all non-personnel)

Description of Item

The proposed offset will reduce the Sentinel budget to cover only Operations and Maintenance of the completed system.

Impact on Performance

This reduction will not impact the FBI’s ability to support the existing Sentinel system as the FBI plans to complete work in the fall of FY 2011.

**Funding**

Base Funding

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| FY 2010 Enacted | | | | FY 2011 Continuing Resolution | | | | FY 2012 Current Services | | | |
| Pos | Agt | FTE | ($000) | Pos | Agt | FTE | ($000) | Pos | Agt | FTE | ($000) |
| … | … | … | $54,991 | … | … | … | $45,447 | … | … | … | $45,447 |

Non-Personnel Decrease Cost Summary

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Non-Personnel Item | Unit Cost | Quantity | FY 2012 Request  ($000) | FY 2013 Net  Annualization  (Change from 2012)  ($000) |
| Sentinel | n/a | n/a | ($15,000) | $… |
| Total Non-Personnel |  |  | ($15,000) | $… |

Total Request for this Item

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Pos | Agt | FTE | Personnel  ($000) | Non-Personnel  ($000) | Total  ($000) | FY 2013 Net  Annualization  (Change from 2012)  ($000) |
| Current Services | … | … | … | $… | $45,447 | $45,447 | $… |
| Decreases | … | … | … | … | (15,000) | (15,000) | … |
| Grand Total | … | … | … | $… | $30,447 | $30,447 | $... |

**Item Name: Task Force Consolidation**

Budget Decision Unit(s): Criminal Enterprises and Federal Crimes

Strategic Goal(s) & Objective(s): 1.1, 2.2, 2.3, 2.5, 2.6

FMS SMS Objective: R-01

Organizational Program: Criminal Investigative

Program Reduction to Direct S&E Appropriation: Dollars ($898,000) (all non-personnel)

Description of Item

Recognizing the constrained resource environment, the FBI proposes to reduce its criminal task force footprint through consolidating up to 48 task forces within the same geographic area.  The $898,000 savings reflects overhead and infrastructure support costs; task force positions will be realigned to other priority areas.

Impact on Performance

Task forces are one of the cornerstones of the FBI’s and DOJ’s anti-crime strategy by integrating federal, state, and local counterparts. Task forces serve as force multipliers in efforts to combat violent crime and promote national security by providing expertise and experience to local communities. The FBI is dedicated to identifying cost efficiencies within its base budget and is determined to find unique methods to ensure implementation. Positions will be reassigned to other task forces and high priority areas, which will allow the FBI to maintain current levels of investigative capacity and operational effectiveness.

**Funding**

Base Funding

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| FY 2010 Enacted | | | | FY 2011 Continuing Resolution | | | | FY 2012 Current Services | | | |
| Pos | Agt | FTE | ($000) | Pos | Agt | FTE | ($000) | Pos | Agt | FTE | ($000) |
| 11 | 7 | 11 | $1,671 | 11 | 7 | 11 | $8,408 | 11 | 7 | 11 | $8,408 |

Non-Personnel Decrease Cost Summary

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Non-Personnel Item | Unit Cost | Quantity | FY 2012 Request  ($000) | FY 2013 Net  Annualization  (Change from 2012)  ($000) |
| Task Forces | n/a | n/a | ($898) | $... |
| Total Non-Personnel |  |  | ($898) | $... |

Total Request for this Item

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Pos | Agt | FTE | Personnel ($000) | Non-Personnel ($000) | Total | FY 2013 Net Annualization  (Change from 2012) ($000) |
| Current Services | 11 | 7 | 11 | $1,671 | $6,737 | $8,408 | $… |
| Decreases | … | … | … | … | (898) | (898) | … |
| Grand Total | 11 | 7 | 11 | $1,671 | $5,839 | $7,510 | $ … |

**Item Name:** **Secure Work Environment (SWE)**

Budget Decision Unit(s): All

Strategic Goals & Objectives(s): 1.4

FMS SMS Objective: T-07

Organizational Program: Facilities & Logistics, National Security

Program Reduction to Direct CNST Appropriation: Positions … Agt … FTE …

Dollars ($26,328,000) (All non-personnel)

Description of Item:

The Secure Work Environment (SWE) Program provides Field Offices, Resident Agencies, Legal Assistance Offices, and Off-sites with the physical and information technology infrastructure required by FBI personnel to share information at all levels of classification with our Intelligence Community partners and local law enforcement officials. This offset would reduce the program’s recurring funding by 25 percent, leaving $78,982,000 in FBI’s base to maintain and operate the current SWE infrastructure while working towards the goal of providing a secure work environment for all FBI National Security Professionals by 2014.

Impact on Performance

By the end of FY 2011, the FBI will have approximately 11,500 Top Secret (TS) workstations, with a goal of installing 15,000 TS workstations by FY 2014. At full base funding of $105.3 million, the FBI is currently able to install an additional 1,500 TS workstations each year and would be able to meet its goal within the original timeframe. However, a 25 percent reduction would fund the installation of only 750 TS workstations each year, resulting in only 13,750 TS workstations by FY 2014. The FBI will attempt to limit the impact of this reduction by prioritizing remaining locations previously slated for SWE improvements.

**Funding**

Base Funding

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | FY 2010 Enacted | | | | FY 2011 Continuing Resolution | | | | FY 2012 Current Services | | | |
| Initiative | Pos | Agt | FTE | ($000) | Pos | Agt | FTE | ($000) | Pos | Agt | FTE | ($000) |
| Secure Work Environment | … | … | … | $105,310 | … | … | … | $105,310 | … | … | … | $105,310 |
| Total | … | … | … | $105,310 | … | … | … | $105,310 | … | … | … | $105,310 |

Non-Personnel Decrease Cost Summary

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Non-Personnel Item | Unit Cost | Quantity | FY 2012 Request ($000) | FY 2013 Net Annualization (Change from 2012)  ($000) |
| Secure Work Environment | n/a | n/a | ($26,328) | $ … |
| Total Non-Personnel |  |  | ($26,328) | $ … |

Total Request for this Item

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Pos | Agt | FTE | Personnel  ($000) | Non-Personnel  ($000) | Total  ($000) | FY 2013 Net  Annualization  (Change from 2012)  ($000) |
| Current Services | … | … | … | $... | $105,310 | $105,310 | $... |
| Decreases | … | … | … | … | (26,328) | (26,328) | … |
| Grand Total | … | … | … | $... | $78,982 | $78,982 | $... |

**A. Appropriations Language and Analysis of Appropriations Language**

**Appropriations Language for Construction**

*For necessary expenses, to include the cost of equipment, furniture, and information technology requirements, related to construction or acquisition of buildings, facilities and sites by purchase, or as otherwise authorized by law; conversion, modification and extension of Federally-owned buildings; preliminary planning and design of projects; and operation and maintenance of secure work environment facilities and secure networking capabilities; $80,892,000, to remain available until expended.*

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.

1. Report of the Congressional Oversight Panel (dated 02/10/2010), entitled "Commercial Real Estate Losses and the Risk to Financial Stability." [↑](#footnote-ref-1)
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. [↑](#footnote-ref-2)
3. McAfee, *Unsecured Economies: Protecting Vital Information*, 2009 [↑](#footnote-ref-3)
4. This survey was conducted in 2005 and is the most recent data point available. While the trend has hopefully improved, the statistic still underscores the lack of visibility Law Enforcement has into these incidents. [↑](#footnote-ref-4)
5. The National Institute of Justice, Tribal Crime and Justice: Social and Legal Contexts. http://www.ojp.usdoj.gov/nij/topics/tribal-justice/contexts.htm. [↑](#footnote-ref-5)