U.S. Department of Justice
Federal Bureau of Investigation

FY 2011
Authorization and Budget Request to Congress

February 2010

Table of Contents

I. OVERVIEW FOR THE FEDERAL BUREAU OF INVESTIGATION

A. Introduction

Budget Summary: The Federal Bureau of Investigation's (FBI's) Fiscal Year (FY) 2011 budget request proposes a total of $8,264,677,000 in direct budget authority, including 33,810 permanent positions (13,057 Special Agents, 3,165 Intelligence Analysts (IAs), and 17,588 Professional Staff) and 32,908 full time equivalents (FTE). The request includes a total of $8,083,475,000 for Salaries and Expenses and $181,202,000 for Construction, and is critical to the FBI's investment strategy to acquire capabilities needed to counter known or anticipated national security threats and crime problems.

The FBI request includes 812 new positions (276 Special Agents, 187 IAs, and 349 Professional Staff) and 510 FTE. Additionally, a total of $306,642,000 in new funding is requested – $232,750,000 for Salaries and Expenses and $73,892,000 for Construction. This new funding would support several critical initiatives, to include:

- Cybersecurity;
- Counterterrorism and counterintelligence investigations;
- Child Exploitation investigations;
- Intelligence gathering and analysis;
- Mortgage fraud and other white collar crime investigations;
- WMD preparedness and response; and
- Priority facility construction.

In addition to directly appropriated resources, the FBI proposes reimbursable resources in the amount of $1,534,820,000 and 3,399 FTE for FY 2011. These totals include $134,929,000 and 776 FTE pursuant to the Health Insurance Portability and Accountability Act (HIPPA) of 1996. Reimbursable resources also include $148,467,000 and 868 FTE under the Interagency Crime and Drug Enforcement Program and $189,855,000 and 1,303 FTE for the Fingerprint Identification User Fee and the National Name Check Programs. The remaining reimbursable resources are used to facilitate a number of activities, including pre-employment background investigations, providing assistance to victims of crime, and temporary assignment of FBI employees to other agencies.

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

Department of Justice

As a component of the DOJ, the FBI's efforts contribute to DOJ's overall strategic goals and objectives in multiple ways. Listed below are the DOJ strategic goals and objectives to which the FBI contributes, along with the total level of resources being requested in FY 2011 (Salaries and Expenses) that will support each of the goals.

Strategic Goal 1: Prevent Terrorism and Promote the Nation's Security: $4,871,077,000

- 1.1: Prevent, disrupt, and defeat terrorist operations before they occur

- 1.2: Strengthen partnerships to prevent, deter, and respond to terrorist incidents
- 1.4: Combat espionage against the United States

Strategic Goal 2: Prevent Crime, Enforce Federal Laws and Represent the Rights and Interests of the American People: $3,212,398,000

- 2.1: Strengthen partnerships for safer communities and enhance the Nation's capacity to prevent, solve, and control crime
- 2.2: Reduce the threat, incidence, and prevalence of violent crime
- 2.3: Prevent, suppress, and intervene in crimes against children
- 2.4: Reduce the threat, trafficking, use, and related violence of illegal drugs
- 2.5: Combat public and corporate corruption, fraud, economic crime, and cybercrime
- 2.6: Uphold the civil and Constitutional rights of all Americans

Organization of the FBI: The FBI operates field offices in 56 major United States cities and over 400 "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 65 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 United States 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 Office of International Operations, and the Office of Law Enforcement Coordination.
- The Science and Technology Branch, which includes the Criminal Justice Information Services Division, the Laboratory Division, the Operational Technology Division, and the Special Technologies and Applications Office.

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

- The Chief Information Officer oversees the Office of Information Technology Program Management, the Office of Information Technology Policy and Planning, and the Information Technology Operations Division, and the Office of IT Systems Development.
- 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 though 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

National Security Threats

In an effort to better address all aspects of the FBI's requirements, the FY 2011 budget has been structured according to the threats that the FBI works to deter. The FY 2011 threat packages include: Terrorism, Foreign Counterintelligence, White Collar Crime, Violent Crime and Gangs, Child Exploitation, Weapons of Mass Destruction, Organized Crime, and Operational Enablers. These threats have been identified by the Director as the FBI's priorities and thus must be resourced accordingly. Within each threat package, both operational and support requirements are integrated to show the areas necessary when counteracting a threat. Without the proper support and operational requirements, a threat cannot be adequately addressed.

Terrorism Threat: Terrorism, in general, and al-Qa'ida and its affiliates in particular, continue 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 United States and continues to include proven tactics and tradecraft with adaptations designed to address its losses and the enhanced security measures of the United States. Al-Qa'ida continues to seek to infiltrate overseas operatives who have no known nexus to terrorism into the United States 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 United States. 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.

The diversity of homegrown extremists and the direct knowledge they have of the United States potentially poses a very serious threat. The radicalization of United States Muslim converts is of particular concern. While conversion to Islam, in itself, does not lead to radicalization, converts appear to be more vulnerable and in situations that put them in a position to be influenced by Islamic extremists.

While much of the national attention is focused on the substantial threat posed by international terrorists to the Homeland, the United States must also contend with an ongoing threat posed by domestic terrorists based and operating strictly within the United States. Domestic terrorists, motivated by a number of political or social issues, continue to use violence and criminal activity to further their agendas.

Weapons of Mass Destruction Threat: The global Weapons of Mass Destruction (WMD) threat to the United States 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, Nuclear (CBRN) through 2013. The assessment concluded that it remains the intent of terrorist adversaries to seek the means and capability to use WMD against the United States 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 WMD is a "religious duty" and is reported to have sought to perpetrate a "Hiroshima" on United States soil. Globalization makes it easier for terrorists, 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 WMD have been active and as such "the margin of safety is shrinking, not growing."

Foreign Intelligence Threat: The foreign intelligence threat to the United States continues to increase as foreign powers seek to establish economic, military, and political preeminence and to position themselves to compete with the United States in economic and diplomatic arenas. The most desirable United States 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 United States 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 United States institutions.

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 United States 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.

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 United States national security.

Criminal Enterprises and Federal Crime Problems

White Collar Crime: The White Collar Crime (WCC) problem focuses on six priorities: (1) Corporate, Security, and Commodities frauds; (2) Financial Institution Fraud (FIF); (3) Public Corruption; (4) Health Care Fraud (HCF); (5) Insurance Fraud; and (6) Money Laundering. Today's most significant white collar issue – mortgage fraud – falls within both Corporate and Financial Institution fraud.

- Corporate and Financial Institution Fraud: The FBI has identified mortgage fraud as the number one problem in these two WCC programs. The number of pending investigations of mortgage fraud against financial institutions has risen from 436 at the end of FY 2003 to over 2,600 by the end of FY 2009. Many of these investigations involve traditional mortgage frauds where the creditworthiness of the loan applicant is exaggerated by relatively small-time operators attempting to defraud banks or other lending institutions. The FBI also recently initiated 19 corporate fraud cases involving sub-prime mortgage lending companies. In addition to significant financial losses to investors, corporate fraud has the potential to cause immeasurable damage to the United States economy and investor confidence. The FBI is focusing its efforts on cases which involve accounting schemes designed to deceive investors, auditors, and analysts about the true financial condition of a corporation, self-dealing by corporate executives, and obstruction of justice.

  Although mortgage fraud will be a major priority, the FBI will continue other investigations to safeguard the integrity and credibility of corporations and the securities and commodities markets, and to identify, disrupt, and dismantle criminal organizations and individuals who engage in fraud schemes, which impact financial institutions in the United States.

- Public Corruption: The corruption of local, state, and federally elected, appointed, or contracted officials undermines our democratic institutions and sometimes threatens public safety and national security. Public corruption can affect everything from how well United States borders are secured and neighborhoods protected, to verdicts handed down in courts, and the quality of public infrastructure such as schools and roads. Many taxpayer dollars are wasted or lost as a result of corrupt acts by public officials.

- Health Care Fraud: It is estimated that fraud in health care industries costs consumers more than $60 billion annually. Some of the most prolific and sophisticated WCC investigations during the past decade have involved health care fraud. Today, the FBI seeks to infiltrate illicit operations and terminate scams involving staged auto accidents, online pharmacies, Durable Medical Equipment (DME), 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.
- Insurance Fraud: There are more than 5,000 companies with a combined $1.8 trillion in assets engaged in non-health insurance activities, making this one of the largest United States industries. Insurance fraud increases the premiums paid by individual consumers and threatens the stability of the insurance industry. Recent major natural disasters and corporate fraud scandals have heightened recognition of the threat posed to the insurance industry and its potential impact on the economic outlook of the United States.

- 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.

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 United States' territory, 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 2007, 7,624 total incidents were voluntarily reported by local law enforcement to the FBI's Uniform Crime Reporting Program. Conservative estimates indicate that the level of voluntarily reported hate crimes is less than half of the actual hate crimes that occur annually in the United States.

- Color of Law (COL): COL violations are the deprivation of any rights, privileges, or immunities secured or protected by the United States 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 Inspector Generals for other federal agencies.

- Human Trafficking: The trafficking of persons and violations in the United States is a worldwide human rights crime problem. 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.

Transnational and National Criminal Organizations and Enterprises: Transnational/National 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 six distinct groups: (1) Eurasian Organizations that have emerged since the fall of the Soviet Union (including Albanian Organized Crime); (2) Asian Criminal Enterprises; (3) traditional organizations such as the La Cosa Nostra (LCN) and

Italian Organized Crime; (4) Balkan Organized Crime; (5) Middle Eastern Criminal Enterprises, and (6) African Criminal Enterprises.

Due to the wide range of criminal activity associated with these groups, each distinct organized criminal enterprise adversely impacts the United States in numerous ways. Threats from international organized criminals are covered below.

- International organized criminals control substantial portions of the global energy and strategic materials markets that are vital to United States national security interests. These activities impede access to strategically vital materials, which has a destabilizing effect on United States geopolitical interests and places United States businesses at a competitive disadvantage in the world marketplace.
- International organized criminals provide logistical and other support to terrorists, foreign intelligence services, and hostile foreign governments. Each of these groups is either targeting the United States or otherwise acting in a manner adverse to United States interests.
- International organized criminals smuggle people and contraband goods into the United States, seriously compromising United States border security and at times national security. Smuggling of contraband/counterfeit goods costs United States businesses billions of dollars annually, and the smuggling of people leads to exploitation that threatens the health and lives of human beings.
- International organized criminals exploit the United States and international financial systems to transfer billions of dollars of illicit funds annually.
- International organized criminals use cyberspace to target individuals and United States infrastructure, using an endless variety of schemes to steal hundreds of millions of dollars from consumers and the United States economy. These schemes also jeopardize the security of personal information, the stability of business and government infrastructures, and the security and solvency of financial investment markets.
- International organized criminals are manipulating securities exchanges and perpetrating sophisticated financial frauds, robbing United States consumers and government agencies of billions of dollars.
- International organized criminals corrupt and seek to corrupt public officials in the United States and abroad, including countries of vital strategic importance to the United States, in order to protect their illegal operations and increase their sphere of influence.
- International organized criminals use violence and the threat of violence as a basis for power, and those especially prone to violence are increasingly making inroads in the United States.

In addition to criminal enterprises that are transnational in origin, communities across the United States face challenges from domestic criminal gangs and organizations. Gangs and other American criminal enterprises, operating in the United States and throughout the world, are more violent, more organized, and more widespread than ever before. They pose one of the greatest threats to the safety and security of all Americans.

Finally, 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 CEs; Columbian 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.

Violent Crimes: Preliminary Uniform Crime Report statistics for 2008 indicate a 3.5 percent decrease nationally in violent crimes (murder and non-negligent manslaughter, forcible rape, robbery, and aggravated assault) for the first six months of the year compared to the same period in 2007. This follows a slight decline (1.4 percent) for all of 2007 compared to 2006. The 2008 decline was enjoyed by cities of all sizes and by both metropolitan and non-metropolitan counties, although the decrease for very large cities (one million and over) was less than one percent, perhaps due in part to gang violence.

While this overall trend is encouraging, individual violent crime incidents, such as sniper murders, serial killings, and child abductions remain threats to paralyze whole communities and stretch state and local law enforcement resources to their limits. In addition, crimes against children, including child prostitution and crimes facilitated through the use of the Internet, continue to serve as a stark reminder of the impact of violent crime on the most vulnerable members of society.

Indian Country: The FBI has 104 full-time dedicated SAs who currently address 2,406 Indian Country (IC) cases on approximately 200 reservations. Seventy-five percent of the cases are investigated in the Minneapolis, Salt Lake City, Phoenix, and Albuquerque Field Offices. Fifty percent of the cases involve death investigations, sexual and physical assault of children, and felony assaults, with little or no support from other law enforcement agencies due to the jurisdictional issues in IC. There are only half as many law enforcement personnel in IC as in similar sized rural areas. Tribal authorities can only prosecute misdemeanors of Indians, and state/local law enforcement do not have jurisdiction within the boundaries of the reservation, with the exception of Public Law 280 states and tribes. The Indian Gaming Industry reported 26.7 billion dollars in revenue in 2008 and has very few FBI dedicated resources. There are 18 Safe Trails Task Forces who address drug/gang and violent crimes in IC. The current gang problem 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.

Gang Violence: The United States has seen a tremendous increase in gangs and gang membership. Gang membership has grown from 55,000 in 1975 to approximately 960,000 nationwide in 2007. The FBI National Gang Intelligence Center (NGIC) has determined that there are identified street gangs and gang members in all 50 states and the District of Columbia. Thirty-nine of these gangs have been identified as national threats based on criminal activities and interstate/international ties. NGIC estimates the direct economic impact of gang activity in the United States at $5 billion and the indirect impact as much greater. Furthermore, NGIC identified a trend of gang members migrating to more rural areas. This information would correspond with the increased inquiries from local law enforcement agencies in rural and suburban areas regarding participating in Safe Streets Task Forces. NGIC has also seen an expansion of United States based gangs internationally, with such gangs currently identified in over 20 countries.

Impact of External Drivers and Influences

The FBI's budget builds upon both current knowledge of threats and crime problems and a forward look to how terrorists, foreign agents and spies, and criminal adversaries are likely to adapt tactics and operations in a constantly evolving and changing world. This forward look helps inform and determine the critical operational and organizational capabilities the FBI must acquire over the same time period to remain vital and effective in meeting future threats and crime problems.

When assessing the impact of the external operating environment, United States Government, private industry, and others generally look to global "drivers" – broad factors that can directly or indirectly cause changes in the future threat environment – to guide their thinking and planning. In examining forecasts and assessments of the future, the most likely drivers that the FBI must take into consideration, and some of the likely operational impacts, include the following:

- Global and domestic demographic changes – expanded need for operations abroad as more investigations and operations include an international nexus; growth in immigrant and émigré populations within the United States present new language and cultural barriers during investigations;
- Communications revolution – advances in communications technology challenge the ability of the FBI to perform court-authorized intercepts; use of encryption and other communications technologies requires closer access to end-nodes; identity theft will make perpetrator identification more difficult;
- Global economic changes – terrorism and organized crime converge; greater need for coordinating countermeasures with foreign countries and financial organizations;
- Rising belief in non-material values abroad – increasing danger to agents working abroad as anti-Americanism increases and actors disperse; easier acceptance of "suicide" missions among disaffected, alienated individuals;
- Technological and scientific revolutions – reduced ability for threat groups or governments to hide undercover identity of agents; increase in espionage and cyber crime against United States corporations; increased opportunity for "bio-terror" as well as "bio-error;" inexpensive computing technology stretches FBI forensic science capacities;
- Revolutions in security technology and practice – more "policing" actions abroad by non-government, contract private entities; more espionage against United States defense and contractors; advances in biometric technologies and science permit greater opportunities for positive identification of individuals; and
- Changing role of state and law – need to cooperate with more entities; need more methods of cooperation beyond task forces and cases.

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

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

Most experts believe that technological innovation will have the most profound impact on the collective ability of the federal, state, and local governments to protect the United States. Advances in information technology, as well as other scientific and technical areas, have created the most significant global transformation since the Industrial Revolution. These advances allow terrorists, disaffected states, weapons proliferators, criminal enterprises, drug traffickers, and other threat enterprises easier and cheaper access to technology to facilitate crime, including computer, communications, and weapons technology. It is essential – but difficult – for law enforcement countermeasures to stay ahead of the increasing use of technology for illegal purposes.

To meet these threats and crime problems and operate successfully in a challenging external environment, the FBI needs to be able to fuse and integrate intelligence and law enforcement. As a member of the Intelligence Community, the FBI has placed an increased emphasis on threat-based, intelligence-driven investigations and operations, especially in the areas of counterterrorism and counterintelligence, and on internal and external information sharing. The FBI must also create an awareness of, and become receptors for, changes in threats and the ability to make immediate corrections in FBI priorities and focus to address those changes. Finally, the FBI must recognize that alliances with others in law enforcement, at home and abroad, are absolutely essential.

C. FBI's 2011 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 2011 budget upon addressing eight key national security and criminal threats noted above. 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 these threats in FY 2011:

- National Security – Requested FY 2011 Increases: 90 positions (27 Agents, 32 IAs) and $25,179,000 ($8,275,000 non-personnel)
- Weapons of Mass Destruction – Requested FY 2011 Increases: 35 positions (15 Agents), and $9,141,000 ($2,600,000 non-personnel)

- Render Safe – Requested FY 2011 Increases: 13 positions (6 Agents) and $40,000,000 ($35,756,000 non-personnel)
- Computer Intrusions – Requested FY 2011 Increases: 163 positions (63 Agents, 46 IAs), and $45,926,000 ($14,737,000 non-personnel).
- Child Exploitation – Requested FY 2011 Increases: 20 positions (4 Agents, 1 IA), and $10,838,000 ($6,242,000 non-personnel).
- White Collar Crime – Requested FY 2011 Increases: 367 positions (143 Agents, 39 IAs), and $75,265,000 ($897,000 non-personnel).
- Organized Crime – Requested FY 2011 Increases: 4 positions (3 Agents), and $952,000.
- Violent Crime/Gangs – Requested FY 2011 Increases: 2 positions and $328,000.

In addition to addressing these threats, the FBI's FY 2011 budget focuses on critical operational enabling resources required to ensure these threats are addressed and neutralized. The FBI's budget request includes additional resources for its overall Intelligence Program, intelligence sharing and analysis tools, information technology upgrades, and facility improvements. The FBI requests an increase of 118 positions (15 Agents, 69 IAs), and $99,013,000 ($79,892,000 non-personnel) for these initiatives in FY 2011.

The following six enterprise-wide capabilities that the FBI identified are critical to ensuring the FBI possesses the capabilities and capacities to carry out its national security and criminal investigative missions to thwart the threats listed above. The capabilities are:

- Domain and Operations: A mature enterprise capability for employing intelligence and analysis to identify and understand the national security threats and crime problems challenging America, and developing and executing operational strategies to counter these threats and crime problems;
- Surveillance: Surveillance (physical, electronic, human source) and operational technology capabilities to meet operational requirements;
- Partnerships: An established and productive network of partnerships with local, state, federal, and international law enforcement and criminal justice agencies;
- Leveraging Technology: An enhanced capability for providing forensic, operation technology, identification, training, and criminal justice services to our local, state, federal, and international partners;
- Workforce: A professional workforce that possesses the critical skills and competencies (investigative, technical, analytical, language, supervisory, and managerial), experiences, and training required to perform our mission; and
- Infrastructure: A safe and appropriate work environment and information technology infrastructure to facilitate the performance of the FBI's mission.

As part of its strategic planning process and development, the FBI is continuing to refine the definition of these capabilities and is continuing to incorporate them into its over-arching Strategy Management System (SMS), discussed below. The following chart illustrates the relationship between the FBI's budgetary end-state capabilities and its SMS themes.

SMS Theme	SMS Objectives		Capability	Definition
Management Excellence	P1: Streamline administrative and operational processes; P2: Assign responsibility and own accountability; P3: Maximize organizational collaboration; P11: Incorporate forecasting and planning into FBI processes; P12: Improve internal communication		ALL	*Note: This SMS theme is woven throughout all End States and does not have its own End State associated.*
Deter, Detect and Disrupt National Security Threats and Criminal Activity	P4: Collection; P5: Information dissemination and integration; P6: Analysis; P7: Action and/or Requirements	→	Surveillance	A surveillance (physical, electronic, human source) and operational technology capability to meet operational requirements
			Domain and Operations	A mature enterprise capability for employing intelligence and analysis to identify and understand the national security threats and crime problems challenging America, and developing and executing operational strategies to counter these threats and crime
Maximize Partnerships	P8: Expand partner relationships; P9: Enhance international operations; P10: Enhance trust and confidence in the FBI	→	Partnerships	An established and productive network of partnerships with local, state, federal, and international law enforcement and criminal justice agencies
Maximize Workforce Success	T1: Improve recruiting, selection, hiring and retention; T2: Train and develop skills and abilities of our workforce; T3: Link skills and competencies to needs; T4: Identify, develop and retain leaders throughout our organization	→	Workforce	A professional workforce that possesses the critical skills and competencies (investigative, technical, analytical, language, supervisory, and managerial), experiences, and training required to perform our mission
	T5: Enhance work environment to facilitate mission	→	Infrastructure	A safe and appropriate work environment and information technology to facilitate the performance of the FBI's mission
Leverage Technology and Science	T6: Align science and technology to our strategic objectives; T7: Deploy technology and science to make our workforce more effective and efficient	→	Leveraging Technology	An enhanced capability for providing forensic, operation technology, identification, training, and criminal justice services to our local, state, federal, and international partners
Optimize Resources	R1: Utilize and align existing resources and assets in an efficient manner; R2: Secure and align appropriate resources		ALL	*Note: This SMS theme is woven throughout all End States and does not have its own End State associated.*

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 the efforts of the SET team; (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 has implemented a Strategy Management System to guide its strategy development and decision-making. Through the SMS, the FBI will 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, will help address both the current mission and position the FBI to meet future challenges.

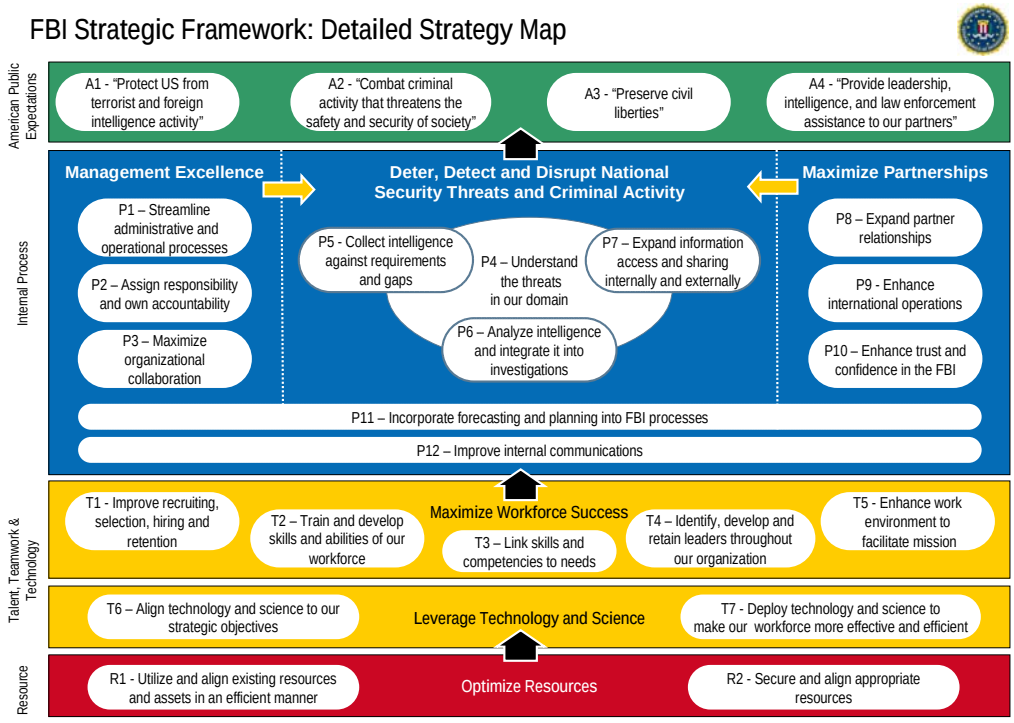
  The SMS is based on the balanced scorecard management tool adapted by the FBI for its own unique structure, culture, and mission. The Strategic Management System will provide a formal method for executing and reviewing strategy, and making that strategy a part of daily activities and decision-making. Specifically, the SMS will:

  - Provide a common framework to ensure that executive leadership clarifies and gains consensus around a single, unified strategy;
  - Link strategic and operational decision-making;
  - Provide a balanced set of measures to monitor strategic performance;
  - Create a vehicle to assign accountability for specific performance objectives and measures;
  - Institute regularly scheduled strategy review meetings to focus executives on strategic objectives/measures and provide a forum for strategy discussions and debates;

- Enable more objective and strategic resource allocation decisions; and
- Communicate the FBI's strategy throughout the organization, thereby creating both a common language and a "line of sight" between individuals and the strategy they support.

The FBI Strategy Map consists of 25 strategic objectives. Each objective has between one and three measures and each measure has a target that defines success. Key corporate strategic initiatives have been identified and progress tracked to close any performance gaps. The FBI "enterprise" objectives and measures will eventually cascade down to each part of the organization, including field offices, and executive management will review each component's progress in achieving its objectives through regular strategy review meetings and through the performance appraisal system.

The SMS is a continuous process for driving evolutionary improvements. Reviews will not only track strategic progress, they will 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 will be provided with the support they need to succeed or will be eliminated, and other initiatives will be added to address identified gaps. The SMS will provide the flexibility the FBI needs to stay ahead of changing threats and demographic and other trends that impact its mission.



- The Strategic Execution Team (SET): The Strategic Execution Team was created by Director Mueller in September 2007 to build on the FBI's Strategy Management System and accelerate improvements in the intelligence arena. The team was made up of FBI employees in different job roles from both field offices and FBI Headquarters.

SET initiatives and results include:

- Intelligence Operations: The team developed a standardized model for field intelligence that can be adjusted to the size and complexity of small, medium, and large offices. It also developed the Collection Operations Requirements Environment (CORE), an FBI intelligence requirements solution. CORE makes FBI and national intelligence requirements easily accessible to all field office personnel, facilitates completion of FBI forms, and improves information flow between operational squads and the FIGs. It is designed to help generate raw intelligence that is responsive to requirements and to help track progress in meeting those requirements.
- Human Capital: SET established core intelligence tasks for Special Agents, defined their intelligence career path, and tailored individual development plans. Additionally, SET worked on refining the Intelligence Analyst career path, including training, experiences, and roles that are required to develop this cadre.
- Program Management: SET identified six core desired strategic shifts and ways to achieve them (i.e., from criminal vs. intelligence to integrated mission, from limited internal information-sharing to internal/external information-sharing with intelligence community.)

- 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. This approach is also intended to bring continuity to the FBI's budget.

- Decision Units: The FBI's budget is based on four Decision Units that align with the key areas of FBI operations. These four Decision Units, established by the FY 2005 Consolidated Appropriations Act, are:

  - Intelligence
  - Counterterrorism/Counterintelligence
  - Criminal Enterprises and Federal Crimes
  - Criminal Justice Services

  The costs of support functions are prorated to programs in each of the four Decision Units, providing a better picture of the full cost of each of the four major mission areas. These support functions include training, human resources, inspection, security, finance, records management, information technology, and facilities and logistics services. Support costs were allocated to individual programs based on historical information about use of the services, or by using factors that are primary determinates of the level of use of a particular service, such as the number of employees. Now, support functions are applied to the division within each decision unit responsible for executing those funds. Full program costing links budgets to strategic planning, and enables the development of measures of program performance.

- Managed Growth: The FBI continues to work within its recognized organizational capacities, such as hiring and training, and other internal constraints, such as information technology, facilities, and other infrastructure. The 2011 budget proposes enhancements to

grow critical hiring and training process capacities – such as training classrooms and other training facilities – to accommodate personnel growth.

D. Environmental Accountability

The FBI has begun developing an Organizational Environmental Management System (EMS) that will provide a corporate-wide standard to deploy to the field offices and major facilities (to include CJIS, Quantico, and JEH). This organizational EMS is slated to be developed and implemented by the end of FY 2010, with individual facility EMSs to follow. 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 also has developed and deployed green purchasing training to all government purchase card holders, Contracting Officers Technical Representatives, and Contracting Officers. This training reviews the green purchasing requirements and the methods in which members of the FBI acquisition workforce can meet the requirements. This training is provided to over 500 members of the acquisition workforce annually.

The FBI has developed a sustainable building policy that addresses requirements of Executive Order 13423, 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/Ranking	Description	Pos.	FTE	Dollars ($000)	Page
Salaries and Expenses Enhancements					
1. Computer Intrusions	To increase the FBI's efforts to combat attacks against the U.S. information infrastructure.	163	81	45,926	5-1
2. White Collar Crime	To address increasing mortgage, corporate, and securities and commodities fraud schemes.	367	289	75,265	5-8
3. Operational Enablers	To address shortfalls in the FBI's information technology (IT) infrastructure, enhance laboratory capabilities, and to bolster the FBI's intelligence program.	118	59	25,121	5-17
4. National Security Threats	To expand the FBI's surveillance capabilities, intelligence analysis resources, and Legal Attache program to address National Security threats.	90	44	$25,179	5-24
5. Weapons of Mass Destruction (WMD)	To further develop the FBI's ability to implement wide-spread countermeasures, provide rapid responses to WMD incidents, and enhance the collection and analysis of related WMD materials, technology, and information.	35	18	9,141	5-25
5. WMD/Render Safe Capability	To provide response aircraft and personnel for the FBI's WMD response mandates.	13	6	40,000	5-30
6. Violent Crime/Gangs	To increase investigative efforts to thwart crime in Indian Country.	2	1	328	5-32
7. Child Exploitation	To more efficiently and effectively safeguard the nation's youth.	20	10	10,838	5-35
8. Organized Crime	To modernize the law enforcement approach to combatting International Organized Crime.	4	2	952	5-43
Subtotal, Salaries and Expenses Enhancements		**812**	**510**	**$232,750**	

Threat Name	Description	Pos.	FTE	Dollars ($000)	Page
Construction Enhancements					
Operational Enablers	To provide funding for priority construction projects at the FBI Academy, to include a new dormitory.	…	…	$73,892	8-1
Subtotal, Construction Enhancements		**…**	**…**	**$73,892**	
Total, FBI Direct Enhancements		**812**	**510**	**$306,642**	
Offsets					
Travel	To reduce FBI travel funding including travel for operational requirements as well as conferences and educational functions.	…	…	($10,282)	6-1
Cyber Education and Development	Improvements in information technology and online training programs have created opportunities to reduce training costs by reducing costs of delivery. Because of this, the FBI proposes to reduce cyber training funding.	…	…	(3,200)	6-2
Vehicles	This proposed reduction will limit vehicle purchases to those necessary to maintain the size of the current vehicle fleet.	…	…	(3,788)	6-3
Rescission of Prior Year TEDAC Appropriations	This proposal rescinds funding from available TEDAC balances.	…	…	[98,886]	6-4
Total, Offsets		**…**	**…**	**($17,270)**	
Grand Total, Program Changes		**812**	**510**	**$289,372**	

Note: Detailed initiative rankings are included in the Classified Addendum.

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, [$7,658,622,000] *$8,083,475,000*, [of which $101,066,000 is designated as being for overseas deployments and other activities pursuant to sections 401(c)(4) and 423(a)(1) of S. Con. Res. 13 (111th Congress), the concurrent resolution on the budget for fiscal year 2010; and] of which not to exceed $150,000,000 shall remain available until expended: *Provided*, That not to exceed *$205,000* shall be available for official reception and representation expenses[: *Provided further*, That notwithstanding section 205 of this Act, the Director of the Federal Bureau of Investigation, upon a determination that additional funding is necessary to carry out construction of the Biometrics Technology Center, may transfer from amounts available for ``Salaries and Expenses'' to amounts available for ``Construction'' up to $30,000,000 in fees collected to defray expenses for the automation of fingerprint identification and criminal justice information services and associated costs: *Provided further*, That any transfer made pursuant to the previous proviso shall be subject to section 505 of this Act]. (Department of Justice Appropriations Act, 2010.)

Analysis of Appropriations Language

Deletes language designating $101,066,000 for Overseas Contingency Operations.

Deletes language authorizing the Director of the Federal Bureau of Investigation to transfer up to $30,000,000 from this account to the Construction account for the Biometrics Technology Center.

IV. Decision Unit Justification

A. Intelligence Decision Unit

INTELLIGENCE DECISION UNIT TOTAL	Perm. Pos.	FTE	Amount ($000)
2009 Enacted with Rescissions	6,217	5,906	$1,487,262
2009 Supplementals	…	…	7,592
2009 Enacted w/ Rescissions and Supplementals	6,217	5,906	1,494,854
2010 President's Budget	6,878	6,455	1,606,025
Adjustments to Base and Technical Adjustments	38	277	86,704
2011 Current Services	6,916	6,732	1,692,729
2011 Program Increases	266	134	55,513
2011 Program Offsets	…	…	(2,796)
2011 Request	7,182	6,866	1,745,446
Total Change 2010-2011	**304**	**411**	**$139,421**

Intelligence Decision Unit—Information Technology Breakout	Perm. Pos.	FTE	Amount* ($000)
2009 Enacted with Rescissions	222	222	$277,707
2009 Supplementals	…	…	…
2009 Enacted w/Rescissions and Supplementals	222	222	277,707
2010 President's Budget	281	281	278,158
Adjustments to Base and Technical Adjustments	(18)	(18)	(20,221)
2011 Current Services	299	299	257,937
2011 Program Increases	…	…	200
2011 Request	299	299	258,137
Total Change 2010-2011	**(18)**	**(18)**	**($19,439)**

*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

A goal of FBI Intelligence Analysts (IAs) is to anticipate customer requirements and proactively identify intelligence gaps associated with criminal or national security threats. Intelligence analysis is fundamental to understanding these threats to national security and ultimately to developing a deeper understanding of tomorrow's potential threats. To protect national security, the FBI must focus significant analytic resources to analyze the threat, its nature, potential courses of action, and to then put this threat analysis in the context of ongoing intelligence and investigative operations. The FBI's intelligence analysis capability consists of various resources that involve analyzing information collected from a variety of Confidential Human Sources (CHSs) and reporting this collected information as "intelligence products" to the customers at all levels of government through a variety of information sharing channels. The products generated by intelligence analysis drive FBI investigative and operational strategies by ensuring that these strategies are based on an enterprise-wide understanding of the current and future threat environment.

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 coordination, 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, 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.

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 19,308 known or suspected terrorists (KST) domestically as well as globally in FY 2008 alone. Additionally, it has allowed FBI field offices to open 471 KST cases against targets which were previously unknown by the IC and law enforcement community to be present in the United States.

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 and provide access, using analytical tools, to FBI Foreign Intelligence Surveillance Act (FISA) electronic surveillance data and data from seized media for analysis and exploitation by FBI and IC Agents, IAs, and linguists.

Infrastructure and Technology
The Intelligence Decision Unit (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, dissemminate, 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.

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 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, send notifications and alerts, and provide an avenue to remotely access other law enforcement and intelligence systems and resources. LEO currently supports a user base of more than 142,000 vetted members that can access LEO through any connection to the Internet such as cable modem, Digital Subscriber Line, Local Area Network, or a 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.

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 USIC. In an effort to train the intelligence workforce and to build a cadre of highly skilled intelligence professionals, the FBI is developing a competency-based career path for Special Agents and Intelligence Analysts. 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.

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 2009		FY 2009		2010 Enacted		Current Services Adjustments & FY2011 Program Changes		FY 2011 Request	
Total Costs and FTE		**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		5,906	1,494,854	5,187	1,217,000	6,455	1,606,025	411	139,421	6,866	1,745,446
TYPE / GOAL / STRATEGIC OBJECTIVE	**FY 2008**	**FY 2009**		**FY 2009**		**2010 Enacted**		**Current Services Adjustments & FY2011 Program Changes**		**FY 2011 Request**	
Performance Measure	% of Counterterrorism FISA collection reviewed by the Language Program: • Audio • Text • Electronic File		100% 100% 100%		85% 100% 87%		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)		90%		97%		95%		--		95%
Performance Measure: *Responsiveness*	% of FBI *Field Office* finished intelligence reports that are responsive to National Intelligence Priority Framework topics. (Internally disseminated)		90%		100%		95%		--		95%
Performance Measure: *Responsiveness*	% of FBI finished intelligence reports that are responsive to National Intelligence Priority Framework topics. (Disseminated to Intelligence Community)		90%		96%		95%		--		95%

TYPE / GOAL / STRATEGIC OBJECTIVE	PERFORMANCE	FY 2009	FY 2009	2010 Enacted	Current Services Adjustments & FY2011 Program Changes	FY 2011 Request
Performance Measure: *Accuracy*	Number of high priority sources put through an enhanced validation process.	This information is Classified.				
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.	42%	42%	44%	--	44%
Efficiency Measure (Discontinued Measure)	Staff time (in workyears) saved on asset management activities through changes in the human source business process (via the new "Delta" system).	1,627	0	N/A	--	N/A
Efficiency Measure (New Measure)	% of FBI Confidential Human Sources (CHS) validated	25%	14%	25%	--	25%

Data Definition, Validation, Verification, and Limitations:

- All data are provided by records maintained and verified by the FBI's Directorate of Intelligence, except for LEO data which are provided through CJIS Division. 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
		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%	 100% 100% 100%	 85% 100% 87%	 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%	90%	97%	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%	90%	100%	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%	90%	96%	95%	95%
Performance Measure: *Accuracy*	Number of high priority sources put through an enhanced validation process.	This information is Classified.									
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.	N/A	N/A	45%	39%	26%	41%	42%	42%	44%	44%
Efficiency Measure (Discontinued Measure)	Staff time (in workyears) saved on asset management activities through changes in the human source business process (via the new "Delta" system).	0	0	0	0	0	0	1,627	0	N/A	N/A
Efficiency Measure (New Measure)	% of FBI Confidential Human Sources (CHS) validated	N/A	N/A	N/A	N/A	N/A	N/A	25%	14%	25%	25%

2. Performance, Resources, and Strategies

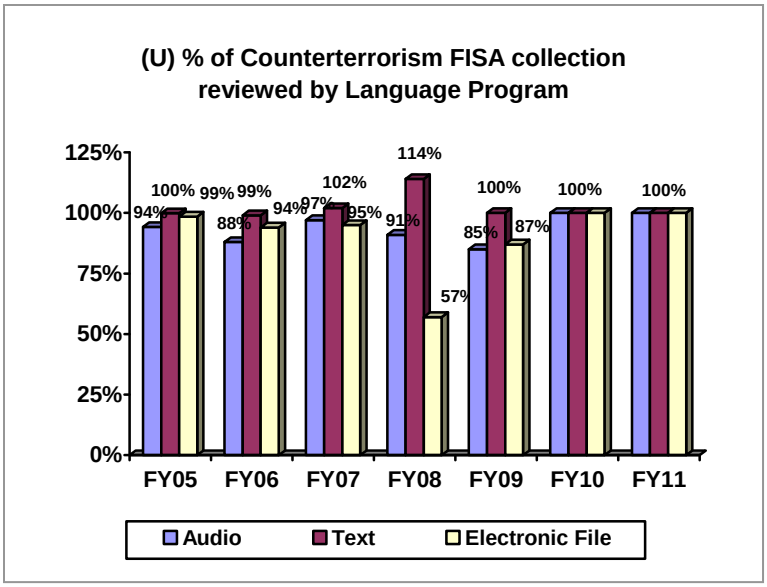
The Intelligence Decision Unit contributes to DOJ's first two Strategic Goals: Goal 1, "Prevent Terrorism and Promote the Nation's Security" (Objectives 1.1, 1.2, & 1.4) and Goal 2, "Prevent Crime, Enforce Federal Laws, and Represent the Rights and Interests of the American People" (Objectives 2.1-2.6). 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 Directorate of Intelligence (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.

Measure changes for this performance report are proposed as a result of an internal review of the FBI's performance measures, pursuant to an initiative coordinated by DOJ's Performance Improvement Officer (PIO) Panel in Spring, 2009.

a. Performance Plan and Report for Outcomes

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



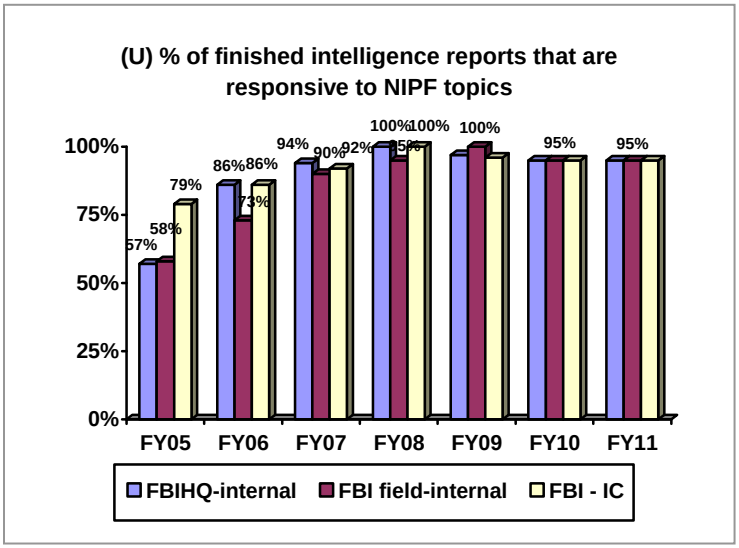
FY 2009 Target: 100% for Audio
100% for Text
100% for Electronic File

FY 2009 Actual: 85% for Audio
100% for Text
87% for Electronic File

Discussion: Collection of Counterterrorism is anticipated to expand by 138 % between FY 2008 and FY 2011, while the FBI's processing capacity will only grow by 11%. Without the enhancement, the FBI's ability to process incoming foreign language terrorism-related collections will decline significantly, compromising the overall effectiveness of all other Counterterrorism initiatives. The failure to provide timely and accurate translation of foreign language material has been identified by Congress, numerous special panels and committees, the media and the Executive Branch as a major vulnerability in the Intelligence Community. At current staffing and funding levels, the FBI is unable to meet the need to address all collected FISA Counterterrorism materials. Even though the substantive divisions prioritize their FISA needs via a complex five-tiered schema with high/medium/low subcategories within each tier and readjust these based on their changing priorities, at present only 78% of all foreign-language collected material is being reviewed. The volume and diversity of the material is simply too great for available resources to process it all. Without the enhancement, the FBI would see the backlog of unprocessed material grow exponentially with the attendant risk that actionable intelligence will be lost. The consequences of such a missed opportunity will be serious. As the Department begins prosecuting cases developed from years of investigative work (an 876% increase since 9/11/01), the FBI's linguists will be called upon more and more to ensure compliance with the Brady requirements and prepare labor-intensive verbatim translation for use in court, further eroding the processing of incoming collections.

FY 2010 Target: 100% for each category
FY 2011 Target: 100% for each category

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



FY 2009 Target: 90%
FY 2009 Actual: 97%

Discussion: This measure illustrates the Intelligence Program's responsiveness to Intelligence Community (IC) intelligence priorities (i.e., whether or not the finished intelligence produced by the FBI is filling important, high priority intelligence gaps). Because the FBI has some regional or local priorities to fulfill, there will always be some intelligence reports filed that are of interest to the Bureau and its law enforcement colleagues but are not responsive to national-level NIPF topics.

FY 2010 Target: 95%
FY 2011 Target: 95%

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

FY 2009 Target: 90%
FY 2009 Actual: 100%

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

FY 2010 Target: 95%
FY 2011 Target: 95%

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

FY 2009 Target: 90%
FY 2009 Actual: 96%

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

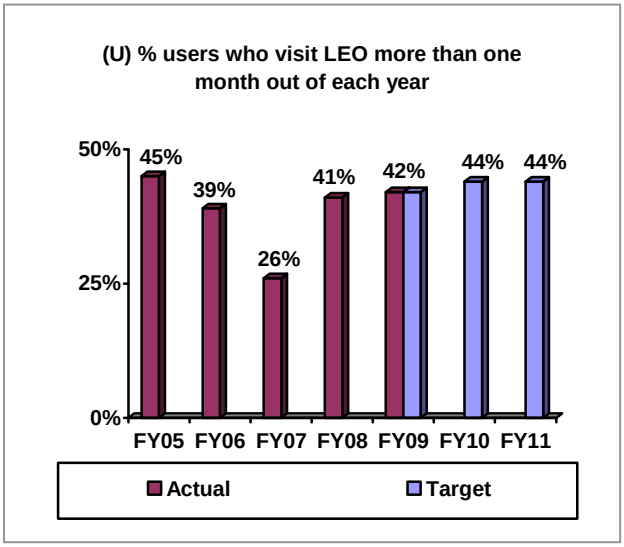
FY 2010 Target: 95%
FY 2011 Target: 95%

***Performance Measure -- Accuracy*:** Number of high priority sources put through an enhanced validation process

Refer to classified version.

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 134,000 vetted members.

FY 2009 Target: 42%
FY 2009 Actual: 42%



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 FY10. 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.

FY 2010 Target: 44%
FY 2011 Target: 44%

Efficiency Measure: DISCONTINUED MEASURE: Staff time (in work years) saved on source management activities through changes in the human source business process (via the new "Delta' system).

FY 2009 Target: 1,627
FY 2009 Projected Actual: 0

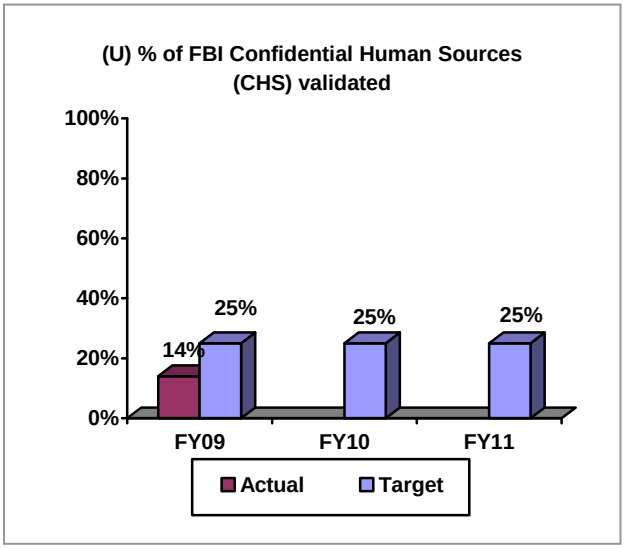
Discussion: The FBI has deployed the "Delta" system that facilitates implementation of a major change in the FBI's Confidential Human Source (CHS) management business process. Delta automates administrative and management functions that Special Agents (SAs) and support personnel would normally perform for CHS operations. Delta includes user requirements and design functions, such as standardized forms, calendar reminders of Source-related activities, secure storage of Source information, workflow and electronic approval features, pre-populated data fields, pop-up ticklers, and role-based access. This automated application reduces employees' work time, eliminates burdensome paperwork, and increases compliance with requirements and guidelines for handling CHSs. In addition, Delta promotes intelligence information sharing among agents and other members of the Intelligence Community, provides greater protection of source identities, and improves internal source reporting between SAs and selective support personnel.

As agreed, this measure is being discontinued because of concerns the data would always be rough estimates built upon assumptions of how much work was avoided. Instead, the proposed alternative "% of Confidential Human Sources (CHS) validated" will better demonstrate FBI progress in accomplishing a core intelligence activity.

FY 2010 Target: N/A
FY 2011 Target: N/A

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

FY 2009 Target: 25%
FY 2009 Projected Actual: 14%



Discussion:
The ability to meet targets for this measure will develop over the next several years as additional resources (government and contractor personnel) are authorized and appropriated to implement the new validation process. The FBI anticipates improvement based on new hires, training, and increased experience of those on board.

FY 2010 Target: 25%
FY 2011 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 Field Intelligence Groups (FIGs), which manage the FBI's intelligence functions in each Field Office, include members of state and local law enforcement and other intelligence agencies. Additionally, in 29 of the FBI's Field Offices, 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)
2009 Enacted with Rescissions	12,480	12,121	$2,884,041
2009 Supplementals	…	…	60,480
2009 Enacted w/ Rescissions and Supplementals	12,480	12,121	2,944,521
2010 Enacted	12,646	12,092	3,156,342
Adjustments to Base and Technical Adjustments	(39)	276	33,745
2011 Current Services	12,607	12,368	3,190,087
2011 Program Increases	139	69	87,057
2011 Program Offsets	…	…	(7,674)
2011 Request	12,746	12,437	3,269,470
Total Change 2010-2011	**100**	**345**	**$113,128**

Counterterrorism/Counterintelligence Decision Unit – Information Technology Breakout	Perm. Pos.	FTE	Amount ($000)
2009 Enacted with Rescissions	365	365	$407,125
2009 Supplementals	…	…	…
2009 Enacted w/Rescissions and Supplementals	365	365	407,125
2010 Enacted	417	417	396,374
Adjustments to Base and Technical Adjustments	16	16	(10,326)
2011 Current Services	433	433	376,048
2011 Program Increases	…	…	5,441
2011 Request	433	433	381,489
Total Change 2010-2011	**16**	**16**	**($4,885)**

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, 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 24/7 Terrorist Screening Center (TSC) and Foreign Terrorist Tracking Task Force (FTTTF)[1] help identify terrorists and keep them out of

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

the United States. 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 US-bound airplanes from the United Kingdom (U.K.) in July 2006. The experience of the Counterterrorism 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.

Foreign Counterintelligence Program
Refer to classified version.

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.

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.

Management and Support Services

In addition to the CT, FCI, Cyber, CIRG, and Legat Programs, which make up the core elements of the CT/CI Decision Unit, the FBI's various human resources, administrative and security programs provide essential support services. A prorated share of human resources, administrative and support services is scored to the CT/CI Decision Unit based on the percentage of the FBI's core functions that contain CT/CI core elements.

The FBI's human resources and administrative programs lead the FBI through the challenges and changes that are continuously presented to federal law enforcement; provide direction and support to investigative personnel; and ensure that adequate resources are available to address the FBI's criminal investigative, national security, and law enforcement support responsibilities. A prorated share of the resources associated with the Finance Division, Human Resources Division, Inspection Division, Office of Equal Employment Opportunity Affairs, Office of Public Affairs, Office of Congressional Affairs, Office of General Counsel, and Office of Professional Responsibility support the CT/CI Decision Unit.

The FBI's Security Program enables the FBI to serve and protect the American people and protecting and keeping secure FBI people, information, operations and facilities by providing services that enable the FBI to achieve its mission. The FBI's Security Program seeks to prevent and/or neutralize the possibility of the hostile penetration of the FBI by foreign intelligence services (FISs), terrorist groups, or other persons/organizations, and is responsible for the oversight and national coordination of the FBI's efforts to protect national security information (NSI) and sensitive but unclassified (SBU) information within the FBI. The program develops policies and guidelines relative to the FBI's security functions and oversees field security activities.

The mission of the FBI's Training Program is to lead and inspire, through excellence in training and research, the education and development of FBI personnel. The FBI's Training Program provides training to FBI personnel and the law enforcement community. The cornerstone of FBI

training efforts is the New Agent training program, which provides comprehensive instruction to ensure entry level Special Agents possess the basic knowledge and skills required to serve the American public.

The FBI also recognizes a continuing need to provide training and development courses for FBI personnel. This training maintains and enhances the professional skills of FBI personnel in their current assignments, equips personnel to handle investigative and administrative requirements, and develops the leadership and management skills of potential managers and executives.

The FBI Laboratory, one of the largest and most comprehensive criminal laboratories in the world and the only full-service civilian federal forensic laboratory in the U.S., performs examinations of evidence for all duly constituted federal, state, tribal, and local law enforcement agencies in the U.S. upon request. The FBI Laboratory is recognized as the leader in the scientific analysis and solution of crime in the U.S. The successful investigation and prosecution of crimes requires the collection, examination, and scientific analysis of evidence recovered at the scene of the incident and obtained during the course of the investigation. Prosecutors frequently use physical evidence to demonstrate the guilt, either directly or circumstantially, of the person on trial. In other instances, evidence can exonerate individuals wrongly accused of crimes.

The mission of the FBI's Information Technology (IT) Program, which includes the Office of the Chief Information Officer, the Office of IT Policy and Planning, the Office of the Chief Technology Officer, the Office of IT Program Management, and the IT Operations Division, is to provide secure information management and information technology services for the FBI's worldwide operational and administrative activities. This organizational model, which is based on best practices within industry and the federal government, ensured that all FBI IT functions work closely with each other in implementing full life cycle management of all FBI IT systems, programs, and projects. The Information Technology Program develops and procures systems capable of performing effective and efficient case management, information analysis, and intelligence sharing, both internally and with other law enforcement entities. The program is responsible for maintenance of over 50 FBI computer systems, computer data centers, and information technology centers.

The mission of the FBI's Criminal Justice Information Services (CJIS) Division is to reduce terrorist and criminal activities by maximizing the ability to provide timely and relevant criminal justice information to the FBI and qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies concerning individuals, stolen property, criminal organizations and activities, and other law enforcement-related data. The CJIS Division has several major program activities that support this mission including the Integrated Automated Fingerprint Identification System (IAFIS), National Crime Information Center (NCIC), National Instant Criminal Background Check System, Uniform Crime Reporting, and Law Enforcement Online (LEO).

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 2009		FY 2009		2010 Enacted		Current Services Adjustments & FY2011 Program Change		FY 2011 Request	
Number of Cases: Counterterrorism, Counterintelligence, & Computer Intrusions		†		41,874		†		†		†	
Positive encounters with subjects through screening process		20,250		19,043		N/A		N/A		N/A	
Total Costs and FTE		**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		12,121	2,944,521	11,710	2,698,100	12,092	3,156,342	345	113,128	12,437	3,269,470
TYPE/ STRATEGIC OBJECTIVE	**PERFORMANCE**	**FY 2009**		**FY 2009**		**2010 Enacted**		**Current Services Adjustments & FY2011 Program Change**		**FY 2011 Request**	
Program Activity/ 1.1; 1.2	**1. Counterterrorism (CT)**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		7,011	1,718,225	6,994	1,287,104	7,501	1,957,887	6	15,633	7,507	1,973,520
Workload -- # of cases investigated (pending and received)		†		24,016		†		†		†	
Performance Measure (Revised Measure)	Catastrophic Acts of Terrorism	0		0		0		--		0	
Performance Measure	Number of participants in the JTTF	4,450		4,597		4,520		405		4,925	
Performance Measure (Renamed Measure)	Percentage of Counterterrorism Career Path Agents Completing Specialized CT Training	80%		92%		85%		--		85%	
Performance Measure (Discontinued Measure)	Percentage of CTD human sources validated	100%		12%		N/A		--		N/A	
Efficiency Measure (Renamed Measure)	Percentage of Counterterrorism Cases targeting Top Priority Groups	45%		45%		50%		--		50%	

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)											
Program Activity/ 1.4	**2. Counterintelligence**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		4,275	1,004,060	3,718	1,294,228	4,025	1,050,745	234	68,682	4,259	1,119,427
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)		3,252		5,786		4,500		500		5,000
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)			†		3,974		†		†		†
Performance Measure	Number of Priority Criminal Computer Intrusion Investigations Successfully Satisfied		31		24		33		2		35
Efficiency Measure	Cost savings from online Cyber training ($000)		567		809		596		29		625
Performance Measure	Computer Intrusion Program Convictions/Pre-trial diversions		††		142		††		††		††

PERFORMANCE/RESOURCES TABLE

Decision Unit: Counterterrorism/Counterintelligence

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

Data Definition, Validation, Verification, and Limitations:

- "Terrorist "acts," domestic or internationally-based, count separate incidents that involve the "unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives." (28 C.F.R. Section 0.85). For the purposes of this measure, the FBI defines a terrorist act as an attack against a single target (e.g., a building or physical structure, an aircraft, etc.). Acts against single targets are counted as separate acts, even if they are coordinated to have simultaneous impact. The FBI uses the term terrorist incident to describe the overall concerted terrorist attack. A terrorist incident may consist of multiple terrorist acts. For the purposes of these performance data, a catastrophic terrorist act is defined as an act resulting in significant loss of life and/or significant property damage (e.g., each of the individual attacks that took place on September 11, 2001, the attack on the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma on April 19, 1995)."
- Other Counterterrorism measures are provided through records kept by the FBI's Counterterrorism Program, including the Terrorist Screening Center. The count of JTTF participants erroneously did not include part-time participants until FY 2008, but will henceforth include them. No other known data limitations exist.
- Counterintelligence measures are based on records kept by the FBI's Counterintelligence Program. These records are based upon the results of field reviews of CI squads done on a periodic basis. Since the end of March 2007, all FBI field offices have undergone at least one CI field review. Percentages are updated based upon the most recent field review. IMIS cost savings data are based upon estimates of cost savings per student taking an online course, compared with an in-service training. During FY 2009, contracting delays will effect 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
		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
Performance Measure	Positive encounters with subjects through screening process	N/A	5,396	15,730	19,967	20,500	19,306	20,250	19,043	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	4,450	4,597	4,520	4,925
Performance Measure (Renamed Measure)	Percentage of Counterterrorism Career Path Agents Completing Specialized CT Training	3%	10%	15%	74%	77%	80%	80%	92%	85%	85%
Performance Measure (Discontinued Measure)	Percentage of CTD human sources validated ** Historical data for this measure have been revised – see Discussion.*	N/A	N/A	N/A	N/A	2%*	7%*	100%	12%	N/A	N/A
Efficiency Measure (Renamed Measure)	Percentage of Counterterrorism Cases targeting Top Priority Groups	15%	35%	34%	33%	34%	44%	45%	45%	50%	50%
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	3,252	5,786	4,500	5,000
Performance Measure	Number of Priority Criminal Computer Intrusion Investigations Successfully Satisfied	N/A	N/A	34	24	27	31	31	24	33	35
Efficiency Measure	Cost savings from online Cyber training ($000)	N/A	N/A	N/A	N/A	331	511	567	809	596	625
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*	N/A	142	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.

Measure changes for this performance report are proposed as a result of an internal review of the FBI's performance measures, pursuant to an initiative coordinated by DOJ's Performance Improvement Officer (PIO) Panel in Spring, 2009.

Counterterrorism

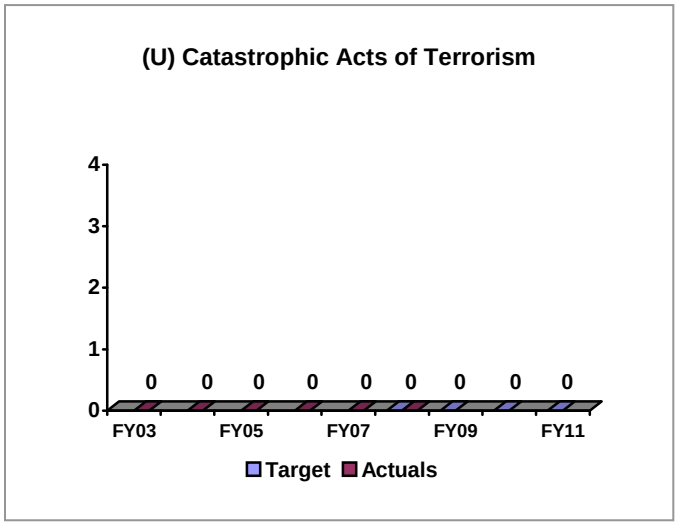
a. Performance Plan and Report for Outcomes

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. 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. Finally, to develop a comprehensive intelligence base, the FBI will employ 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.

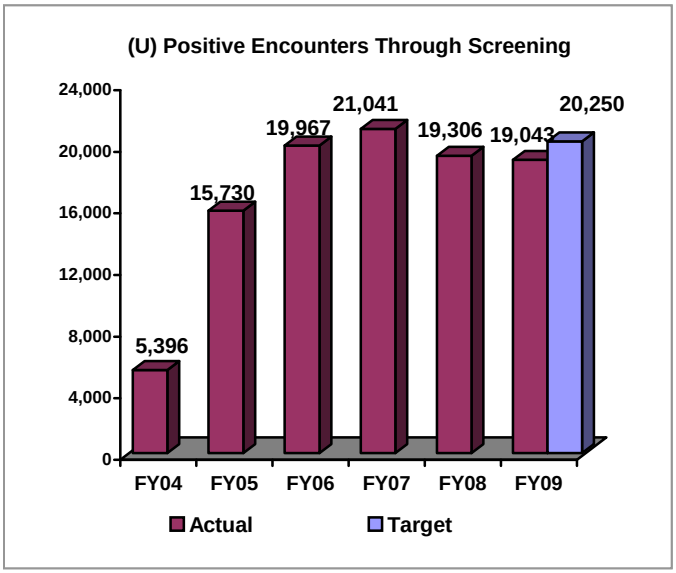
Performance Measure: REVISED MEASURE: Catastrophic acts of terrorism



FY 2009 Target: Zero terrorist acts.
FY 2009 Actual: Zero
Discussion:
This measure was revised to include both domestic and international terrorist acts, and replaces a similar measure reporting all acts of international terrorism committed by foreign nationals within U.S. borders, regardless of scope. For the purpose of this performance report, 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)." Using this determination, in FY 2009, there were no catastrophic acts of terrorism perpetrated on American soil.
FY 2010 Target: Zero terrorist acts.
FY 2011 Target: Zero terrorist acts.

Performance Measure: Positive encounters with subjects through screening process.

FY 2009 Projection: 20,250
FY 2009 Actual: 19,043



Discussion: Identifying terrorists and facilitating the prevention of their entry into the U.S. is the function of the Terrorist Screening Center (TSC), a joint Department of Justice venture with the Department of Homeland Security (DHS), the Department of State, the Department of Defense, and other stakeholders. The TSC was started in December 2003, and consolidates the U.S. Government's approach to screening for individual terrorists by creating a single comprehensive database of known or appropriately suspected terrorists. A positive encounter is one in which an encountered individual is positively matched with an identity in the Terrorist Screening Data Base (TSDB).

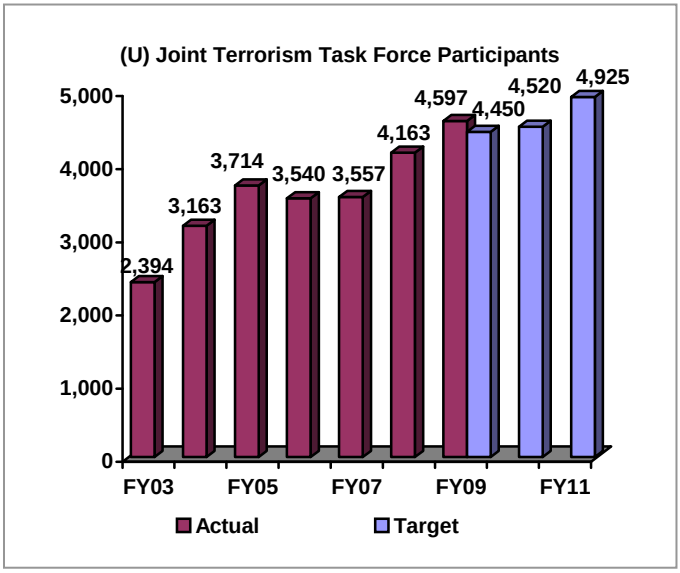
The TSC's FY 2009 actual data for positive encounters was 19,043, under the trend projection of 20,250 positive matches. There are no empirical data indicating a technological, policy or procedural issue with the actual data deviation from the trend projection. The TSC simply processes submissions resultant from encounters by law enforcement and screening agencies domestically and internationally. The more encounters by these entities increases the probability of more positive encounters.

Due to the trending issues with this particular measure, FBI will report this measure as a workload activity in the future, and not as a targetable performance measure.

FY 2010 Projection: N/A
FY 2011 Projection: N/A

Performance Measure: Number of participants in the Joint Terrorism Task Force.
FY 2009 Target: 4,450
FY 2009 Actual: 4,597

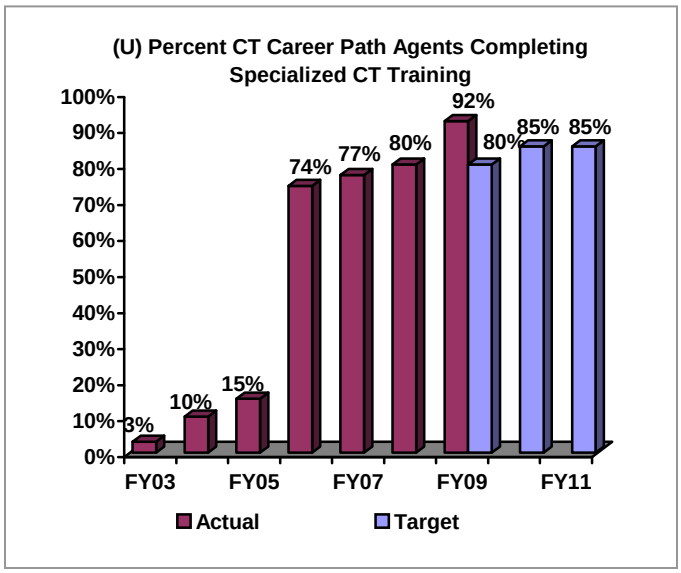
Discussion: The FBI's Joint Terrorism Task Force participants serve as the "operational arm" of the U.S. Government's domestic Counterterrorism strategy, and partner FBI personnel with hundreds of investigators from various federal, state, and local agencies in field offices across the country and are important force multipliers aiding our fight against terrorism.



The JTTF is focused on maximizing interagency cooperation and coordination by employing cohesive units of full and part-time Federal, state, and local officers that are capable of addressing a wide variety of terrorism matters. The JTTF has developed a synergistic structure designed to bring all available assets to bear in the War on Terrorism by focusing existing domestic and international law enforcement capabilities in concert with intelligence community assets.
During FY 2009, JTTF participation exceeded it target for number of full-time and part-time members by 147 resulting in a 3.3% increase over the target.

FY 2010 Target: 4,520
FY 2011 Target: 4,925

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 2009 Target: 80%
FY 2009 Actual: 92%

Discussion: In FY 2009, CTD developed the Counterterrorism Investigations and Operations course for CT agents after they reach Stage II of the CT career path. The CTIOPS course was designed to enhance the SA's awareness of the CT Program's policies, procedures and strategy for conducting counterterrorism investigations. All CT Special Agents are required to complete CT courses with a passing grade in Stage II and Stage III in the CT Career Path before being considered "CT proficient."

There are currently 4 stages in the CT Career Path. Director Mueller and Congress have mandated the FBI to provide additional CT training to FBI personnel. CTD has identified a need for additional CT courses to be developed and implemented for all CTD personnel. Once the courses have been developed they will be incorporated into the Special Agent Career Path Program and the CT proficiency levels will be revised once again.

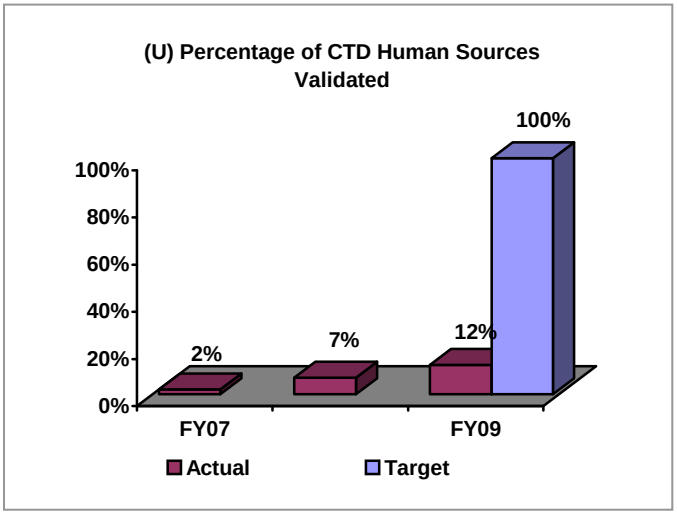
The CTD reports that 92% of CT Career Path agents budgeted to complete the CT Investigations and Operations (CTIOPS) course were certified by the end of FY 2009. This figure exceeds the established target. The CEPDU developed CTIOPS to replaced Stage II Academy; the first iteration of the course was rolled out in January 2009.

FY 2010 Target: 85%
FY 2011 Target: 85%

Performance Measure: DISCONTINUED MEASURE: Percentage of CTD human sources validated.
Note: Historical data for this measure have been revised.

FY 2009 Target: 100%
FY 2009 Actual: 12.4%

Discussion: Gathering intelligence from all sources to stop terrorism requires the FBI to ensure the validity, reliability, and productivity of all human sources. Source validation is a process which allows the FBI to measure value and manage risks associated with the operation of a confidential human source.



On December 13, 2006, the Attorney General issued new guidelines concerning use of confidential human sources (CHSs). These new guidelines require all CHSs go through an annual validation process. The FBI Human Source Validation program was initiated in 2006 with the goal of conducting a Validation Review of every CHS. This required the establishment of new Human Source Validation Policy, the training of new personnel, and the application of the validation process through new Delta program. Also, the source validation function was transferred at FBIHQ from operational program divisions to the authority of the Directorate of Intelligence (DI).

Over the past three years, the DI, Counterterrorism HUMINT Validation Unit (CT-HVU) had to respond to several changes in policy. The DI, CT-HVU originally reported this performance measure as a total percentage of sources validated compared to the new sources being submitted in Phase I of the new Human Source Validation program, and met those annual performance goals. However, this program is now taking the view that its progress should be tracked against its overall CT CHS backlog. Thus, because the previous FY 2009 target was established against a single-year influx of CHS's, the current data show a much smaller proportion of validations completed, even though the amount of activity has increased substantially.

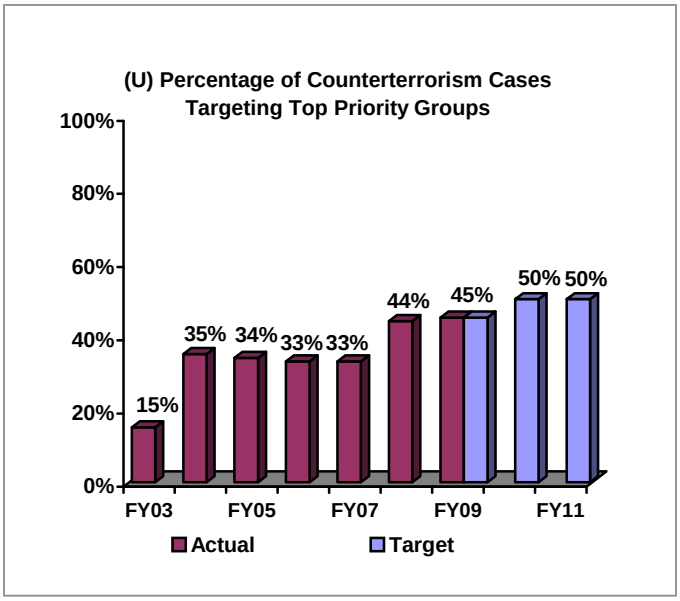
As the DI, CT-HVU developed the unit has completed a greater number of validation reviews. During FY2009, the unit more than doubled the productivity of the previous two years combined, in part due to the assistance of the new Delta system. The total volume of CT CHS's is 3,078; of this total, the DI, CT-HVU validated 542 sources in FY 2009, compared to 48 in FY 2007 and 164 in FY 2008. This trend is expected to continue into FY 2010 and FY 2011 until the CHS validation backlog has been eliminated. Nonetheless, since the DI now proposes that it track CHS validation on an FBI-wide level (see Intelligence Decision Unit performance measures), the FBI proposes that this measure be discontinued.

FY 2010 Target: N/A
FY 2011 Target: N/A

Efficiency Measure: RENAMED MEASURE: Percentage of Counterterrorism cases targeting Top Priority Groups *(formerly named "Percentage of human sources reporting on Tier 1 groups").*

FY 2009 Target: 45%
FY 2009 Actual: 45%

Discussion: In December 2002, the FBI's Counterterrorism Division (CTD) completed a comprehensive national assessment of the terrorist threat to the U.S. homeland based on comprehensive intelligence and priority groups were identified. The groups were prioritized by their intent to harm the US homeland, their links to al-Qa'ida, and their capabilities.



In 2009, the Counterterrorism Program met its target for the percentage of cases targeting top priority groups. Using a five-tiered ranking system, the FBI continues to focus it resources on issues, opportunities or threats that pose a clear and intermediate threat to the U.S. persons and interests. Additionally, the FBI continues to use best practices to uncover the identities of heretofore unknown terrorist organizations.

FY 2010 Target: 50%
FY 2011 Target: 50%

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 2011 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

During FY 2005, the Counterintelligence program underwent a review of its performance measurement in conjunction with a program review by OMB. The FBI has adopted several performance measures related to the review of field operations conducted by the Counterintelligence Program. As of March 31, 2007, all FBI field offices have gone through this review at least once. Data will be updated as field offices undergo reevaluations.

The CI Program conducts field office reviews to assist field offices in understanding their domain, identifying the gaps in their performance, and providing recommendations and guidance that specifically addresses an individual office's requirements.

Earlier in FY 2009, the FBI had contracting issues that affected its ability to schedule on-site Counterintelligence program reviews at FBI field offices with an independent contractor. These reviews are necessary for compiling various Counterintelligence performance measures. The contracting issues have been resolved at this time, and the reviews are now being conducted at their standard pace. The percentages reported here will include the ratings from some older on-site program reviews of field offices, combined with the newer reviews, until the full schedule can be completed.

Performance Measure: Percentage of field offices that have sufficiently identified Foreign Intelligence Service (FIS) activities

Refer to classified version.

Performance Measure: Percentage of field offices with adequate coverage of known or suspected intelligence officers

Refer to classified version.

Performance Measure: Percentage of field offices satisfactorily engaged in strategic partnerships with other U.S. Intelligence Community (USIC) entities

Refer to classified version.

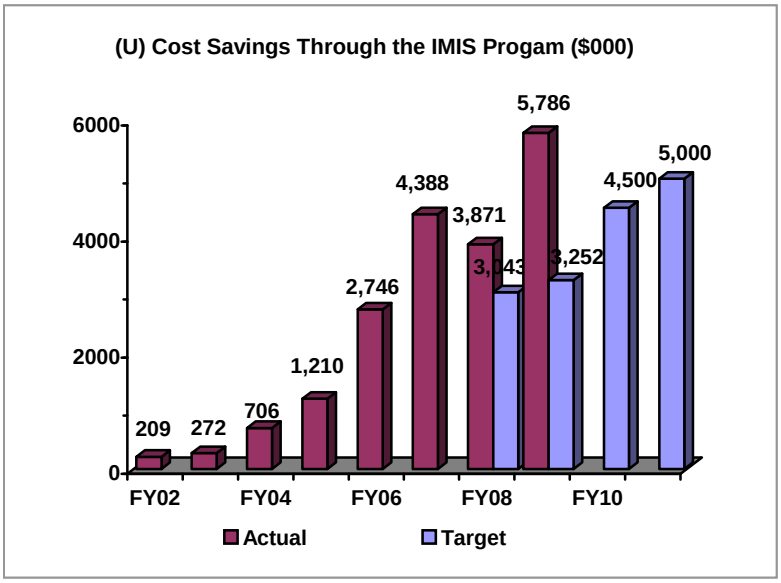
Performance Measure: Percentage of field offices that have satisfactorily demonstrated knowledge of and liaison with vulnerable entities within their domain

Refer to classified version.

Performance Measure: Percentage of field offices that have identified and documented priority threat country operations

Refer to classified version.

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



FY 2009 Target: 3,252
FY 2009 Actual: 5,786

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 2009, cost-saving for virtual or computer-based training enabled more employees to be trained, thereby providing an opportunity to improve performance across all program strategy measures. CD has exceeded the target because the target number did not originally reflect the fact that the IMIS courses would later be designated as mandatory for all new agent trainees.

FY 2010 Target: 4,500
FY 2011 Target: 5,000

b. Strategies to Accomplish Outcomes

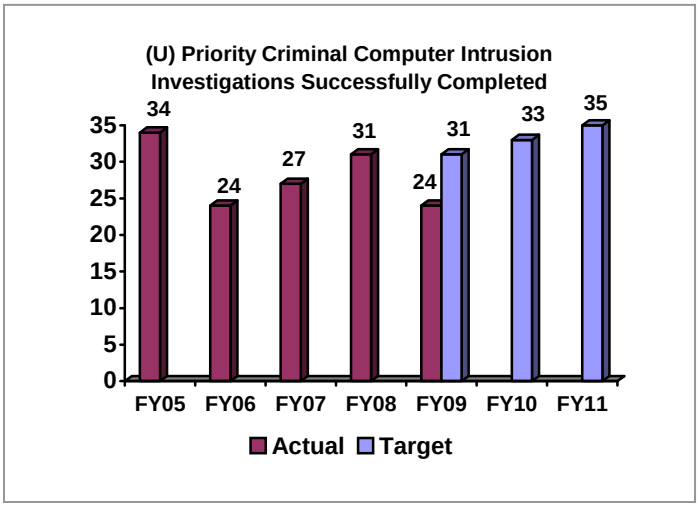
The FBI's Counterintelligence (CI) Program continues to execute a comprehensive National Strategy for CI. This strategy is predicated on the need for a centralized national direction that facilitates a focus on common priorities and specific objectives in all areas of the country. It also recognizes 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 has enabled the program to more effectively combat the intelligence threats facing the U.S. The FBI needs to maintain its resources that are currently directed against the CI symmetrical threat, while concurrently obtaining resource enhancements to deploy against the CI asymmetrical threat throughout the CI domain fieldwide.

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. New performance measures for computer intrusions were created in FY 2008.

Performance Measure: Number of Criminal Computer Intrusion Investigations Successfully Completed



FY 2009 Target: 31
FY 2009 Actual: 24

Discussion:
The FBI did not meet its target for this measure. The drop is partially attributable to a shifting paradigm in the neutralization of the cyber threat. Increasingly, cyber threat actors are attacking from abroad. Our international law enforcement partners are prosecuting in their own countries rather than extraditing 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

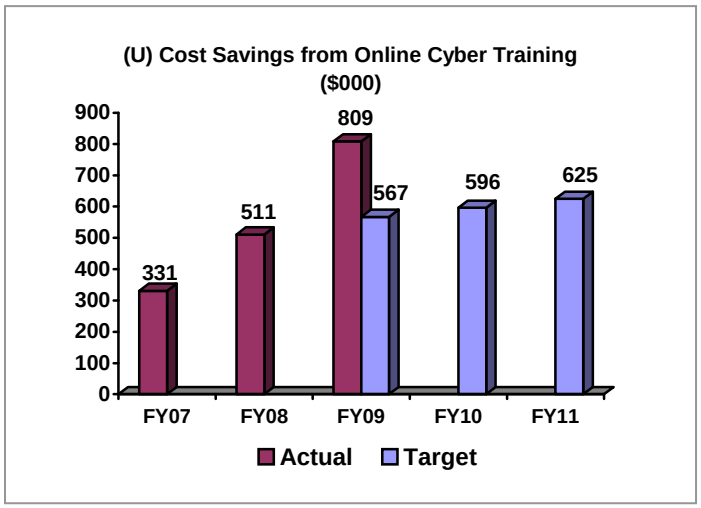
Method:
- Unauthorized access, exceeding authorized access, malicious code, denial of service, botnets, phishing, illegal wiretap, social engineering, physical access, network recon.

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.

FY 2010 Target: 33
FY 2011 Target: 35

Efficiency Measure: Cost Savings from Online Cyber Training

FY 2009 Target: $567,189
FY 2009 Actual: $808,867



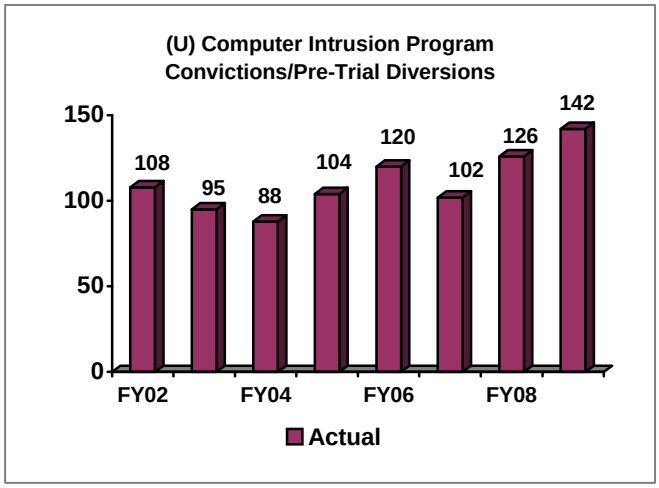
Discussion:
The FBI's Cyber Program is progressing towards providing training for conducting cyber investigations via online training courses. The student population for the majority of these classes is quite broad, including FBI Special Agents, support employees and state and local law enforcement or 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 2010 Target: $595,548
FY 2011 Target: $625,326

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

FY 2009 Target: In accordance with Department guidance, targeted levels of performance are not projected for this indicator.
FY 2009 Actual: 142
* Actual number of convictions and pre-trial diversions were revised to reflect criminal computer intrusion cases only.



Discussion: Computer intrusion convictions are expected to rise as a result of increased investigations and level of agent expertise.

FY 2010 Target: N/A
FY 2011 Target: N/A

b. Strategies to Accomplish Outcomes

In FY 2011, 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.

C. Criminal Enterprises and Federal Crimes Decision Unit

CRIMINAL ENTERPRISES AND FEDERAL CRIMES DECISION UNIT TOTAL	Perm. Pos.	FTE	Amount ($000)
2009 Enacted with Rescissions	10,850	10,596	$2,275,754
2009 Supplementals	…	…	35,473
2009 Enacted w/ Rescissions and Supplementals	10,850	10,596	2,311,227
2010 Enacted	11,484	11,090	2,471,964
Adjustments to Base and Technical Adjustments	10	270	89,253
2011 Current Services	11,494	11,360	2,561,217
2011 Program Increases	406	307	86,813
2011 Program Offsets	…	…	(6,122)
2011 Request	11,900	11,667	2,641,908
Total Change 2010-2011	**416**	**577**	**$169,944**

Criminal Enterprises and Federal Crimes Decision Unit – Information Technology Breakout	Perm. Pos.	FTE	Amount* ($000)
2009 Enacted with Rescissions	301	301	$283,816
2009 Supplementals	…	…	…
2009 Enacted w/Rescissions and Supplementals	301	301	283,816
2010 Enacted	660	660	666,212
Adjustments to Base and Technical Adjustments	7	7	(57,655)
2011 Current Services	667	667	608,557
2011 Program Increases	…	…	6,301
2011 Request	667	667	614,858
Total Change 2010-2011	**7**	**7**	**($51,354)**

*Includes both direct and reimbursable funding

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, such as 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.

Public Corruption/Civil Rights

The Public Corruption and Government Fraud programs involve sensitive and complex cases where the FBI is the only law enforcement agency primarily charged with investigating legislative, executive, judicial, and significant law enforcement corruption. The FBI is the only law enforcement agency that targets federal campaign finance violations and ballot fraud, most obstruction of justice violations, and Foreign Corruption Practices Act (FPCA) violations.

Criminal Enterprises

Through the Organized Crime and the Gang/Criminal Enterprise programs the FBI seeks to dismantle criminal organizations by employing the enterprise theory of investigation to identify, investigate, and prosecute members of the groups. Within these programs, the FBI's investigative mission is to disrupt and dismantle the local, regional, national, and transnational criminal enterprises that pose the greatest threats to the economic and national security of the United States.

The FBI's Violent Gang and Major Theft programs have combined efforts to increase the number of investigations and cases, sharing equitable intelligence resources in similar areas of interest and providing leadership to state and local law enforcement agencies.

To challenge the growing narcotics industry, often controlled by violent gang elements, the FBI provides resources to major Department of Justice (DOJ) initiatives such as the Organized Crime Drug Enforcement Task Force (OCDETF) program and the High Intensity Drug Trafficking Area (HIDTA) initiative. Both programs work closely with other federal law enforcement agencies in addition to state and local government authorities.

The FBI has developed a comprehensive counter-drug strategy 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 52 international organizations identified on DOJ's Consolidated Priority Organizational Targets (CPOT) list. These organizations are associated primarily with the Colombian, Mexican, and Caribbean drug trafficking organizations that have the most adverse impact on United States national interests.

The FBI will maintain focus on organized criminal enterprise groups, including the Eurasian criminal enterprises; Asian criminal enterprises; La Cosa Nostra/Italian organized crime groups; Balkan/Albanian organized crime groups; Middle Eastern criminal enterprises; and African criminal enterprises. These organized criminal enterprise groups are engaged in a myriad of criminal activities including racketeering activity, extortion, murder, money laundering, prostitution, human trafficking, alien smuggling, and drug trafficking.

Violent Crime
Through the Violent Crime Program, the FBI investigates a wide range of federal criminal violations, including crimes against children; crimes on federal reservations/property (including Indian reservations); assaults against public officials; unlawful flight to avoid prosecution; and manufacturing and distribution of child pornography.

In addition to responding to reports of individual crimes, the FBI participates in groups that employ proactive investigative techniques, such as joint agency violent crime Safe Streets Task Forces; wire intercepts; the Indian Gaming Working Group; and undercover operations. The current major areas of focus for the Violent Crime Program are crimes against children and child abductions.

Financial Crime
Through the Financial Crime Program, the FBI investigates a myriad of financial crimes including health care fraud, public corruption, financial institution fraud, insurance fraud, securities and commodities fraud, telemarketing fraud, bankruptcy fraud, money laundering, and intellectual property rights violations. In addition, the program facilitates the forfeiture of assets from those engaging in federal crimes.

In the United States, citizens and businesses lose billions of dollars each year to criminals engaged in non-violent fraudulent enterprises. The globalization of economic and financial systems, advancement of technology, decline of corporate and individual ethics, and sophistication of criminal organizations have resulted in annual increases in the number of illegal acts characterized by deceit, concealment, or violations of trust. The loss incurred as a result of these crimes is not merely monetary. These crimes also contribute to a loss of confidence and trust in financial institutions, public institutions, and industry.

The scope and impact of these financial crimes has become more evident with the economic downturn that began in 2007. The economic downturn revealed significant criminal activity in regards to the sub-prime mortgage industry with mortgage fraud Suspicious Activity Reports (SAR) expanding to 67,190 at the end of FY2009 from 35,617 in FY 2006. The number of sub-prime related corporate fraud investigations has also grown from 28 in October of 2008 to 45 in December of 2009. With the economic downturn, high yield investment schemes and Ponzi schemes have been exposed and fraud cases involving the tens of billions of dollars are now being investigated. These three major areas of financial crimes have resulted in losses measured in the hundreds of billions of dollars.

The FBI also recognizes the risks of fraud and abuse associated with the various Federal economic recovery programs. The Troubled Asset Relief Program (TARP) and the Termed Asset-Backed Securities Loan Facility (TALF) each pose risks of corporate fraud and malfeasance requiring additional attention by law enforcement and regulators.

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 United States 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

- 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.
- Infiltrate, disrupt and dismantle violent gang activities by targeting groups of gangs using sensitive investigative and intelligence techniques to initiate long term proactive investigations.
- Reduce the economic loss associated with the theft of United States intellectual property by criminals.
- Reduce the incidence of public corruption within targeted sectors of local, state, and federal government.
- Deter civil rights violations through aggressive investigation of those crimes wherein the motivation appears to have been based on race, 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.
- Identify, investigate, disrupt, and dismantle major criminal enterprises, including violent gangs.
- Continue to support the Southwest Border Initiative, which focuses the FBI's efforts on the most significant criminal enterprises operating along the southwest border.
- Reduce the amount of economic loss and market instability resulting from corporate fraud committed by both individuals and enterprises.
- Minimize the economic loss due to mortgage fraud by identifying, investigating, and disrupting fraudulent activity.
- Minimize the amount of economic associated with fraud related to Federal economic recovery programs.
- 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 reported economic loss due to fraud and abuse in federally funded procurement, contracts, Electronic Benefits Transfer, and entitlement programs.
- 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 United States economic loss due to national and international telemarketing fraud and Internet fraud.
- Reduce the amount of economic loss caused by fraudulent bankruptcy filings throughout the United States.
- Provide timely and coordinated responses to violent and serious crimes in connection with the FBI's investigative mandate in Indian Country and strengthen the capabilities of Indian Country law enforcement investigators through training programs and investigative assistance.

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 2009		FY 2009		2010 Enacted		Current Services Adjustments & FY2011 Program Changes		FY 2011 Request	
Workload -- # of cases investigated (pending and received)		†		90,824		†		†		†	
Total Costs and FTE		FTE	$000	FTE	$000	FTE	$000	FTE	$000	FTE	$000
		10,596	2,311,227	10,076	2,698,140	11,090	2,471,964	567	166,035	11,667	2,641,908
TYPE/ STRATEGIC OBJECTIVE	**PERFORMANCE**	FY 2009		FY 2009		2010 Enacted		Current Services Adjustments & FY2011 Program Change		FY 2011 Request	
Program Activity/ 2.3, 2.5	**1. White-Collar Crime/Cybercrime**	FTE	$000	FTE	$000	FTE	$000	FTE	$000	FTE	$000
		4,874	1,073,664	5,333	1,292,919	5,539	1,225,060	447	123,236	5,996	1,352,205
Workload -- # of cases investigated (pending and received)		†		35,594		†		†		†	
Performance Measure	Restitutions & Recoveries / Fines ($000) • Intellectual Property Rights Violations • Public Corruption • White-Collar Crimes (all other)	††		5,389 / 3,346 220,787 / 887,672 15,956,528 / 1,134,306		††		††		††	
Performance Measure	Convictions/Pre-Trial Diversions (total) • Intellectual Property Rights Violations • Public Corruption • White-Collar Crimes (all other)	††		88 981 2,910		††		††		††	
Performance Measure	Number of Criminal Enterprises Engaging in White-Collar Crimes Dismantled	160		250		160		40		200	
Performance Measure (Discontinued Measure)	Number of Major Corporate Fraud Cases Successfully Investigated	55		N/A		N/A		--		N/A	
Efficiency Measure	% of Major Mortgage Fraud Investigations to all pending	65%		66%		67%		1%		68%	

TYPE/ STRATEGIC OBJECTIVE	PERFORMANCE	FY 2009		FY 2009		2010 Enacted		Current Services Adjustments & FY2011 Program Change		FY 2011 Request	
Performance Measure (Renamed Measure)	Number of Children Depicted in Child Pornography Identified by the FBI	150		118		130		10		140	
Performance Measure	Number of high-impact Internet fraud targets neutralized	12		13		13		--		13	
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**
		5,722	1,237,563	4,743	1,405,221	5,551	1,246,904	120	42,799	5,671	1,289,703
Workload -- # of cases investigated (pending and received)		†		55,230		†		†		†	
Performance Measure	Convictions/Pre-trial Diversions • Organized Criminal Enterprises • Gangs/Criminal Enterprises • Crimes Against Children • Civil Rights	††		395 2,136 270 222		††		††		††	
Efficiency Measure	% of FBI OCDETF Investigations with links to CPOT-linked DTOs	12%		14%		12%		--		12%	
Performance Measure	CPOT-Linked DTOs • Disruptions • Dismantlements	30 15		35 20		30 15		-- --		30 15	
Performance Measure	Number of Organized Criminal Enterprise Dismantlements	36		43		36		1		37	
Performance Measure	Number of Gangs/Criminal Enterprises Dismantlements*	99		135		99		--		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	FY 2011
		Actual	Actual	Actual	Actual	Actual	Actual	Target	Actual	Target	Target
Performance Measure	Restitutions & Recoveries ($000)										
	• Intellectual Property Fraud	205,120	115,967	432,316	111,877	238,832	260,219	N/A	5,389	N/A	N/A
	• Public Corruption	1,631,692	101,647	1,116,266	321,815	157,440	676,889	N/A	220,787	N/A	N/A
	• White-Collar Crimes (all other)	8,433,421	7,881,151	13,056,937	7,799,218	19,516,406	18,502,635	N/A	15,956,528	N/A	N/A
Performance Measure	Fines ($000)										
	• Intellectual Property Fraud	1,053	208	538	1,005	6,587	320	N/A	3,346	N/A	N/A
	• Public Corruption	3,293	22,657	25,500	29,542	73,710	37,136	N/A	887,672	N/A	N/A
	• White-Collar Crimes (all other)	362,396	532,496	757,113	1,363,711	1,252,963	2,114,424	N/A	1,134,306	N/A	N/A
Performance Measure	Convictions/Pre-Trial Diversions (total)										
	• Intellectual Property Fraud	110	116	121	194	136	116	N/A	88	N/A	N/A
	• Public Corruption	579	661	812	929	943	987	N/A	981	N/A	N/A
	• White-Collar Crimes (all other)	5,022	4,368	3,976	3,707	3,347	3,834	N/A	2,910	N/A	N/A
Performance Measure	Number of Criminal Enterprises Engaging in White-Collar Crimes Dismantled	73	137	163	231	277	211	160	250	160	200
Performance Measure (Discontinued Measure	Number of Major Corporate Fraud Cases Successfully Investigated	58	46	35	45	64	57	55	N/A	N/A	N/A
Efficiency Measure	% of Major Mortgage Fraud Investigations to all pending	N/A	N/A	N/A	N/A	56%	63%	65%	66%	67%	68%
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	150	118	130	140
Performance Measure	Number of high-impact Internet fraud targets neutralized	5	7	10	9	11	11	12	13	13	13
Performance Measure	Convictions/Pre-Trial Diversions:										
	• Organized Criminal Enterprises	824	572	897	674	693	595	N/A	395	N/A	N/A
	• Gangs/Criminal Enterprises	4,089	2,923	4,292	2,070	2,218	2,242	N/A	2,136	N/A	N/A
	• Crimes Against Children	154	145	164	170	207	246	N/A	270	N/A	N/A
	• Civil Rights	163	155	139	195	207	208	N/A	222	N/A	N/A
Efficiency Measure	% of FBI OCDETF Investigations with links to CPOT-linked DTOs	N/A	N/A	11%	13%	14%	15.47%	12%	14%	12%	12%
Performance Measure	CPOT-Linked DTOs										
	• Disruptions	41	27	25	36	45	50	30	35	30	30
	• Dismantlements	15	12	18	17	15	18	15	20	15	15
Performance Measure	Number of Organized Criminal Enterprise Dismantlements	17	29	34	36	43	38	36	43	36	37
Performance Measure	Number of Gangs/Criminal Enterprise Dismantlements	138	112	138	119	144	114	99	135	99	99

2. Performance, Resources, and Strategies

The Criminal Enterprises/Federal Crimes decision unit contributes to the Department's Strategic Goal 2: Prevent Crime, Enforce Federal Laws, and Represent the Rights and Interests of the American People, Objectives 2.2-2.6. This decision unit also ties directly to six FBI priorities: 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; and Priority 8 – Combat significant violent crime.

Measure changes for this performance report are proposed as a result of an internal review of the FBI's performance measures, pursuant to an initiative coordinated by DOJ's Performance Improvement Officer (PIO) Panel in Spring, 2009.

Organized Criminal Enterprises & Gangs/Criminal Enterprises

a. Performance Plan and Report for Outcomes

In FY 2004 and the first three quarters of FY 2005, the Criminal Investigative Division (CID) at FBI Headquarters reorganized several of its programs. Future performance data will be reported to reflect the realigned focus of the FBI towards these types of criminal enterprises. In May 2006, CID changed the name of the Transnational Criminal Enterprises Program back to its original name, the Organized Crime Program, and the Americas Criminal Enterprises Program to the Gangs/Criminal Enterprise Program.

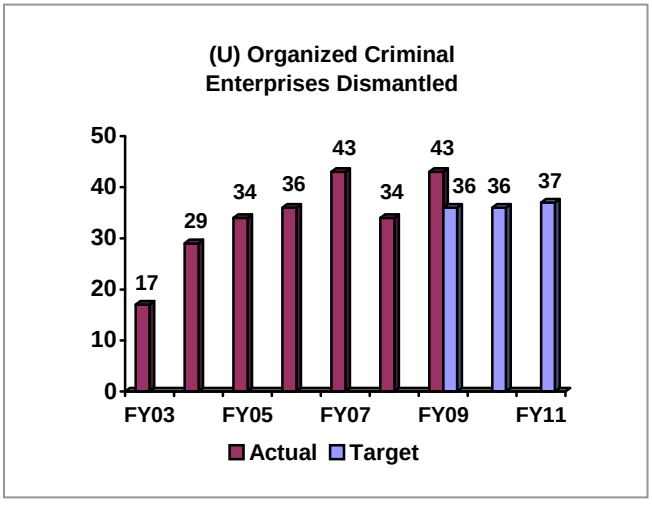
Organized Criminal Enterprises

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 La Cosa Nostra and Italian organized crime groups, Russian/Eastern European/Eurasian organized crime groups, Balkan/Albanian Organized crime groups, Middle Eastern criminal enterprises, Asian criminal enterprises and Nigerian/West African criminal enterprises. Each of these groups is engaged in a myriad of criminal activities.

Performance Measure: Organized Criminal Enterprises Dismantled

FY 2009 Target: 36
FY 2009 Actual: 43

Discussion:
The FBI's Organized Crime program surpassed its target for this measure.



Notable case accomplishments for FY 2009 are described below:

- The FBI's Detroit office investigated a Lebanese criminal enterprise that engaged in producing false identification documents, mortgage fraud, identity theft, and money laundering. The ring leader, Alaa Koubayssi, was arrested and subsequently cooperated which led to the discovery of a wider-scale identity theft and mortgage fraud ring, responsible for over millions of dollars in fraud. To date, there have been six federal indictments; three Federal complaints and three Federal informations; five Federal convictions (one of the defendants, Somail Aoun, is a fugitive believed to be hiding in Lebanon), $1,000,000 in federal restitution and two asset forfeitures. This investigation also led directly to the opening of an identity theft and mortgage fraud investigation into a second Lebanese criminal enterprise that is operating in the Dearborn, Michigan area.
- The Kansas City Division of the FBI, along with the Bureau of Immigration and Customs Enforcement (ICE), the Department of Labor's Office of the Inspector General, the Internal Revenue Service's Criminal Investigative Division (IRS-CID), and the Kansas Department of Revenue obtained a 45 count RICO Indictment against 12 individuals and three corporations. The charges include forced labor trafficking, fraud in foreign labor contracting, aggravated identity theft, marriage fraud, visa fraud, money laundering, mail fraud, wire fraud, and extortion. The indictment included a $6 million forfeiture count. This three-year joint investigation targeted both Uzbekistan foreign nationals and U.S. citizens associated with Giant Labor Solutions and their affiliated corporations. The organization recruited primarily Uzbekistani and other Eastern European workers to pay fees for the opportunity to obtain high-paying jobs in the United States. Upon arrival in the United States, workers were forced into low-paying jobs and charged exorbitant fees for substandard housing, food, and transportation. Occasionally, the use of force or threat of force was utilized to keep workers from contacting and cooperating with law enforcement officials. To date, more than one hundred victim/workers have been recovered and placed into the care of the victim witness program.

FY 2010 Target: 36
FY 2011 Target: 37

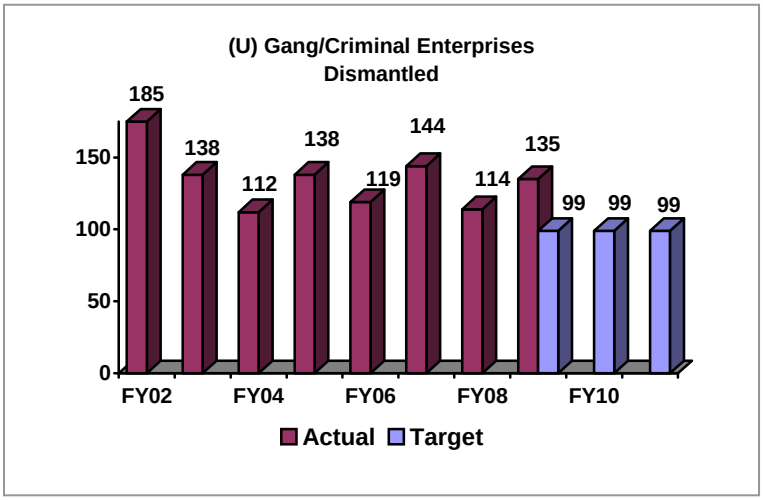
Gang/Criminal Enterprises

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, some of whom have ties to North, Central, and South America that pose the greatest threats to the economic and national security of the U.S. 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 FBI has concentrated anti-gang efforts in four arenas; neighborhood based gangs, prison gangs, Mara Salvatrucha (MS-13) National Gang Task Force, and outlaw motorcycle gangs, which supports, coordinates, and facilitates the development of local, state, federal, and international investigations.

The National Gang Intelligence Center (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 information 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. It facilitates operations across agency lines and promotes the complete dismantlement of 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 2009 Target: 99
FY 2009 Actual: 135

Discussion:
The FBI has exceeded its target for this measure. The FBI has identified the following recent trends in its investigations of local and national gangs:

- Conversion of neighborhood-based gang members to national gangs after serving prison sentence.
- Use of codes and cryptology.
- Use of Internet (e.g., MySpace, instant messaging, online chat) and other communication techniques (VOIP, texting).
- Migration from larger cities to smaller communities.
- Ties between Hispanic gangs and International Drug Trafficking Organizations.

Among its notable accomplishments during FY 2009, the FBI established eight new Safe Streets Task Forces across the country. In the Columbia Division, the Dark Knight investigation began by targeting the Folk Nation and other local gangs in the Columbia area. It progressed into Title III coverage that advanced up the chain from four wire intercepts to a total of 27 separate lines intercepted, beginning in September 2008 and ending in March 2009. There have been 51 Title III court orders in the case. Columbia identified over 150 gang members and gang related subjects through these sophisticated techniques and indicted 112 of those subjects on 07/12/2009. The Columbia Division moved up the chain of suppliers and intercepted Spanish language lines that identified the hierarchy of the Mexican-based suppliers. The investigation was linked through wire intercepts and SOD analysis to several CPOTs including the Gulf Cartel Trio, El Mayo and the Sinaloa Cartel. The Mexican supplier section of the case was indicted in April 2009. There were 19 indictments and 16 arrests of the suppliers. To date, there have been 86 gang arrests, numerous disruptions and $588,000 in seizures in this case.

FY 2010 Target: 99
FY 2011 Target: 99

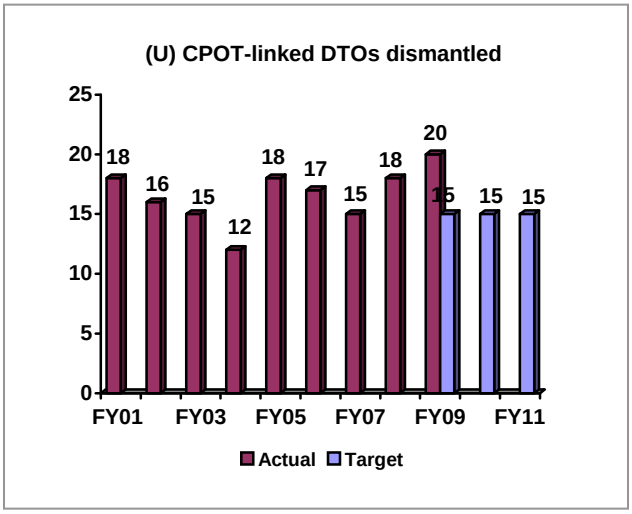
Gang/Criminal Enterprises - Consolidated Priority Organization Targets (CPOT)

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, provided assistance to other law enforcement agencies, and strengthen international cooperation. The strategy focuses the FBI's counter-drug resources on 59 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: CPOT-linked Drug Trafficking Organizations (DTOs) dismantled

FY 2009 Target: 15
FY 2009 Actual: 20



Discussion:
The FBI has exceeded its targets for both measures regarding OCDETF investigations of CPOT-related targets. The FBI's leading OCDETF initiative is known as "Operation Panama Express," which concentrates on maritime drug transportation. The FBI's effectiveness is largely attributable to its partnership in this initiative with the DEA, Immigration and Customs Enforcement (ICE), the United States Coast Guard and the Joint Interagency Task Force-South, which is comprised of both law enforcement and Department of Defense counterparts.

During FY 2009, Operation Panama Express (both North and South components) conducted over 50 successful interdiction operations in the Eastern Pacific Ocean and Caribbean. These efforts resulted in the loss of approximately 120 tons of cocaine that were seized, scuttled at sea, or turned over to foreign governments. During those interdiction events, 211 suspect subjects were detained at sea. Of that number, 119 were brought to the U.S. for prosecution while the remaining 92 were turned over to foreign governments. These "at sea" interdiction efforts, when combined with the much

enhanced second tier prosecution emphasis, resulted in 136 indictments, 132 arrests, 143 convictions and 122 sentencing's. The afore-mentioned emphasis on second tier strategic targeting led to a significant increase in second tier subject prosecutions and led to multiple disruptions and dismantlements, including that of the Daniel Segura-Rodriguez DTO.

Other initiatives implemented by the Strike Force during FY 2009 include the successful use by prosecutors of the newly implemented "Drug Trafficking Vessel Interdiction Act" and the advancement of CPOT and RPOT designations for numerous DTO members. The amount of cocaine seized in this investigation has increased steadily over time and the operation has also produced numerous second and third-tier indictments due to the cooperation obtained from many of the defendants. The stellar results of Operation Panama Express have had a direct impact on criminal organizations who distribute cocaine in the U. S. Intelligence reporting indicates that there has been a definite disruption to cocaine availability in many U.S. drug markets, resulting in higher prices for cocaine.

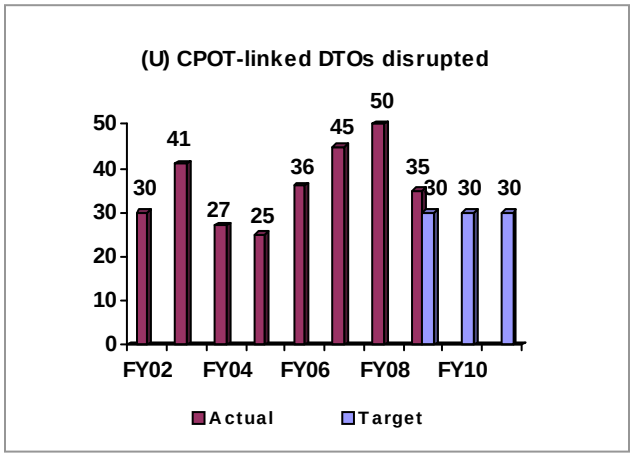
FY 2010 Target: 15
FY 2011 Target: 15

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

FY 2009 Target: 30
FY 2009 Actual: 35

Discussion:
See the measure related to CPOT dismantlements, above, for a discussion of the impact of budget changes upon this measure.

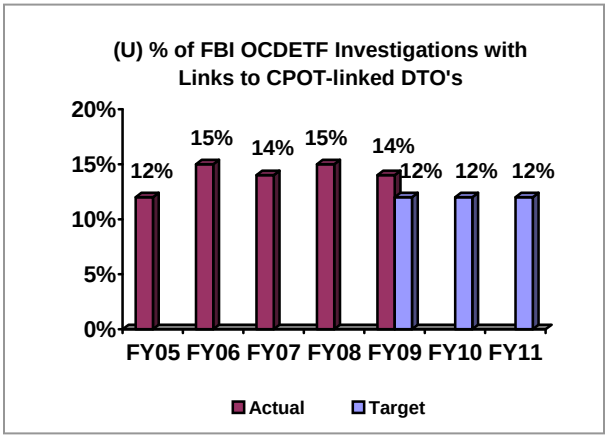
FY 2010 Target: 30
FY 2011 Target: 30



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

FY 2009 Target: 12%
FY 2009 Actual: 14%

Discussion: The FBI has exceeded its targeted proportion of CPOT investigations. The FBI, in conjunction with the Drug Enforcement Administration (DEA) and the Executive Office of Organized Crime Drug Enforcement Task Forces (OCDETF) strives to increase the



proportion of investigations that are linked to CPOT targets. Reclassification of organizations listed on the CPOT list can potentially have an impact on the accomplishments reported. The CPOT Working Group diligently reviews proposals from the OCDETF member agencies for additions to and deletions from the CPOT list.

FY 2010 Target: 12%
FY 2011 Target: 12%

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 158 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, a primarily El Salvadorian gang, 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 GangTECC, a multi-agency initiative anti-gang enforcement, deconfliction, coordination and targeting center headed by an experienced DOJ criminal division prosecutor 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.

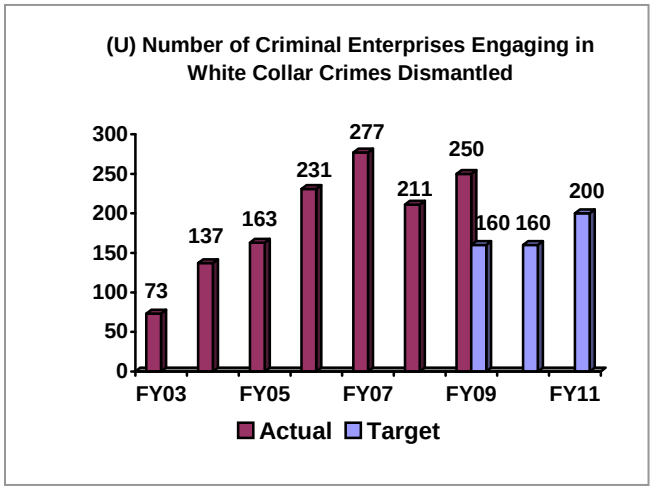
White-Collar Crime

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 2009 Target: 160
FY 2009 Actual: 250



Discussion:
The FBI surpassed its target for this measure in FY 2009. Following are examples of notable cases resolved during this time period:

- On August 10, 2009, a federal jury convicted a prominent Beverly Hills real estate agent, Kyle Grasso, and a licensed real estate appraiser, Lila Rizk, on federal charges resulting from an FBI investigation for their roles in a massive mortgage fraud scheme that caused more than $40 million in losses to federally insured banks. The intended loss was calculated at $242 million, but was mitigated by recoveries after the sale of approximately 80 properties that were funded by bogus loans. The evidence presented at trial showed that a group of real estate professionals obtained inflated mortgage loans on homes in some of California's most expensive neighborhoods. Members of the conspiracy sent false documentation, including bogus purchase contracts and appraisals, to the victim banks to deceive them into unwittingly funding mortgage loans that were hundreds of thousands of dollars higher than the homes actually cost. Eight other real estate professionals who were part of the scheme had previously pleaded guilty to federal felony charges for their roles, including Charles Elliott Fitzgerald and Mark Abrams, both real estate developers who masterminded the fraudulent scheme.

- On March 27, 2009, Lance Poulsen, former co-owner and CEO of National Century Financial Enterprises (NCFE), and Rebecca Parrett, former co-owner of NCFE, were sentenced for their roles in perpetrating a $2.34 billion investment scheme where they were charged with securities fraud, mail fraud, wire fraud, money laundering, and conspiracy. The investigation of this crime was led by the

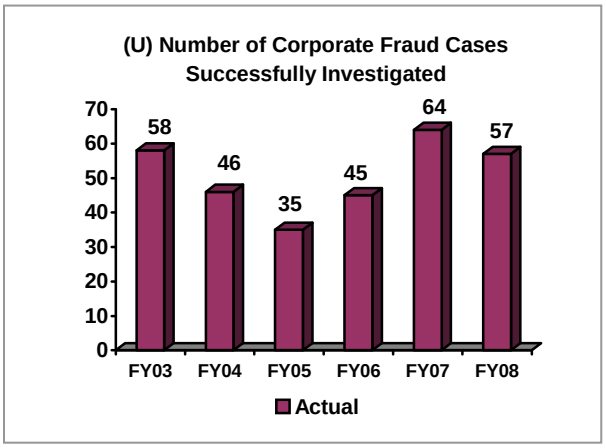
FBI's Cincinnati office. Poulsen and Parrett were convicted for lying to investors about how their funds would be used, diverting the funds, and then hiding the shortfall by shuffling the money between subsidiaries' bank accounts. NCFE operated as a financial service holding company organized to buy accounts receivables from health care providers. As a result, this fraud scheme led to bankruptcies of numerous health care providers. Although Parrett fled following her conviction and her current whereabouts are unknown, her sentencing will proceed.

As part of a related FBI investigation, Karl Demmler was also sentenced on March 27, 2009 for charges of witness tampering and obstruction of justice for his role in conspiring with Poulsen to influence the testimony of a former NCFE executive and witness. Demmler, on behalf of Poulsen, approached a previously convicted subject in this case and offered to pay her money to alter or restrict her testimony against Poulsen.

In light of the growing crime problems associated with White-Collar Crimes, to include an exponential rise in the number of Mortgage and Corporate Fraud investigations, the FBI's has submitted a budget enhancement request for FY 2011. The current FBI personnel level is insufficient to address the burgeoning crime problem as the average case inventory of complex, time-intensive investigations per Agent rapidly increases. In addition, as the mortgage market and Wall Street firms are examined with additional scrutiny from regulators and independent accountants, it is believed further corporate malfeasance will come to light. The number of investigations, and corresponding accomplishments, will increase, provided the resources are available.

FY 2010 Target: 160
FY 2011 Target: 200

Performance Measure: DISCONTINUED MEASURE: Number of Major Corporate Fraud Cases Successfully Investigated.



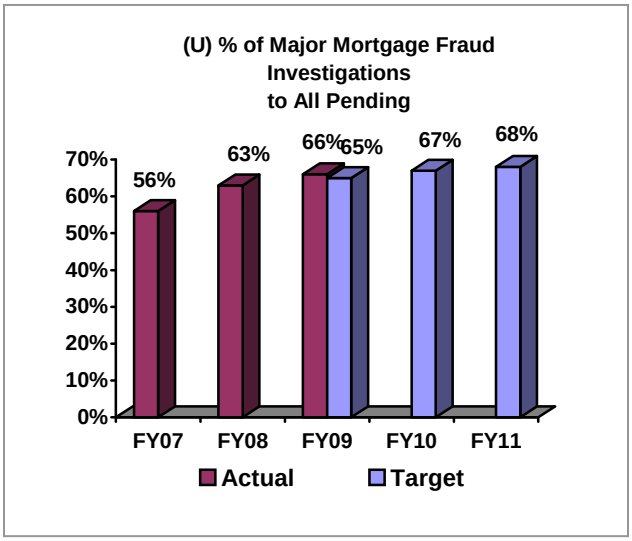
FY 2009 Target: 55
FY 2009 Actual: N/A

Discussion:
While the FBI continues to track the overall progress of its Corporate Fraud investigations, the Financial Crimes Section no longer tracks this measure for internal management purposes, and wishes to discontinue its use.

FY 2010 Target: N/A
FY 2011 Target: N/A

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

FY 2009 Target: 65%
FY 2009 Actual: 66%



Discussion: This measure met its FY 2009 target. The FBI's White-Collar Crime program modified this efficiency measure to concentrate specifically on a subclass of Financial Institution Fraud (FIF), mortgage fraud. Since the spring of 2007, the mortgage industry in the United States has been experiencing severe problems, with late payment defaults and foreclosures significantly increasing. For several months, this has threatened the stability of the economic markets. In some regions of the country, foreclosures have increased over five times what they were in the previous year. Government and industry sources agree, mortgage fraud is a significant crime problem and a major contributing factor in the amount of foreclosures and bad loans involved in the ongoing housing crisis. This measure tracks the proportion of all "major" mortgage fraud investigations (i.e.., those with the highest level of dollar loss tracked by the FBI) to the total pending mortgage fraud caseload.

Mortgage fraud investigations are overwhelming many FBI field offices. While the requested White-Collar Crime enhancements will affect the level of accomplishments measured for mortgage fraud investigations, the FBI still expects the proportion of its caseload dedicated to the highest category of economic loss to remain constant.

FY 2010 Target: 67%
FY 2011 Target: 68%

b. Strategies to Accomplish Outcomes

In FY 2011, the FBI will continue to pursue mortgage fraud and other types of financial institution fraud, health care fraud, money laundering, insurance fraud, and securities/commodities 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.

Cyber Crime

a. Performance Plan and Report for Outcomes

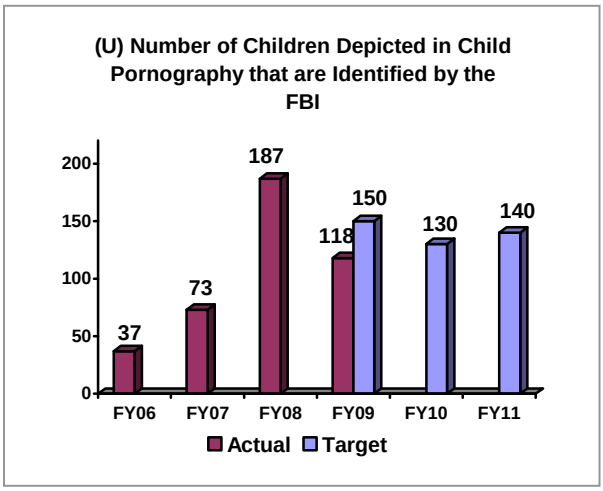
The changing economy and the emergence of Internet technology have created an unprecedented flow, exchange, and production of data. They have also created new arenas and techniques for criminal transactions. Three priority areas of concern with the new vulnerabilities in the era of the Internet's emergence are the online exploitation of children, computer facilitated theft of intellectual property, and Internet fraud. In June 2002, Director Mueller approved the organizational structure of the new Cyber Division. The Cyber Division addresses cyber threats in a coordinated manner, allowing the FBI to stay technologically one step ahead of the cyber adversaries threatening the U.S.

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 on 04/30/2003 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: RENAMED MEASURE: Number of children depicted in child pornography that are identified by the FBI (formerly "Number of children depicted in child pornography that are *rescued* by the FBI")
Note: FY 2006 data in chart are incomplete: data were only collected for part of that year.



FY 2009 Target: 150
FY 2009 Actual: 118

Discussion:
This measure is being renamed to indicate that the data record all children identified through FBI

investigations of child pornography, as well as through partnerships with organizations such as its work with NCMEC.

FBI has not met its target for this measure. While the FBI always makes every effort to identify/rescue victimized children, the FBI cannot directly control the number of children identified and/or rescued at any given time through investigative techniques, due to the reactive nature of this measure. The FBI has, however, taken definitive action to negate data limitations associated with this measure through its continued collaboration with the National Center for Missing & Exploited Children (NCMEC)/Child Victim Identification Program (CVIP) and successful initiatives such as, the Innocent Images International Task Force and the Endangered Child Alert Program (ECAP):

- 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.

- Innocent Images International Task Force became operational in October 2006 and includes law enforcement officers from more than 20 different countries. This task force successfully brings together law enforcement from around the world to address the global crime problem of online child exploitation.

- ECAP, an aggressive approach to identify unknown individuals involved in the sexual abuse of children and the production of child pornography, became operational in February 2004. ECAP uses national and international media exposure of unknown adults featured in child pornography and displays their faces on the "Seeking Information" section of our website in hopes that someone can identify them. To date, ECAP has successfully identified twelve subjects, with eight of those twelve pending prosecution. These investigations have led to the identification of at least 37 child victims.

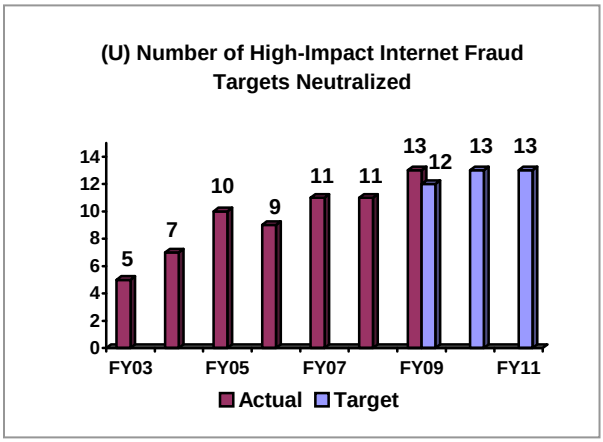
Although precise targets are difficult to establish for this measure, the FBI expects that the requested FY 2011 enhancement for the IINI program will have a positive effect on the number of potential identifications, through increased activity in these investigative efforts, to raise results beyond those expected for the current fiscal year.

FY 2010 Target: 130
FY 2011 Target: 140

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 2009 Target: 12
FY 2009 Actual: 13

Discussion:
The FBI exceeded its target for this measure in FY 2009. Among the notable cases of Internet fraud cited here:

- The FBI provided assistance in the international investigation of a $1.4 million advanced fee scam involving four individuals from the Netherlands. Three of the subjects have been extradited to the U.S. and are awaiting sentencing, and the fourth is awaiting extradition.
- A scam involving sales of undelivered vehicles for a combined loss of approximately $2.5 million that originated in Romania, with many operatives working out of the Las Vegas area. After an investigation by the FBI's Las Vegas office, four subjects have been convicted in relation to this crime, two in federal court and two in state court.
- Following an investigation by FBI's Milwaukee Division, a woman pled guilty to four charges of wire fraud after it was discovered that she fraudulently convinced at least four different families that she was pregnant and wanted each family to adopt the unborn child. In each case, she later told the family either the baby had died or the father would not agree to the adoption.

FY 2010 Target: 13
FY 2011 Target: 13

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 travelers. 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 US. 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's IPR program is in the process of building the FBI HQ capacity to support field divisions with HQ-driven undercover operations. While field offices should tackle the IPR crime problem where it exists, this centralization will allow the FBI to target the heads of organizations that have tentacles throughout the U.S. and the world, and then give those cases back to the division or country with jurisdiction.

The FBI's main mechanism to address Internet fraud is the Internet Crime Complaint Center (IC3). The IC3 receives and analyzes Internet fraud complaint data and serves as a "one-stop-shop" for Internet crime referrals. IC3 started strongly, and needs to continue building on its strength to combat the steadily growing criminal activity on the Internet. By acting as a central hub that links the FBI to the American public to private industry to local law enforcement, the IC3 is quickly becoming an invaluable tool for sharing and relaying information among these sources. As the IC3 continues to develop, it is accumulating a tremendously valuable asset: a centralized repository of Internet crime data. If properly maintained and analyzed, this body of information is likely to yield significant insights about trends, technologies, prevention, and combating techniques for Internet fraud and crime.

D. Criminal Justice Services Decision Unit

CRIMINAL JUSTICE SERVICES DECISION UNIT TOTAL	Perm. Pos.	FTE	Amount ($000)
2009 Enacted with Rescissions	1,947	1,920	$418,043
2009 Supplementals	…	…	14,055
2009 Enacted w/ Rescissions and Supplementals	1,947	1,920	432,098
2010 Enacted	1,990	1,941	424,291
Adjustments to Base and Technical Adjustments	(9)	(3)	(329)
2011 Current Services	1,981	1,938	423,962
2011 Program Increases	1	…	3,367
2011 Program Offsets	…	…	(679)
2011 Request	1,982	1,938	426,651
Total Change 2010-2011	**1**	**…**	**$6,548**

Criminal Justice Services Decision Unit — Information Technology Breakout	Perm. Pos.	FTE	Amount* ($000)
2009 Enacted with Rescissions	364	364	$461,202
2009 Supplementals	…	…	…
2009 Enacted w/Rescissions and Supplementals	364	364	461,202
2010 President's Budget	87	87	44,739
Adjustments to Base and Technical Adjustments	(24)	(24)	(6,134)
2011 Current Services	63	63	38,605
2011 Program Increases	…	…	60
2011 Request	63	63	38,665
Total Change 2010-2011	**(24)**	**(24)**	**($6,074)**

*Includes both direct and reimbursable funding

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 United States 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): 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. As of January 5, 2010, the FBI has conducted over 15.4 million fingerprint background checks during FY 2010.

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 criminal history records available from IAFIS, wanted person information, stolen vehicle information, and other data. In FY 2009, the NCIC processed over 6.8 million transactions per day. On July 24, 2009, NCIC set a record by processing 7.9 million transactions in one day.

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 has processed over 3.8 million inquiries as of December 31, 2009. The FBI conducted approximately 1.8 million of these checks, resulting in 20,929 denials to prohibited persons. Approximately 2 million checks have been 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 Criminal Justice Information Services 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, 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.

Law Enforcement Online (LEO): LEO is a 24-hour-a-day, 7-day-a-week, on-line (real time), state-of-the-art Internet 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 is a secure network that 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 currently supports a user base of over 150,000 vetted and authorized entities that can access LEO through any connection to the Internet.

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 building on 18 remote partnerships in major metropolitan areas accessed by approximately 60,000 users. N-DEx/OneDOJ currently has access to over 506,220,803 million records. These records include over 660,000 records from the FBI on violent crimes, hate crimes, human trafficking, fugitive, transportation crimes, and major theft, among others. N-DEx is still in the development stages, with Increment 1 and Increment 2 completed, and Increment 3 currently being developed.

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 United States. 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 United States 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 United States law enforcement, the Intelligence Community, the United States military, and other partners.

In FY 2009, the FBI Laboratory conducted approximately 717,000 forensic examinations (FBI, other Federal, state, and local). The Laboratory estimates that it will conduct approximately 735,000 forensic examinations in FY 2010 and in FY 2011, respectively.

Training Division

The state and local law enforcement training programs of the Training Division (TD) are scored in the CJS Decision Unit. Additionally, to capture the administrative resources required to support the CJS program, a prorated share of other TD and field training resources are scored in this decision unit.

The FBI provides instruction for state and local criminal justice practitioners, both at the FBI Academy and throughout the United States 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 2009, there were 1,022 state and local law enforcement officers that participated in the National Academy program at the FBI Academy in Quantico, Virginia. The FY 2010 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 2009, 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 2010.

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 2009, the FBI provided training to an estimated 4,800 international police officers and executives representing 95 countries. It is expected that there will be 4,900 international police officers trained in FY 2010.

Management and Support Services

In addition to CJIS and other investigative support divisions which make up the core elements of the CJS Decision Unit, prorated portions of the FBI's various administrative and other support programs that provide essential services are scored to the CJS Decision Unit. The administrative programs lead the FBI effectively through the challenges and changes that are continuously presented to federal law enforcement; provide effective direction and support to investigative personnel; and ensure that adequate resources exist to address the FBI's criminal investigative, national security, and law enforcement support responsibilities. A prorated share of resources associated with the Finance Division, Human Resources Division, Inspection Division, and other administrative entities support the CJS mission.

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 2009	FY 2009	2010 Enacted	Current Services Adjustments & FY2011 Program Change	FY 2011 Request
IAFIS fingerprint background checks	56,343,419	52,693,397	89,019,199	5,341,883	94,361,082
NCIC transactions	2,570,909,502	2,452,765,160	2,728,841,676	272,884,168	3,001,725,844
Total number of federal, state, and local investigations aided by the Combined DNA Index System (CODIS)	†	20,792	†	†	†
Total number of forensic and offender matches identified at CODIS	†	22,652	†	†	†

Total Costs and FTE	Final Target		Actual		Projected		Changes		Requested (Total)	
	FTE	$000	FTE	$000	FTE	$000	FTE	$000	FTE	$000
	1,920	432,098	1,738	492,071	1,941	424,291	…	6,548	1,938	426,651

TYPE/ STRATEGIC OBJECTIVE	PERFORMANCE	Final Target	Actual	Projected	Changes	Requested (Total)
		FY 2009	FY 2009	2010 Enacted	Current Services Adjustments & FY2011 Program Change	FY 2011 Request
Efficiency Measures	**IAFIS:** % of electronically submitted fingerprint identification requests:					
	Criminal:					
	• General checks completed w/in 2 hours	95.0%	98.21%	95.0%	--	95.0%
	• DHS checks completed w/in 72 hours	95.0%	99.99%	95.0%	--	95.0%
	Civil:					
	• General checks completed w/in 24 hours	99.0%	98.78%	99.0%	--	99.0%
	• DOS checks completed w/in 15 minutes	97.0%	99.74%	97.0%		97.0%
Performance Measure	**NCIC:**					
	• System availability	99.7%	99.8%	99.7%	--	99.7%
	• Downtime in minutes	1,440	1,028	1,440	--	1,440
Performance Measure	**NICS:** % of NICS checks with an Immediate Determination	90.0%	91.9%	90.0%	--	90.0%

TYPE/ STRATEGIC OBJECTIVE	PERFORMANCE	FY 2009	FY 2009	2010 Enacted	Current Services Adjustments & FY2011 Program Change	FY 2011 Request
Performance Measure	Student-weeks of Instruction at the Hazardous Devices School (HDS)	2,668	2,437	2,668	30	2,698

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
		Actual	Actual	Actual	Actual	Actual	Actual	Target	Actual	Target	Target
Efficiency Measures	**IAFIS:** % of electronically submitted fingerprint identification requests: <u>Criminal</u>: • General checks completed w/in 2 hours • DHS checks completed w/in 72 hours <u>Civil</u>: • 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	 95.0% 95.0% 99.0% 97.0%	 98.21% 99.99% 98.78% 99.74%	 95.0% 95.0% 99.0% 97.0%	 95.0% 95.0% 99.0% 97.0%
Performance Measure	**NICS:** % of NICS checks with an Immediate Determination	91.23%	91.85%	91.45%	91.46%	91.63%	91.66%	90%	91.9%	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	99.7% 1,440	99.8% 1,028	99.7% 1,440	99.7% 1,440
Performance Measure	Student-weeks of Instruction at the Hazardous Devices School (HDS)	2,245	2,304	2,593	2,614	2,159	2,605	2,668	2,437	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.

Measure changes for this performance report are proposed as a result of an internal review of the FBI's performance measures, pursuant to an initiative coordinated by DOJ's Performance Improvement Officer (PIO) Panel in Spring, 2009.

a. Performance Plan and Report for Outcomes

Integrated Automated Fingerprint Identification System

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. Today, the CJIS Division averages 140,000 fingerprints submissions daily.

The FBI's Criminal Justice Information Services (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.

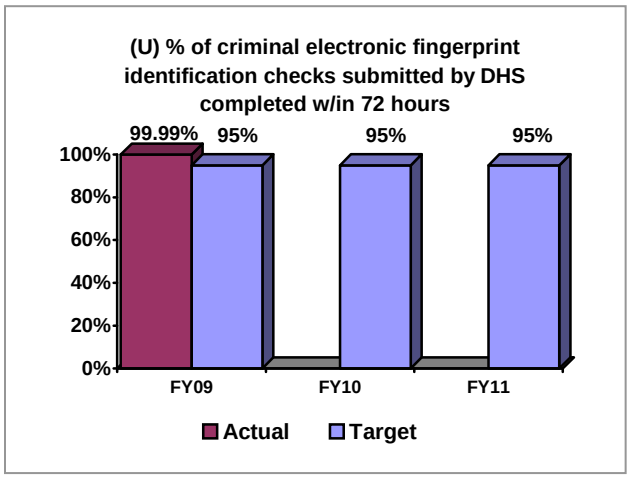
The project managers in the Biometrics Services Section (BSS) of CJIS are transitioning to revised performance metrics for the IAFIS system. These revised metrics would concentrate on targeting mean processing time to perform identifications, rather than the percentage of identifications meeting their goal for turnaround time. The proposed changes to the reporting of performance standards would allow for the BSS to project movable metrics as system and operational decisions change. Future budget reports will use these data to track performance of this system.

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

FY 2009 Target: 95%
FY 2009 Actual: 99.99%

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. Presently, these account for 36.23% of the daily criminal workload.

FY 2010 Target: 95%
FY 2011 Target: 95%

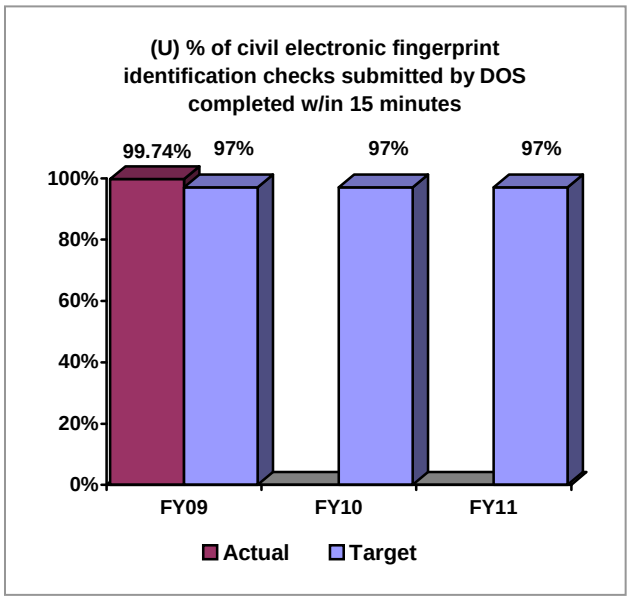


Performance Measure: NEW MEASURE: Percentage of civil electronic fingerprint identification checks submitted by the Department of State completed within 15 minutes.

FY 2009 Target: 97%
FY 2009 Actual: 99.74%

Discussion:
In November 2007, the Department of State and the FBI agreed that civil submissions from consulates would be processed within 15 minutes. Presently, these account for 6.03% of the daily civil workload.

FY 2010 Target: 97%
FY 2011 Target: 97%



Hazardous Devices School

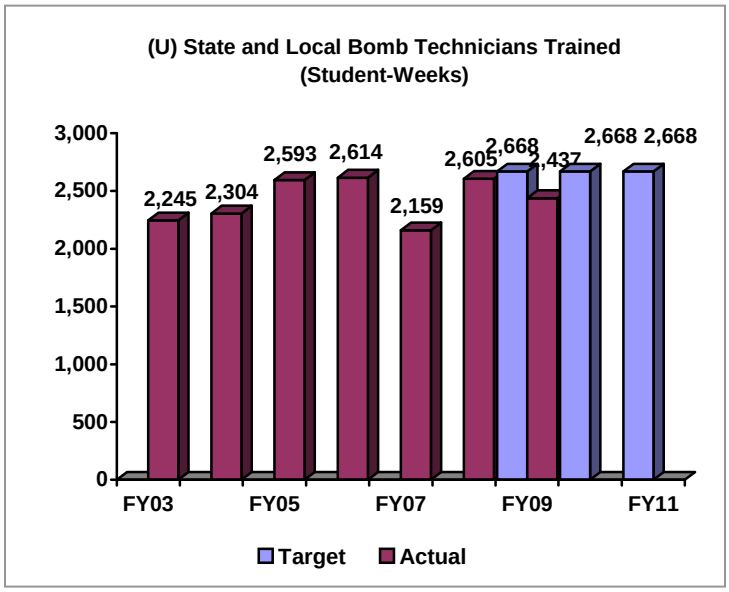
Two key elements of domestic preparedness are expertise in hazardous devices and emergency response capabilities to address threats such as weapons of mass destruction (WMD). The HDS is the only formal domestic training school for state and local law enforcement to learn safe and effective bomb disposal 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 Hazardous Devices School (HDS)

FY 2009 Target: 2,668
FY 2009 Actual: 2,437

Discussion:
HDS reports that the amount of training for FY 2009 was slightly lower than expected. This result is due to the delay of a pilot program that will be delayed until FY 2010.

FY 2010 Target: 2,668
FY 2011 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 mandate of an Immediate

Determination Rate (IDR) of 90%, and the Brady Act's three business day deadline for a final determination. As transaction volumes increase, the NICS program risks missing its IDR target in order to ensure compliance with the federal statutory deadline. Personnel budget enhancements in support of the NICS program ensure that it is able to meet both performance goals.

The FBI Hazardous Devices School (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 United States and its interests. This training includes countermeasures targeting suicide bombers, vehicle borne IED's, stand-off weapons, WMD devices, and radio-controlled IED's. 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.

Item Name: **Computer Intrusions**

Budget Decision Unit(s): All
Strategic Goal(s) & Objective(s): 1.1
FBI SMS Objective: A-01, A-02, P-03, P-04, P-05, P-06
Organizational Program: Cyber, Counterintelligence, Intelligence, and Security
End-State Capability: Domain & Operations, Leveraging Technology, Partnerships, Surveillance, Workforce

Program Increase: Positions 163 Agt 63 FTE 81 Dollars $45,926,000 ($14,737,000 non-personnel)

Description of Item
The FBI requests 163 positions (63 Agents, 46 Intelligence Analysts (IAs)) and $45,926,000 ($14,737,000 non-personnel) to increase investigatory capability and protect critical technology network infrastructure from malicious cyber intrusions.

Justification
Threat Summary
Attacks against the information infrastructure of the U.S. are a grave threat to the national and economic security of the U.S. All critical infrastructures are dependent on reliable access to the Internet. Terrorist groups, hostile foreign intelligence services, and transnational criminal organizations target computer networks to steal classified, proprietary, and sensitive information, manipulate critical data, and perpetrate fraud. According to one authoritative estimate, companies worldwide lost more than $1 trillion last year through data theft and cybercrime.[2]

Over the past 15 years, the global online community has grown from a few million users to nearly a quarter of the world's population. All critical infrastructure sectors to include water, health, energy, finance, defense, information technology, communications, chemical, transportation, and emergency services conduct significant activities over systems which reside upon, or can be accessed via the Internet. The communication of vital and sensitive economic, political and private information is sent over the Internet, the disruption of which could have catastrophic results around the world.

China
According to the Department of Defense,[3] China is in the midst of what it terms the "revolution in military affairs with PLA characteristics." This long-term, comprehensive transformation is intended to enable China to engage in "local wars under informatized conditions." In the near term, China seeks the ability to project power across the Taiwan

[2]McAfee, *Unsecured Economies: Protecting Vital Information*, 2009

[3]*DoD, Annual Report to Congress: Military Power of the People's Republic of China 2008* http://www.defenselink.mil/pubs/pdfs/China-Military-Report-08.pdf

Straits. In support of this effort, China aggressively collects classified, proprietary, and sensitive data from national laboratories, U.S. government agencies, contractors, and other commercial and academic institutions. Among the key technologies China seeks to acquire are state-of-the-art Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR), space systems, advanced nuclear and undersea weapons, and cruise missiles. Most significantly, China seeks to establish "electromagnetic dominance" on the battlefield. Toward that end, the PLA is expanding and improving its capability to conduct all forms of Computer Network Operations (CNO), including Network Exploitation and Network Attack. The PLA has fielded information warfare units which, among other things, developed viruses for preemptive attacks against enemy networks. In 2005, the PLA conducted its first military exercises which incorporated offensive CNO; PLA information warfare units practiced conducting cyber first strikes against notional enemy networks.

Russia

Russian Organized Cyber Crime is the third greatest presently identified threat. Groups centered in Russia and other eastern European countries penetrate networks and individual computers to support a wide range of fraud schemes. These groups create botnets, enormous networks of hijacked victim computers, which they rent to criminals for distributed denial of service attacks or spam propagation, which support a wide arrange of scams, including identity theft and credit card fraud. One group in St. Petersburg is known to have hacked into 13 banks from which they stole hundreds of millions of dollars. In one day last November, this group stole almost $10 million from a debit card processor. For several weeks prior to the attack, the group resided on the victim's computer network, which enabled it to collect account numbers for 45 payroll debit cards. In addition, the hackers overcame the victim's encryption to collect the PINs for these debit cards. On the day of the attack, hackers continuously reset account limits on these 45 accounts while cashers in 28 countries withdrew money from ATMs. This group currently plans to target a stock exchange.

Technology Advances

The overall threat to U.S. networks will continue to grow in size, impact, and complexity. Computer intrusions are a low-cost, low-risk vehicle for conducting espionage, economic espionage, and fraud. Currently, an arms race is underway between hackers and the information assurance community. As losses to victims, particularly in the private sector, continue to mount, more and more firms enter the information assurance, incident response, and forensic analysis industry with a concomitant rise in preventative innovation measures. However, the hackers – particularly state-sponsored actors – have proven extremely nimble and quickly overcome new countermeasures. In this environment, the U.S. Government simply cannot keep up with the state-of-the-art. By the time government can certify and implement new procedures for evidence collection and analysis, those techniques have become obsolete.

The cyber issue cannot be addressed by law enforcement or intelligence action alone. This effort will require the coordination of many sectors of the U.S. Government. However, those pieces of the problem which fall within the FBI's competency – domestic

counterintelligence and law enforcement – are daunting and will require greater inputs of personnel and non-personnel resources to address.

Role of the FBI

Law enforcement plays an important role in addressing this threat. Cyber threats transcend international borders, leveraging domestic systems as unwilling accomplices in attacks against U.S. critical infrastructures and cyber assets. In several cases, threat actors also reside and operate from within our borders. As with the Global War on Terror, our efforts to thwart the cyber domain problem are not limited to our intelligence capabilities abroad, but depend heavily on our ability to lawfully track, understand, and mitigate these threats domestically.

Law enforcement is focused on the identification, pursuit, and mitigation of threat organizations and threat actors themselves. Unlike many other cyber-oriented initiatives within the federal government that focus on building more secure computer systems and developing our ability to actively block cyber attacks as they occur, the FBI focuses on the pursuit of the persons behind cyber attacks.

Historically, no matter how secure the system, criminals and nation-state adversaries have discovered ways to undermine it. To expect security design alone to prevail assumes that construction of an invincible system is possible. Given the realities of our performance in this area, we must not only strive for better systems, but also the pursuit of those that would seek to do harm to them. Law enforcement plays an important role in cyber threat deterrence by assigning the consequences of attribution and legal recourse to threat actors, thereby raising the risk to anyone perpetuating cyber attacks. Even in the national security domain, this deterrence can have a powerful affect as it forms the basis for action under national political doctrine and international treaty, both of which are strong motivators in our efforts to create safety for our critical infrastructures and valuable cyber assets.

The importance of law enforcement as an enabling element was recognized in the Comprehensive National Cyber Security Initiative established by the previous administration under the Homeland Security Presidential Directive 23/National Security Presidential Directive 54. Under this directive, the FBI was also identified as the executive agent for the National Cyber Investigative Joint Task Force (NCIJTF). The NCIJTF has been instrumental in bringing a threat-centric approach to response and proactive mitigation within the IC, having already contributed to identifying numerous threat actors, attributing several computer intrusion activities, and working proactively with targeted victims to reduce or eliminate losses.

These demonstrated successes have not gone unnoticed. The FBI and NCIJTF are routinely highlighted by others in all branches of the USG as capable and effective elements in developing a national cyber strategy. The recently released Center for Strategic and International Studies (CSIS) Report on Cybersecurity for the 44th Presidency emphasizes the role of the FBI, the NCIJTF, and law enforcement as a whole.

The President's 60-day cyber study entitled "Cyberspace Policy Review," released May 2009, also highlights a number of activities across the U.S. Government that demonstrate progress towards improving and managing the nation's cybersecurity. With the prevalence and danger of cyber threats well established, the report calls for increased engagement of counterintelligence and law enforcement on a well established track of achieving desirable outcomes that identify, mitigate, and disrupt cyber threats domestically. As has been shown, this domestic capacity is critical to understanding and managing the global cyber threat, as well as ensuring the effective management of U.S. cyber defenses. As an added challenge, domestic management of this threat must carefully balance the privacy and civil liberties of U.S. citizens and corporations falling victim to these threats. The report also recognized the significant operational progress of the FBI-led NCIJTF, with the NCIJTF established as an example of successful multi-agency collaboration on cyber threat investigations. To this end, the FBI is expected to lead the development and furtherance of these law-enforcement missions, with the aim to get ahead of these dangerous cyber adversaries.

FBI Cyber Strategy

The FBI's strategy to address the cyber domain problem is built around a threat-centric approach. This strategy consists of interdivisional and interagency investigative teams focused on collections of related intrusions or activity known to be originating from a given threat country or threat organization. Each of these threat focus teams (Threat Focus Cells or TFCs) are guided by five structural pillars of investigation maturity and development. Addressing each of these pillars is needed to reach mission goals to identify, pursue and mitigate cyber threats. These pillars build incrementally towards the goal of proactive mitigation, establishing competencies in capabilities that are needed along the way. The pillars include:

Pillar I – Structure and Method

This pillar focuses on understanding the mechanics behind current intrusion activity, establishing lawful surveillance, identifying current victims, and notifying them of intrusions (where such notification does not undermine investigative or national security goals, pursuant to Title I of the Justice For All Act of 2004).

Pillar II – Victim Evaluation

This pillar focuses on understanding why a victim might have been targeted, assessing the damage done by the attackers, and evaluating the level of sophistication of threat actors.

Pillar III – Subject Targeting

This pillar focuses on identifying threat actors and related persons, selecting which of these human subjects will provide value to the investigation, and developing Confidential Human Source (CHS) targeting packages necessary to direct human source development by FBI Field Agents domestically or other IC member agencies abroad.

Pillar IV – Consumer Identification
As all national-security and organized crime computer intrusions are motivated by some adversary seeking specific gains, this pillar focuses on understanding the motivations, goals, and requirements of the ultimate consumer. This pillar seeks to understand the threat organization.

Pillar V – Operation Development
With consumers and their motivations identified, operations that directly mitigate or neutralize threat organizations can be designed. Mitigations may include operations that deny an adversary the gains of their conquest, or deceive the adversary by introducing misinformation that limits the adversary's effectiveness or forces the adversary to question the value of the gains they may have made. Additional tools within this pillar also include covert and undercover operations intended to penetrate and undermine threat organizations.

This 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. Managing cyber threats in this model is a continual and iterative process – although each pillar builds on the previous, the FBI cannot stop activity in one pillar when an investigation matures to the next. This necessitates that the FBI invest to address gaps in all of these capabilities. This model forms the basis for the Computer Intrusions Program (CIP) enhancement submission.

Justification for Program Increases

I.) Comprehensive National Cybersecurity Initiative – 163 positions (63 Agents, 46 IAs) and $45,926,000 ($14,737,000 non-personnel)

Within the cyber domain, it is unrealistic to scale our historical investigative methods and approaches to the extensive incorporation of technology into society and the proliferation of malicious cyber activity. In the cyber domain of yesterday, the FBI established great success in forensically extracting evidence of criminal activity from hard drives and removable media. Although the FBI maintains an impressive capability in this method to this day, criminals and other adversaries are now compromising individual computers by the tens of thousands, limiting the feasibility of these methods. Similarly, whereas lawful intercept may be useful today to watch the actions of a subject, the increased proliferation of social networks, mobile devices, and the ubiquitous and often anonymous access to the Internet is challenging our ability to sustain comprehensive surveillance of suspects. The explosive volumes of data generated for even simple end-user actions, and the increasing use of strong encryption and the boundless resources required to defeat it are also bringing an end to the usefulness of our current methods.

To overcome these limitations, the FBI must operate differently, changing its paradigm to incorporate agile use of the lawful means at its disposal, while more efficiently leveraging current methods where they still apply. In operating with agility, the FBI must migrate from reactively responding to intrusions that occur to proactively tracking and

mitigating domestic national security threats and criminal enterprises. The CIP has forecast a number of gaps in the core capabilities that support the five pillars above. These gaps impact the FBI's ability to achieve these goals. Four areas to address these gaps are presented below:

1. Cyber Threat Investigative Capabilities
2. Cyber Intelligence Analysis
3. Science and Technology Tools to Enhance Investigatory and Intelligence Collection Capabilities
4. Information Assurance

1.) Cyber Threat Investigative Capabilities – 102 Positions (63 Agents) and $22,418,000 ($228,000 non-personnel)

Expand Cyber and Counterintelligence Investigative Capacity
The FBI requests 63 Field Agents to expand cyber and counterintelligence investigatory capabilities. Although computer intrusion activity domestically is greatest in high-tech regions, the borderless nature of cyberspace means that intrusions can occur anywhere. To this end, the CIP must provide a minimum capacity in every field office, while providing additional support to field offices with disproportionate workloads. Nonpersonnel funding of $228,000 is requested to provide Cyber equipment to outfit the requested Field Agents.

2.) Cyber Intelligence Analysis – 61 Positions (46 IAs) and $8,999,000 (all personnel)

3.) Science and Technology Tools to Enhance Investigatory and Intelligence Collection Capabilities – $11,009,000 (all non-personnel)

NCIJTF Analytic Platform (Lighthouse) – $11,009,000 (all non-personnel)

Fully provisioned, this enhancement provides the NCIJTF with a capability that enhances analytic capability, facilitates inter-agency collaboration, and enables the FBI to operate proactively against the threat. Furthermore, with this enhancement, the Lighthouse project will serve as a prototype to explore the concepts behind an FBI-wide cyber-analytic capability.

4.) Information Assurance (ODNI Transfer) - $3,500,000 (all non-personnel)

Impact on Performance (Relationship of Increase to Strategic Goals)

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

Funding

Base Funding

FY 2009 Enacted				FY 2010 President's Budget				FY 2011 Current Services			
Pos	Agt	FTE	($000)	Pos	Agt	FTE	($000)	Pos	Agt	FTE	($000)
300	68	195	$74,648	560	175	430	$135,828	560	175	560	$135,828

Personnel Increase Cost Summary

Item Name	Type of Position	Modular Cost per Position ($000)	Number of Positions Requested	FY 2011 Request ($000)	FY 2012 Net Annualization (change from 2011) ($000)
Investigative Requirements	Clerical	$91	22	$2,002	$154
Investigative Requirements	Information Technology	146	2	292	160
Investigative Requirements	Investigative	121	15	1,815	465
Investigative Requirements	Special Agent, Field	287	63	18,081	(3,024)
Intelligence Collection	Clerical	91	14	1,274	98
Intelligence Collection	Information Technology	146	1	146	80
Intelligence Collection	Intelligence Analyst, Field	165	35	5,775	2,030
Intelligence Collection	Intelligence Analyst, HQ	164	11	1,804	616
	Total Personnel		163	$31,189	$579

Non-Personnel Increase Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2011 Request ($000)	FY 2012 Net Annualization (Change from 2011) ($000)
Cyber Field Agent Equipment	n/a	n/a	$228	$...
NCIJTF Analytic Platform	n/a	n/a	11,009	…
Information Assurance	n/a	n/a	3,500	…
Total Non-Personnel			$14,737	$…

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	560	175	560	$92,929	$42,899	$135,828	$…

Increases	163	63	82	31,189	14,737	45,926	579
Grand Total	723	238	642	$124,118	$57,636	$181,754	$579

Item Name: **White Collar Crime**

Budget Decision Unit(s): Criminal Enterprises and Federal Crimes
Strategic Goal(s) & Objective(s): 1.2, 2.1, 2.5
FBI SMS Objective(s): A-02, A-24, P-03, P-05
Organizational Program: Criminal Investigative
End-State Capability: Domain & Operations

Program Increase: Positions 367 Agt 143 FTE 289 Dollars $75,265,000 ($897,000 non-personnel)

Description of Item
The FBI requests 367 positions (143 Agents and 39 Intelligence Analysts (IAs)) and $75,265,000 ($897,000 non-personnel) to address the White Collar Crime (WCC) threat[4]. The requested resources support the Financial Crime and Government Fraud Initiatives.

Justification
Threat Summary
The housing and financial system collapse revealed a myriad of mortgage, corporate, and securities and commodities fraud schemes costing Americans and world financial markets trillions of dollars. Governments have responded with various multibillion dollar assistance/bailout programs that will lead to an increase in both expected fraud, such as government fraud, and unanticipated fraud schemes. The current resource level of the FBI's White Collar Crime program is inadequate to address gaps in current and anticipated fraud workload in the following areas:

- Mortgage and sub-prime industry related fraud
- Emergency Economic Stabilization Act of 2008 (EESA) Troubled Asset Relief Program (TARP) criminal abuse and fraud
- Housing and Economic Recovery Act (HERA) fraud
- Corporate Fraud
- Securities and commodities fraud (including Ponzi schemes and high yield investment fraud)
- Block grant abuse and fraud against the United States Government

Mortgage and Sub-Prime Industry Related Fraud
Mortgage fraud continues to absorb considerable FBI resources and has not yet begun to abate. At the start of FY 2010, over 68 percent of the FBI's 2,944 mortgage fraud cases involved losses exceeding $1 million. FBI intelligence, 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 failure, regulatory agency/independent auditor fraud referrals, and governmental housing relief fraud. In particular, the increases in

[4] This includes resources required to make permanent the FY 2010 Financial Crime Supplemental, which includes 211 positions (81 Agents, 3 IA) and $44,765,000 ($113,000 non-personnel).

foreclosures are creating new opportunities for criminals as they defraud homeowners desperate to forestall the loss of their home. At the start of FY 2010, the Federal Deposit Insurance Corporation (FDIC) had also identified 552 financial institutions with $346 billion in assets as having the potential to become insolvent. The FBI anticipates that some of these failures will require criminal investigations into the companies' investments derived from fraudulent loans and deceptive accounting practices.

EESA/TARP Related Fraud

The FBI further anticipates new opportunities for fraud through the EESA. Through the EESA, the United States Government originally planned to purchase large amounts of liquid, risky mortgage backed securities from financial institutions through the TARP, which was estimated to involve a minimum of $700 billion in additional commitments. However, the program evolved into 12 interconnected programs involving USG and private funds with potential expenditures of up to nearly $3 trillion, roughly the size of the entire federal budget for FY 2008. The plan has directly shifted the burden of accounting oversight and due diligence to the United States Government, and the level of controls to address possible fraud is insufficient according to the SIGTARP[5]. As the United States Treasury Department and other government programs continue to develop, the possibility of corporate fraud and fraud against the government increases.

HERA Related Fraud

The FBI also foresees an increase in fraud related to HERA. HERA authorizes the Federal Housing Administration (FHA) to insure up to $300 billion in mortgage loans, appropriates almost $4 billion to states and local governments for the redevelopment of abandoned and foreclosed homes, and allots $180 million for pre-foreclosure counseling and legal services for distressed homeowners. The FBI and the U.S. Department of Housing and Urban Development's (HUD) Office of Inspector General (OIG) anticipate the need to investigate mortgage fraud and fraud against the government schemes as a result of the substantial increase in volume of FHA insured mortgages and subsidies, including fraud by homeowners seeking to qualify for FHA loans; fraudulent appraisals designed to cover up original lender losses; fraud by third party facilitators; fraudulent "windfall" schemes; and fraud, waste or abuse by third parties in the counseling or legal services business.

Corporate Fraud

The majority of corporate fraud cases pursued by the FBI involve accounting schemes designed to deceive investors, auditors, and analysts about the true financial 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 United States economy and investor confidence. Industry survey results reported in *Financial Week* indicate an estimated loss of $8.2 million per company[6] due to fraud.

[5] "SIGTARP Quarterly Report to Congress"; 10/21/2009

[6] Financial Week, "Corporate Fraud Cost is Up 22% at Average Biz" by Beth Braverman; 09/14/08

Securities and Commodities Fraud
Estimated losses due to securities and commodities fraud are measured in the tens of billions of dollars per year, and are associated with decreased market value of businesses, reduced or non-existent return on investments, and legal and investigative costs. The victims of securities and commodities frauds include individual investors, financial institutions, public and private companies, government entities and retirement funds. To illustrate the scale of such fraud and its impact on the economy, the Bernard Madoff case alone represented losses of over $50 billion.

The FBI anticipates an increase in the volume of fraud investigations pertaining to high yield investment frauds, or "Ponzi schemes," as a result of the dramatic decline in the financial markets. High yield investment frauds survive by utilizing new investment money from new investors to pay returns to previous investors. When there is a dramatic market decline in the financial markets as seen in 2008, investors limit or stop investing and often request pay-outs from their investment portfolio. As a result, Ponzi schemes are exposed when the perpetrators do not have the funds available to pay the investors. The collapse of Ponzi schemes can have a dramatic impact on investors and financial markets. As of August 2009, the FBI had already opened twice as many high yield investment fraud investigations than in all of FY 2007.

Government Fraud
Of new and growing concern to the FBI is the government fraud threat posed by recent economic recovery-oriented legislation. The FBI anticipates a marked increase in government fraud matters, which include the theft of government money by private citizens and government employees as the funding trickles down to all levels to finally rest at the local and private industry level. With appropriations for economic stimulus and recovery programs potentially surpassing $3 trillion over the next three years, the FBI forecasts a sizeable threat to the integrity of government and loss of significant taxpayer dollars if not effectively addressed.

Justification
Financial Crime Investigations: 343 positions (143 Agents and 21 IA) and $71,497,000 ($645,000 non-personnel)

Making the FY 2009/2010 Supplemental Permanent – 211 positions (81 Agents, 3 IA) and $44,765,000 ($113,000 non-personnel)
The FBI requests that the 211 positions, and the requisite funding to support them, from the FY 2009/2010 Supplemental be made a permanent part of the FBI's base in order to sustain this capacity and meet the demands of the current and future financial crimes workload.

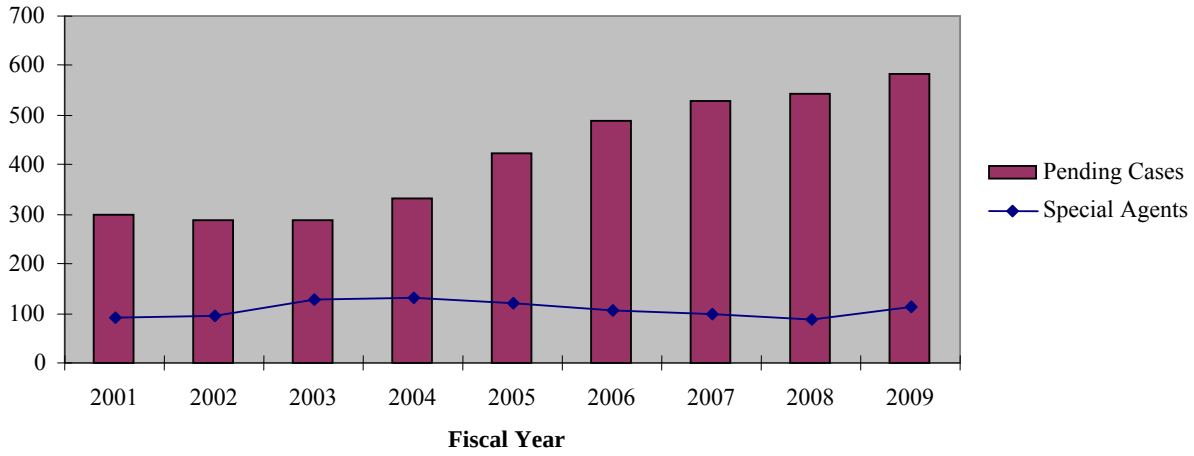
Corporate Fraud Investigations – 79 positions (41 Agents and 9 IA) and $16,714,000 ($468,000 non-personnel)

The FBI anticipates an increase in corporate fraud investigations as a result of the current financial crisis partly caused by the collapse of the sub-prime mortgage market. As Wall Street firms are examined with additional scrutiny from regulators and independent

accountants, it is believed that further corporate malfeasance will come to light and the number of corporate fraud investigations will increase. As previously mentioned, Congress recently enacted EESA, HERA, and the American Recovery and Reinvestment Act of 2009 (ARRA) in an effort to return stability to the United States financial and housing markets. It is anticipated that the new legislation will also result in increased levels of fraud.

The growth in caseloads is particularly disturbing in that fully addressing a typical corporate fraud case may require 18 months to 5 years to complete with a team of 5 to 10 agents and the accompanying professional staff. An ideal ratio of corporate fraud agents to pending cases would be nearly 1:1, with a maximum acceptable ratio of three cases per agent (3:1) assuming full support from analytical, accounting, and technical support positions. The ratio at the start of FY 2010 is approximately 5:1.

Corporate Fraud Workload



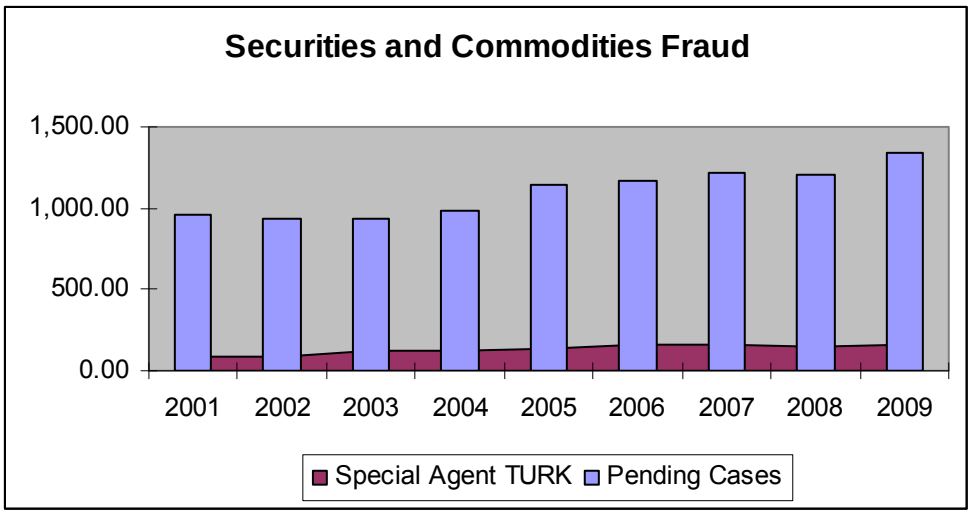
The FBI requests 41 new agents, which would permit the FBI to fully address an estimated 123 additional corporate fraud cases each year. To realize this impact, however, requires an increase in analytical and support resources to support the new agents.

The FBI requests 9 IAs to support intelligence driven corporate fraud investigations. Through the expansion of the Directorate of Intelligence, the FBI has identified numerous advantages of using intelligence to drive investigations. At the start of FY 2010, only 4 IAs were addressing corporate fraud across all field offices. The inability to generate tactical and strategic intelligence has crippled the FBI's ability to properly identify major fraud risks and perpetrators, anticipate new schemes, and prioritize investigations for maximum impact with limited resources. The requested 9 IAs would bring the ratio of IAs per investigative agents to 1:12 from the 1:28 ratio at the start of FY 2010.

The FBI also requests $468,000 in additional case funding to employ effective techniques, including the use of confidential sources, technical and physical surveillance, and undercover and sensitive operations to support White Collar Crime investigations.

Securities and Commodities Fraud Investigations – 53 positions (21 Agents and 9 IA) and $10,018,000 ($64,000 non-personnel)

Market manipulation investigations are particularly complicated, requiring proactive and sophisticated investigative techniques, including undercover operations and technical and human surveillance. Addressing this threat is manpower and time intensive, and can not be accomplished with current resource levels.



The growth in caseload is especially alarming considering that a typical securities and commodities fraud case may require over one year to address. The ratio of open pending cases to agents at the end of FY 2009 was approximately 9:1 without accounting for any unaddressed work.

The FBI requests an additional 21 Agents, which would allow the FBI to address an estimated 84 additional securities and commodities fraud cases each year. However, this impact relies on the use of analytical and support resources in coordination with the Special Agents to realize this rate of return.

Given the large quantities of evidence and data collected during a single investigation, the FBI requests 6 Forensic Accountants to review, analyze, and prepare seized financial data for investigation and the production of evidence. This enhancement would improve the FBI's abilities to process cases faster, focus investigations on the pertinent individuals and facts, and support successful prosecutions with appropriate sentences. More accurate and thorough evaluation of financial evidence would also improve the United States Government's capability to identify assets used to facilitate the criminal activity and the

proceeds derived from that activity, and thereby improving the ability to provide restitution to victims through the Asset Forfeiture program.

The FBI requests 9 IAs to generate tactical and strategic intelligence, identify major fraud risks and perpetrators, anticipate new schemes, and prioritize investigations for maximum impact. As of the beginning of FY 2010, only 5 IAs for all field offices were addressing the problem of securities and commodities fraud.

The FBI requests $64,000 in additional case funding to employ effective investigative techniques, including confidential sources, technical and physical surveillance, and undercover and sensitive operations.

Government Fraud: 24 positions (18 IA) and $3,768,000 ($252,000 non-personnel)

Government Fraud Investigations – 24 positions (18 IA) and $3,768,000 ($252,000 non-personnel)

With the recent appropriation and expenditure of billions of dollars in government spending, the FBI anticipates a marked increase in government fraud. More specifically, through the Neighborhood Stabilization Program (NSP), HUD will manage the distribution of $3.92 billion through community development block grants (CDBGs). Based on a study of foreclosed properties, all 50 states and an additional 258 communities were chosen to receive CDBGs. Every state will receive a minimum of $19.6 million and every community chosen receives a minimum of $2.2 million. The majority of funding will be distributed from February 2009 to August 2010. Because of the rapid implementation and large amount of funding associated with the NSP, it is anticipated that government fraud violations will occur before, during and after this funding is distributed. The FBI currently does not have the resource capacity to effectively address this emerging threat as resource limitations already dictate investigative priority, which currently results in under addressed government fraud cases.

Hundreds of billions of dollars will be distributed through the ARRA to states for a variety of infrastructure and other programs. The scale and size of the taxpayer dollars associated with this appropriation dwarf that of the NSP and the FBI cannot, without additional resources, address the anticipated fraud that puts these taxpayer funds at risk. Fortunately, the majority of the expenditures will not occur until FY 2010 and FY 2011. This request would permit the FBI to build the necessary analytical capacity to identify the most egregious fraud schemes and proactively address this threat.

As small towns and rural areas receive hundreds of millions of dollars in federal funding, FBI Resident Agencies and Field Offices with previously manageable public corruption case loads will find themselves faced with multiple large and complicated public corruption and government fraud cases that exceed available resources. To effectively

target the FBI's limited resources for maximum effect, additional intelligence capacity is required.

To understand the scope of possible fraud, the relief effort for areas affected by Hurricane Katrina reached approximately $149 billion by September 30, 2008. Audits, inspections, reviews, and investigations by members of the law enforcement and Inspector General communities resulted in 1,348 arrests, 1,549 indictments and 1,075 convictions for fraud, theft, false claims, and corruption. A GAO audit in 2006 claimed that 16%, or $1 billion, of the total $6.2 billion Katrina Relief fund were associated with fraudulent or improper claims. Other GAO reports on Katrina relief revealed fraud rates from one of every ten dollars to one of every six dollars. The current economic recovery is larger and more complex than the hurricane relief programs, affects more field offices, and is administered through more federal, state and local offices and non-governmental organizations. In example, the ARRA is five times larger than the Katrina Relief efforts.

With an extremely limited number of IAs addressing government fraud matters throughout the field, the FBI's ability to generate tactical and strategic intelligence is hindered, thus resulting in limited opportunity to effectively identify major fraud risks, anticipate new schemes, and prioritize investigations for maximum impact. The addition of 18 IAs throughout the field would allow the FBI to address a portion of this shortfall in tactical and strategic intelligence by stationing IAs in Field Offices with responsibilities for communities that will receive high levels of federal funding, as well as in the New York and Washington Field Offices due to their unique jurisdictions. Three IAs would be based at FBI Headquarters to coordinate and facilitate a national strategic intelligence approach to the threat.

To best utilize the requested personnel enhancements, the FBI requests $252,000 in case funding to employ effective investigative techniques such as confidential sources, technical and physical surveillance, and undercover and sensitive operations.

Impact on Performance (Relationship of Increase to Strategic Goals)
Without the additional resources requested, the FBI will not be able to address the growing WCC threat. The FBI is currently unable to address the increase in workload in top tier financial crimes and government fraud threats. Between the rapid increases in corporate fraud, securities and commodities fraud, mortgage fraud, and the significant federal expenditures for economic recovery programs, the United States is exposed to an extensive range of criminal threats that the FBI cannot address without additional investigative and support resources.

These resources would be applied to high impact investigations that involve cases of significant losses to the US Government and its citizens. Based on recent average performance in these programs, the enhancements would potentially result in $1.2 billion in the first year alone in restitution orders, recoveries, and the forfeiture of assets, and $5.8 billion over the first three years. These positive financial impacts would be forfeited without the requested resources.

Without the additional resources, hundreds of additional financial crime cases will go unaddressed or under-addressed due to the lack of resources. These numbers would compound over time as criminals defraud additional victims.

Without additional resources to address government fraud risk, potentially trillions of dollars in taxpayer dollars are at risk to fraud and abuse without the ability to fully safeguard those funds and bring those who would defraud the government to justice.

Funding

Base Funding

	FY 2009 Enacted				FY 2010 President's Budget				FY 2011 Current Services			
Program*	Pos	Agt	FTE	($000)	Pos	Agt	FTE	($000)	Pos	Agt	FTE	($000)
White Collar Crime	2,096	1,878	2,096	$341,569	2,239	1,928	2,168	$371,080	2,239	1,928	2,239	$378,400
Total	2,096	1,878	2,096	$341,569	2,239	1,928	2,168	$371,080	2,239	1,928	2,239	$378,400

*Note:
1) WCC resource totals represent the entire WCC field Agent FSL, and Intelligence Analyst and Forensic Accountant TURK in the field supporting the WCC program. Headquarters and administrative support are not included.

Personnel Increase Cost Summary

Initiative	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)
Financial Crime	Corporate Fraud Investigations	Clerical	$91,000	18	$1,638	$126
Financial Crime	Corporate Fraud Investigations	Information Technology	146,000	1	146	80
Financial Crime	Corporate Fraud Investigations	Intelligence Analyst, Field	165,000	9	1,485	522
Financial Crime	Corporate Fraud Investigations	Investigative Support	121,000	10	1,210	310
Financial Crime	Corporate Fraud Investigations	Special Agent, Field	287,000	41	11,767	(1,968)
Financial Crime	Financial Crime Supplemental	Position Upgrades	n/a	-	3,280	714
Financial Crime	Financial Crime Supplemental	Clerical	n/a	28	2,996	1,232
Financial Crime	Financial Crime Supplemental	Forensic Accountant	n/a	50	8,200	4,200
Financial Crime	Financial Crime Supplemental	Information Technology	n/a	4	920	504
Financial Crime	Financial Crime Supplemental	Intelligence Analyst, HQ	n/a	3	633	333
Financial Crime	Financial Crime Supplemental	Investigative Support	n/a	17	2,890	884
Financial Crime	Financial Crime Supplemental	Professional Staff	n/a	28	4,592	2,352
Financial Crime	Financial Crime Supplemental	Special Agent, Field	n/a	70	18,270	8,260
Financial Crime	Financial Crime Supplemental	Special Agents, HQ	n/a	11	2,871	$1,298
Financial Crime	Securities & Commodities Fraud Investigations	Clerical	91,000	11	1,001	77
Financial Crime	Securities & Commodities Fraud Investigations	Forensic Accountant	115,000	6	690	246
Financial Crime	Securities & Commodities Fraud Investigations	Information Technology	146,000	1	146	80
Financial Crime	Securities & Commodities Fraud Investigations	Intelligence Analyst, Field	165,000	9	1,485	522
Financial Crime	Securities & Commodities Fraud Investigations	Investigative Support	121,000	5	605	155
Financial Crime	Securities & Commodities Fraud Investigations	Special Agent, Field	287,000	21	6,027	(1,008)

Initiative	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)
Government Fraud	Government Fraud Investigations	Clerical	182,000	6	546	42
Government Fraud	Government Fraud Investigations	Intelligence Analyst, Field	165,000	18	2,970	1,044
		Total Personnel		367	$74,368	$20,005

Non-Personnel Increase Cost Summary

Initiative	Non-Personnel Item	Unit Cost	Quantity	FY 2011 Request ($000)	FY 2012 Net Annualization (Change from 2011) ($000)
Financial Crime	Corporate Fraud Investigations	n/a	n/a	$468	$ …
Financial Crime	Securities & Commodities Fraud Investigations	n/a	n/a	64	…
Financial Crime	Recurral of Financial Crime Supplemental	n/a	n/a	113	
Government Fraud	Government Fraud Investigations	n/a	n/a	252	…
	Total Non-Personnel			$897	$ …

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	2,239	1,928	2,239	$285,422	$92,978	$378,400	$…
Increases	367	143	289	74,368	897	75,265	20,005
Total	2,606	2,071	2,528	$359,790	$,39,875	$ 453,665	$20,005

Threat Name: **Operational Enablers**

Budget Decision Unit(s): All
Strategic Goal(s) & Objective(s): 1.1, 1.2, 2.1, 2.6, 2.7
FBI SMS Objective(s): All
Organizational Program: Facilities & Logistics, Information Technology, Intelligence, Laboratory
End-State Capability: Domain & Operations, Infrastructure, Leveraging Technology, Partnerships, Workforce

Program Increase: Positions 118 Agt 15 FTE 59 Dollars $25,121,000 ($6,000,000 non-personnel)

Description of Item
The FBI requests 118 positions (15 Agents and 69 Intelligence Analysts (IAs)) and $25,121,000 ($6,000,000 non-personnel) to address the FBI's Operational Enablers requirements. Funding and personnel will allow the FBI to build and maintain Information Technology (IT) connectivity, provide necessary analytical personnel and training for the intelligence transformation, and provide the necessary personnel to address the FBI Laboratory requirements. These initiatives are required for the full functionality of the FBI and necessary to aid personnel in addressing all threats facing the U.S.

Justification
Threat Summary
The FBI is currently facing technical, physical, and personnel constraints causing gaps in intelligence collection and analysis and a lack of sufficient personnel to assist in FBI forensic analysis. 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 and essential support personnel. These are elements of a foundation that determines the FBI's ability to effectively address law enforcement and national security threats. Missions cannot be adequately performed without the foundational elements of infrastructure.

Information Technology (IT) – The general IT infrastructure condition poses a variety of risks for mission support and case analysis. As IT systems are enhanced across the FBI, the networks and enterprise services need to be enhanced accordingly. As new users are added to the overall IT infrastructure, the risk of system failures and performance delays increase, impeding system productivity. With over 50 IT projects and an antiquated network and hardware, the FBI continually runs the risk of failures with mission-critical applications.

Intelligence Transformation – While IT systems are useful to search and manipulate intelligence data, human intelligence (HUMINT) collectors and Intelligence Analysts (IAs) are required to collect and analyze the information. The FBI uses intelligence to protect national security, dismantle criminal organizations, and solve complex cases.

Intelligence helps the FBI identify threats to the U.S., whether they are from foreign governments, gangs, organized criminals, hackers, or terrorists. In addition to the benefits of intelligence on specific cases, it also allows the government to gain perspective on the overarching threat picture or domain. With a big-picture view of the threats facing the nation, the FBI is better able to allocate resources on actors that pose the greatest danger to U.S. strategic interests and its citizenry. The FBI must proactively identify these actors and assess their skills, capabilities, and use of known tradecraft so as to find ways to penetrate and dismantle their operations before significant damage is achieved. Therefore, as part of the FBI's recent intelligence transformation, the FBI implemented the core intelligence functions: Domain management; collection management; requirements-based (sometimes non-case specific) collection - including HUMINT; tactical intelligence; and intelligence production and dissemination. However, many field offices lack the necessary HUMINT collectors, Intelligence Program Coordinators, Domain Manager Coordinators, Domain/All Source IAs, and Reports Officers needed to improve performance on these core intelligence functions.

Mission Achievement through Workforce Planning – In many areas, the FBI is not able to meet both inter- and intra-agency deadlines due to inadequate staffing levels. For example, the FBI Laboratory is many times unable to meet the 60-day turn around time required for investigative and prosecutorial purposes. By not meeting these important deadlines, the FBI faces the risk of delaying important data analysis relevant to cases. The Director of the FBI has recognized the considerable threat facing the organization and has identified targeted personnel augmentation as a critical need.

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 enhancements, the FBI runs the risk of losing critical support for overall functionality.

Justification

Information Technology Infrastructure –$3,000,000 (all non-personnel)

The FBI mission has expanded to include counterterrorism as well as an increased focus on intelligence gathering and sharing, in addition to the more traditional law enforcement activities. This expanded mission requires greater dependence on free flowing information sharing and interoperability with members of other communities.

Connectivity – $3,000,000 (all non-personnel)

In order to improve information integration and information sharing capabilities, the FBI requests $3,000,000 (ODNI transfer). Funding is required to update and maintain the identity and access management capabilities.

Intelligence Transformation – 116 positions (15 Agents, 69 IAs) and $18,829,000 (all personnel)

The FBI's Field Intelligence Groups (FIGs) manage intelligence operations in each of the FBI's 56 field offices. The FIG ensures that the field office integrates intelligence activities into all investigative efforts by systematically assessing their domain to identify potential threats, vulnerabilities, gaps in knowledge, and collection opportunities against

Intelligence Community (IC) and FBI-specific intelligence requirements. Over the last two years, the FBI has undergone an intelligence transformation to ensure that FIG resources are optimally utilized. A Strategic Execution Team (SET) comprised of almost 100 Special Agents (SAs), IAs, and other skilled professionals examined the intelligence activities in each of the FBI's 56 field offices. The team identified optimal structures and processes for intelligence activities and proceeded to implement a common model across each FIG based on these best practices. While the FIG structure has now been standardized across all field offices, critical gaps exist, affecting the FBI's core intelligence functions: domain management; collection management; requirements-based (sometimes non-case specific) collection - including HUMINT; tactical intelligence; and intelligence production and dissemination. To fill performance gaps, the FIGs realigned their analytic resources into these functional areas, for which additional resources are necessary.

Domain Management – 66 positions (50 IAs and 16 professional staff) and $9,816,000 (all personnel)

The FBI requests 66 positions (50 IAs and 16 professional staff) in support of FIG domain awareness and management. Domain awareness is the strategic understanding of threats, vulnerabilities, and gaps; it also contributes directly to the FBI's strategy to collect against these gaps. Domain management is the process by which the FBI manages and improves its domain awareness, and the ability of each field office to each perform this function for its respective domain is crucial to building an enterprise-wide domain understanding on a variety of priority threat issues. Each field office relies on its Domain Management Coordinator (DMC) and in some offices, a limited number of Domain analysts (who are All-Source IAs), as the key analytical personnel that support domain awareness and management. This is achieved through their creation of intelligence products such as Domain Intelligence Notes (DINs), Annual Domain Assessments, and geospatial products such as Common Operational Pictures (COPs) that provide a comprehensive picture of what is known about a threat and related gaps. This information is essential for management decisions regarding how best to allocate scarce investigative and intelligence resources. However, due to limited resources, these Domain analysts are required to simultaneously produce assessments on multiple threat programs while also performing other Domain-related functions, such as those that contribute directly to field office strategic management including threat prioritization, SPS sessions, etc. Insufficient analytic staffing in these critical areas prevents the FBI from optimally performing the core intelligence functions, thereby creating a myopic view of the threats within the domain.

Domain Intelligence Note (DINs) Production	**FY 2009**	**FY 2009 – YTD Oct-Dec**	**Forecasted FY 2010 Total**
Total Number of DINs	**681**	**120**	**800**

In order to ensure that the FBI has the necessary level of domain awareness of the threat environment, the FBI requires an additional 50 IAs and 16 professional staff. The requested personnel will provide strategic domain awareness through production of DINs, COPs and Annual Domain Assessments, develop threat indicators, identify

Domain entities and assist with identification of liaison contacts and Tripwires, and contribute to regional and national threat assessments. This resource level will push the FBI closer towards the optimal performance ratio of one All-Source IA to seven field Agents.

Collection Management – 21 positions (16 IAs) and $3,095,000 (all personnel)
The FBI requests 21 positions (16 IAs) in support of FIG collection management, which is the formal business process for prioritizing competing demands for intelligence collection. Balanced against national and regional requirements, Collection Management Coordinators (the lead strategic All-Source IA of the FIG), in cooperation with the Domain Management Coordinator, the Intelligence Program (IP) Manager, and the IP Coordinator, assess the potential impact of the threat, the magnitude of the vulnerabilities, and the depth of the knowledge gap in order to evaluate and prioritize the collection taskings. While each FIG requires a Collection Manager Coordinator, several field offices still lack this critical position. The requested 16 IAs will ensure that all FIGs are staffed with the minimum requirement of at least one Collection Manager Coordinator.

Requirements-Based HUMINT Collection – 25 positions (15 Agents) and $5,335,000 (all personnel)
The FIG Human Intelligence (HUMINT) Squads (comprised of Agent core collectors) collect intelligence to support domain awareness and satisfy the FBI's priority intelligence requirements. Providing cross-programmatic support by collecting against counterterrorism, counterintelligence, cyber, and criminal program requirements, HUMINT collectors use the full range of appropriate HUMINT tradecraft to develop, recruit, and exploit sources to leverage relationships with external partners in order to collect intelligence on the most critical collection gaps.

Intelligence – Training and Professional Development – 4 positions (3 IAs) and $583,000 (all personnel)
The FBI requests 4 positions (3 IAs) in support of training and professional development requirements for the Intelligence Program. In order to fully realize the successes of the FBI's Intelligence Transformation and to accomplish critical national security and criminal intelligence collection and analysis requirements, additional staffing is required. The additional positions will allow for the implementation of an in-depth training plan as identified in the FBI's Five-Year Intelligence Training Strategy, which identifies key intelligence work roles, responsibilities, and resources to develop the intelligence workforce. This strategy will contribute significantly to furthering the FBI's transformation from a case-driven to a fully capable intelligence-driven organization.

Current staffing of the FBI's Intelligence Training program allows for the delivery of only two programs: 1) maintenance of the Intelligence Basic Course (IBC), which provides basic training in ten weeks to newly hired IAs; and 2) maintenance of the current HUMINT Training Program (the 6-week Domestic HUMINT Collector Course and the 2-week HUMINT Intelligence Course). Current staffing will not allow for courses in intermediate and advanced analytic programs, collection management, targeting, reports

and dissemination, validation, HUMINT and analytic tradecraft for managers, and a course for field office leadership focused on managing intelligence-driven organizations. By staffing the Intelligence Training Program according to its Five-Year Intelligence Training Strategy, the FBI will be able to develop the intelligence workforce that it needs to conduct its national security and criminal missions.

Mission Achievement through Workforce Planning – 47 positions and $12,589,000 ($6,000,000 non-personnel)
The FBI would be incapacitated without the support of personnel dedicated to the forensic analysis of evidence. Professional staff positions are required to address the backlogs of cases and to ensure that the FBI and its partners have the appropriate information when required.

FBI Laboratory Requirements – 2 positions and $3,292,000 ($3,000,000 non-personnel)

Business Process Improvements – $1,000,000 (all non-personnel)
The FBI requests $1,000,000 to support several priority strategic initiatives, including Project Management and Customer/Field Collaboration efforts. The focus of this initiative is the establishment of better discipline around project management and business process improvement through the design, implementation, and execution of a formal project management training and development process. The Laboratory Division will require contract assistance in the implementation of this initiative.

Evidence Tracking System – 2 positions (IT Specialists) $2,292,000 ($2,000,000 non-personnel)
The FBI requests $2,000,000 for continued deployment and O&M of its business intelligence solutions and two positions for full-time system administration, on-site technical support, user training, replacement hardware, data storage and recovery services to operate and maintain the system. The application will track vital information concerning the cycle time evidence spends within the examination process and in transit between units in order to eliminate bottlenecks and objectively analyze the need for additional resources.

Funding

Base Funding

		FY 2009 Enacted				FY 2010 Enacted				FY 2011 Current Services			
Initiative	Program	Pos	Agt	FTE	($000)	Pos	Agt	FTE	($000)	Pos	Agt	FTE	($000)
IT Infrastructure	Connectivity	…	…	…	$…	…	…	…	$…	…	…	…	$…
Intelligence Transformation	Intelligence Transformation	1,171	343	1,171	147,378	1,651	475	1,411	217,342	1,651	475	1,651	224,598
Mission Achievement Through Workforce Planning	Forensic support to all threats*	647	48	595	202,206	644	47	592	216,844	644	47	592	224,216
Total		1,818	391	1,766	$349,584	2,295	522	2,003	$434,186	2,295	522	2,243	$448,814

*Total positions and base funding correspond to the total Laboratory Division base.

Personnel Increase Cost Summary

Initiative	Program	Type of Position	Modular Cost per Position ($000)	Number of Positions Requested	FY 2011 Request ($000)	FY 2012 Net Annualization (change from 2011) ($000)
Mission Achievement Through Workforce Planning	Forensic Support	Information Technology	$146	2	$292	$160
Intelligence Transformation	FIG Collection Management	IA, Field	165	16	2,640	998
Intelligence Transformation	FIG Collection Management	Clerical	91	5	455	35
Intelligence Transformation	FIG Domain Management	IA, Field	165	50	8,250	2,900
Intelligence Transformation	FIG Domain Management	Clerical	91	14	1,274	98
Intelligence Transformation	FIG Domain Management	Information Technology	146	2	292	160
Intelligence Transformation	FIG HUMINT Collection	Agent, Field	287	15	4,305	(720)
Intelligence Transformation	FIG HUMINT Collection	Clerical	91	6	546	42
Intelligence Transformation	FIG HUMINT Collection	Investigative Support	121	4	484	124
Intelligence Transformation	Intelligence Transformation Training and Professional Development	IA, HQ	164	3	492	168
Intelligence Transformation	Intelligence Transformation Training and Professional Development	Clerical	$91	1	91	7
		Total Personnel		118	$19,121	$3,972

Non-Personnel Increase Cost Summary

Initiative	Non-Personnel Item	Unit Cost	Quantity	FY 2011 Request ($000)	FY 2012 Net Annualization (Change from 2011) ($000)
IT Infrastructure	Connectivity	n/a	n/a	$3,000	…
Mission Achievement Through Workforce Planning	Forensic Support	n/a	n/a	3,000	…
	Total Non-Personnel			$6,000	$...

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	2,719	522	2,662	$303,705	$483,899	$787,604	$...
Increases	118	15	59	19,121	6,000	25,121	…
Grand Total	2,837	537	2,721	$322,826	$489,899	$812,725	$...

Item Name: **National Security Threats**

Budget Decision Unit(s): All
Strategic Goal(s) & Objective(s): 1.1, 1.4
FBI SMS Objective: A-01, P-04, P-05, P-06, P-07, T-06, T-07
Organizational Program: Counterintelligence, Intelligence, Critical Incident Response, Laboratory, Criminal Investigative, International OperationsSecurity
End-State Capability: Domain & Operations, Partnerships, Surveillance, Workforce, Infrastructure, Leveraging Technology

Program Increase: Positions 90 Agt 27 FTE 44 Dollars $25,179,000 ($8,275,000 non-personnel)

Description of Item

The FBI requests 90 positions (27 Agents, 32 Intelligence Analysts (IAs)) and $25,179,000 ($8,275,000 non-personnel) to address national security threats. Included are resources to strengthen FBI investigations through the addition of: investigators; intelligence analysts; surveillance resources; Legal Attaché (Legat) resources; and investigative tools. This comprehensive, threat-driven request will enhance capabilities to combat threats to national security and support Investigative Actions to Detect and Disrupt Counterintelligence (CI) threats.

Justification

Threat Summary

The FBI is committed to preventing national security threats at any stage, from thwarting those intending to conduct an act to investigating the financiers of operations. As the lead agency of the nation's counterterrorism (CT) efforts, the FBI must recognize all dimensions of national security threats 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 (Relationship of Increase to Strategic Goals)

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 2012 Net Annualization (Change from 2011) ($000)
Current Services	2,742	1,579	2,742	$395,001	$69,870	$464,871	$...
Increases	90	27	44	16,904	8,275	25,179	342
Grand Total	2,832	1,606	2,786	$411,905	$78,145	$490,050	$342

Item Name: **Weapons of Mass Destruction**

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-04, P-05, P-06, P-07, P-08, P-09, P-11
Organizational Program: Weapons of Mass Destruction, Laboratory, Critical Incident Response Group, Training, Human Resources
End-State Capability: Domain & Operations, Leveraging Technology, Partnerships, Surveillance, Workforce

Program Increase: Positions 35 Agt 15 FTE 18 Dollars $9,141,000 ($2,600,000 non-personnel)

Description of Item
The FBI requests 35 positions (15 agents) and $9,141,000 (2,600,000 non-personnel) to mitigate the Weapons of Mass Destruction threat. The requested resources will reduce the capability gap in the following areas: Counterproliferation, Biological Coverage, Nuclear/Radiological Coverage, and Operations and Response. This request would strengthen the FBI's ability to combat the growing WMD threat.

Justification
Threat Summary

"America's margin of safety is shrinking, not growing."
"The risks are growing faster than our multilayered defenses."

- The World at Risk, The 2008 Report of the Commission on the Prevention of WMD Proliferation and Terrorism.

The WMD threat continues to grow and pose significant danger to the United States. In order to maintain progress in mitigatng 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 Chemical, Biological, Radiological, and Nuclear (CBRN) Materials; and Reduced Controls over Nuclear Materials.

Emerging Threat: Biological Weapons
According to the 2008 WMD Commission Report, a biological WMD attack is anticipated by 2013 "unless the world community acts decisively and with great urgency." Biological weapons are disease-causing microbes (primarily bacterial and viral) and toxins (poisons produced by living organisms). "Dual-use" elements pose significant risks because they are easily obtained and are traditionally used for non-destructive purposes that, unless purchased in very large quantities, go unnoticed. "Dual-use" elements are of particular concern because they can be readily converted into a

WMD. For example, castor beans, the main ingredient in ricin, are used in the food and agriculture industry and in the textile/chemical industry, making them a "dual-use" element. They are used to make products like paper, plastics, rubber, perfumes, cosmetics, electronics, pharmaceuticals, paints, inks, additives, lubricants, and bio-fuels.

DNA synthesis technology continues to advance at a rapid pace. It will soon become feasible to create nearly any virus whose DNA sequence has been decoded – such as smallpox – as well as artificial microbes that do not yet exist in nature. This growing ability to engineer life at the molecular level carries with it the risk of facilitating the development of new and more deadly biological weapons.

The anthrax letters of 2001 demonstrated how devastating biological attacks are. The 15 grams used in these attacks impacted the economy by more than $6 billion and caused 22 people to become sick. Five victims who contracted inhalational anthrax died. The devastation would have been more extensive if a more effective delivery system had been used. The Homeland Security Council modeled a scenario on the effect if terrorists launched a large scale anthrax attack in the United States. Results showed that the effect of anthrax being released in five medium-sized cities would result in 328,848 exposures, 13,208 untreated fatalities, and 13,342 total casualties.

Emerging Threat: Reduced Controls over Nuclear Materials

Experts agree that the risk of a nuclear weapon being used today is growing. This is due in part to the fact that the amount of safeguarded nuclear bomb-making material has grown by a factor of 6 to 10 over the past 20 years while safeguards have not kept pace and the number of International Atomic Energy Agency (IAEA) inspections per facility has actually declined. 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 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/Willis 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.

In order to address the growing threat and ensure the successful discharge of the FBI's WMD-related responsibilities, the following WMD National Program Goals were established:

- Preparedness – Exercise, Training, and Incident Contingency Planning – Produce and sponsor preparedness workshops, training, and exercises enabling FBI personnel and domestic and foreign partners to plan, prepare for, and respond to WMD threats and incidents.
- Countermeasures – Identify and implement targeted initiatives to enhance organizational capability to provide early warning indicators to identify and deny execution by terrorists by detecting and disrupting the movement of WMD, WMD-related materials, recruitment of personnel with WMD training and expertise, and by detecting the support infrastructure for individuals and organizations desiring to acquire WMD.
- Intelligence – Collect, report, analyze, and disseminate WMD specific intelligence to identify gaps and shape requirements regarding the acquisition of WMDs to determine intentions, capabilities, and discover plans to develop or acquire WMD. (Requested resources are merged into the Countermeasures initiative.)
- Investigation, Operations, and Response – Develop operational excellence and leadership to mitigate threats, conduct timely assessments, operations, and investigations to ensure effective crisis response. The FBI will investigate the nature and source of WMD threats, precursors, technologies and materials.

Justification

I. Countermeasures – 16 positions (3 Agents) and $4,970,000 ($2,600,000 non-personnel)

Counterproliferation (CP) Initiatives: 2 positions and $1,664,000 ($1,450,000 non-personnel)

Biological: 9 positions (3 Agents) and $2,021,000 ($400,000 non-personnel)

The FBI is required to respond to the spectrum of bioterrorism concerns as set forth in the National Intelligence Plan, HSPD-10, and HSPD-21. The bioterrorism program currently oversees eight initiatives that focus on prevention. The FBI develops capabilities to identify and detect potential bioterrorism threats, such as the integration of investigative and intelligence resources with public health information and reporting of the theft, loss, and release of dangerous biological agents from laboratories. The FBI also develops capabilities such as Joint Criminal and Epidemiological Investigations to prevent, neutralize, and investigate the threat. The FBI only provides for roughly 25 percent coverage of its targeted 16 initiatives. Growth of the program is critical to ensure adequate coverage is maintained and that foreign partners are fully engaged. The requested positions will enhance the FBI's ability to implement new tripwire efforts with the synthetic biology industry and biological sciences research community, and will provide roughly 35 percent coverage of the 16 initiatives. The non-personnel funding will provide for two contracted SMEs and related travel expenses and supplies for outreach and collaboration efforts. These collaboration efforts will allow the FBI to more

effectively collect, analyze and disseminate intelligence, which will strengthen CONUS and OCONUS partnerships.

Nuclear/Radiological: 5 positions and $1,285,000 ($750,000 non-personnel)
The NSPD-28, HSPD-5, and NSPD-46/HSPD-15 hold the FBI responsible for addressing nuclear and radiological WMD threats. The impact of a nuclear event on the United States or its allies cannot be understated and cannot be ignored. Currently, the FBI is only able to address approximately 20 percent of nuclear program initiatives. The FBI needs to build a team capable of addressing a larger percentage of the nuclear/radiological threat. The requested positions will help alleviate the burden placed on Agents and IAs by some of their initial analysis collection duties. The non-personnel funding will allow the FBI to hire two contracted SMEs. The SMEs will help review and implement tripwires that will increase the awareness of security and response personnel. This gives the FBI a better defense of nuclear sites that perpetrators may target and improves the communication between these sites and associated FBI Field Divisions. The tripwires will serve as an adjunct to an already-established Department of Energy program whose function is to provide hardening of these sites to increase the security of highly radioactive materials, analyze data, attend interagency planning and training exercises, and review and implement national and agency policy, enabling 30 percent coverage of the nuclear program inititives.

II. Investigation, Operations and Response 19 positions (12 Agents) and $4,171,000 (all personnel)

Operations and Response: 19 positions (12 Agents) and $4,171,000 (all personnel)
HSPD-5 and HSPD-8 identify the FBI as the lead agency for preventing, preparing for, and responding to terrorist threats and attacks involving WMD. The FBI plans to deploy 60 WMD Coordinators to the field to coordinate and support these activities. The position of field WMD Coordinator is the key link in the execution of the USG's top national priority – the prevention of the use of a WMD. In furtherance of these efforts, the WMD Coordinator is responsible for WMD response, prevention, outreach, preparedness and program management, as well as the integration of those efforts throughout the USG agencies in their geographic area. The number one FBI WMD priority is prevention. Prevention is achieved via numerous outreach and preparedness activities aimed at critical partners, key infrastructure (18 separate and distinct sectors), technical centers, academia, industry and non-governmental entities. At present, the FBI only provides for roughly 45 percent coverage of the targeted initiatives. To bridge the current capability gap, address the growing threat, and enable 55 percent coverage of the targeted initiatives, the FBI requests personnel to continue to add to its cadre of WMD Coordinators, who will be distributed to the field based on the vulnerabilities and threats in specific areas. The full-time WMD Coordinator enhances liaison relationships, intelligence production, investigation management capabilities, countermeasures and tripwire participation, special event preparation participation, training presentation and participation, and administrative capabilities. Because the WMD Commission anticipates a major WMD event by 2013, the FBI would be remiss if it did not have sufficient WMD Coordinator coverage before that time.

Impact on Performance (Relationship of Increase to Strategic Goals)
The FBI is committed to building and maintaining four critical initiatives designed to combat the growing WMD threat. The Preparedness, Countermeasures, Intelligence and Investigation, and Operation and Response initiatives have been integrated so that they provide a comprehensive, multidisciplinary approach to preventing and, if necessary, responding to a WMD event. These enhancements improve the FBI's ability to fight the WMD threat and therefore improve national security. If the FBI fails to receive any one of these capabilities the FBI would be lagging behind a serious and growing WMD threat.

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

Funding

Base Funding

	FY 2009 Enacted				FY 2010 President's Budget				FY 2011 Current Services			
Program	Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)
Preparedness	131	20	130	$22,466	131	20	130	$28,938	131	20	130	$29,837
Countermeasures	158	38	158	21,560	158	38	158	25,335	158	38	158	25,717
*Investigations, Operations, & Response	869	129	817	289,179	930	166	871	336,705	930	166	878	344,670
**Total	1,158	187	1,105	$333,205	1,219	224	1,159	$390,978	1,219	224	1,166	$400,224

*The Laboratory totals included in the Investigations, Operations and Response represents the entire Lab base .
**The total represents the entire WMD threat base not just the enhancements requested.

Personnel Increase Cost Summary

Initiative	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)
Countermeasures	Counterproliferation Initiatives	Professional Support	107	2	214	60
Countermeasures	Biological	HQ Agent	327	3	981	(18)
Countermeasures	Biological	Professional Support	107	6	642	180
Countermeasures	Nuclear/ Radiological	Professional Support	107	5	535	150
Investigation, Operations and Response	Operations and Response	Field Agent	287	12	3,444	(582)
Investigation, Operations and Response	Operations and Response	Clerical	91	4	364	28
Investigation, Operations and Response	Operations and Response	Investigative	$121	3	363	94

Initiative	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)
		Total Personnel		35	$6,541	($88)

Non-Personnel Increase Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2011 Request ($000)	FY 2012 Net Annualization (Change from 2011) ($000)
Counterproliferation Initiatives	n/a	n/a	1,450	…
Biological	$200	2	400	…
Nuclear Radiological	n/a	n/a	750	…
Total Non-Personnel			$2,600	$…

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	1,219	224	1,166	$162,573	$237,651	$400,224	$…
Increases	35	15	18	6,541	2,600	9,141	(88)
Grand Total	1,254	239	1,184	$169,114	$240,251	$409,365	($88)

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)

Description of Item
Currently, the FBI Render Safe teams are deployed via a specially-configured aircraft whose lease is set to expire in FY 2013. The FBI and the Department of Justice, in consultation with the Office of Management and Budget, are requesting a multi-year phased approach to the acquisition of two planes to replace the current lease and maintain this capability. The phased acquisition of dedicated aircraft represents a more cost effective way to meet the mission requirements than the existing lease.

The outyear requirement for the Render Safe capability is as follows:

	FY 2010	FY 2011	FY 2012	FY 2013	FY 2014 / Outyears
Current Plane Lease	[$14,800,000]	[$14,800,000]	[$14,800,000]	-	-
Aircraft Acquisition	-	35,756,000	-	-	-
Aircraft Outfitting	-	-	38,500,000	-	-
Aircraft O&M	-	-	13,100,000	13,100,000	13,400,000
Non-Personnel Total		**35,756,000**	**51,600,000**	**13,100,000**	**13,400,000**
Personnel [13 positions (6 Agents)]		**4,244,000**	**3,655,000**	**3,999,000**	**3,999,000**
TOTAL / ANNUAL REQUIREMENT		**40,000,000**	**55,255,000**	**17,099,000**	**17,399,000**

Justification
Two specially configured aircraft capable of an immediate response are required, for which $35,756,000 will fund acquisition and provide a turn-key air operations support program with around-the-clock crew and maintenance.

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.

Funding

Base Funding

FY 2009 Enacted				FY 2010 President's Budget				FY 2011 Current Services			
Pos	Agt	FTE	($000)	Pos	Agt	FTE	($000)	Pos	Agt	FTE	($000)
92	20	92	$28,513	106	28	99	$51,788	106	28	106	$51,788

Personnel Increase Cost Summary

Initiative	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)
Render Safe Capability	Hazardous Devices Response Unit	HQ Agent	$327	4	$1,308	($24)
Render Safe Capability	Explosives Unit	HQ Agent	327	2	654	(12)
Render Safe Capability	National Assets Response Unit	Non-Agent Responder	326	3	978	(237)
Render Safe Capability	Hazardous Materials Response Unit	Non-Agent Responder	$326	4	1,304	(316)
Total		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	$37,586	$51,788	$…
Increases	13	6	6	4,244	35,756	40,000	(589)
Grand Total	119	34	112	$18,446	$73,342	$91,788	($589)

Item Name: **Violent Crime/Gangs**

Budget Decision Unit(s): All
Strategic Goal(s) & Objective(s): 1.2, 2.1, 2.2
FBI SMS Objective: P-06
Organizational Program: Laboratory
End-State Capability: Domain & Operations

Program Increase: Positions 2 Agt 0 FTE 1 Dollars $328,000 (all personnel)

Description of Item
The FBI requests 2 positions and $328,000 (all personnel) to address the Violent Crime threat. This request would reduce the gap between capabilities and requirements in Indian Country (IC) crime. Indian Country-related crimes can be linked to Southwest Border (SWB) violence due to alliances that are forming among U.S.-based gangs and criminals with drug trafficking organizations (DTOs) along the SWB. This initiative would also strengthen the FBI's capability for criminal data sharing support to our law enforcement partners.

In addition, the FBI requests 81 positions (45 agents) and $18,890,000 ($1,700,000 non-personnel) as a reimbursable program through the Department of the Interior to support violent crimes within Indian Country.

Justification

Indian Country

Threat Summary
Twenty-five percent of all violent crimes prosecuted by United States Attorneys occur on Indian Reservations. As of March 26, 2009, the FBI had 2,368 pending cases, of which 75 percent involved homicides, sexual/physical abuse of children, rape, and aggravated assault. Few long-term financial investigations associated with Indian Gaming are initiated due to the amount of resources required.

According to DOJ, the violent crime rate among Native Americans (age 12 and older) is at least 2 ½ times the national average outside the Native American race group. Furthermore, more than one-third of all Native American women are likely to be raped at least once during their lifetimes, and nearly two-thirds will be victims of violent assaults. IC is served by half as many police officers as similarly situated rural areas, and police emergency response can be up to 1-1½ hours, compared to a national average of 6 minutes.

Forty-one Indian reservations are located within a 100 mile radius of the Mexican or Canadian borders, making them easily accessible to international drug and alien smugglers. A 2008 Drug Threat Assessment conducted by the National Drug Intelligence Center noted that Mexican Drug Trafficking Organizations (DTOs) are the

principal wholesale suppliers and producers of illicit drugs available in IC, including northern United States reservations, and pose the greatest organizational threat nationally to Native American communities. Native American participants in these criminal networks initially started as lower level transporters but have now risen to leadership roles by drawing on their knowledge of local terrain and by exploiting jurisdictional issues. This criminal activity has spurred the influx and development of gangs and gang activity on reservations.

Justification for Increases to Address Crimes in Indian Country – 2 positions and $328,000 (all personnel)
Forensic Support – 2 positions and $328,000 (all personnel)
The FBI requests two Forensic Examiners to support Indian Country program operations and investigations. Forensic examinations involve nearly every Laboratory discipline, including chemistry, cryptanalysis, DNA, and trace evidence. Field agents collect DNA samples during Indian Country investigations, which are then sent to the FBI Laboratory for forensic examinations. With the average turnaround time of about 164 days to process and analyze those samples, the intelligence and lead generation value they provide is often useless by the time they are completed. Since October 2005, the Laboratory has received 1,124 submissions from Indian Country investigations. Of those submissions, the Laboratory has completed 880 with an average turn-around time of 164 days; of the nearly 250 remaining submissions, the average pending time is 219 days.

Impact on Performance (Relationship of Increase to Strategic Goals)
Failure to enhance the FBI's forensic capabilities will affect the timeliness of Indian Country program operations and investigations. Intelligence and lead information could be either unavailable or useless by the time forensic examinations are completed. As a result, field investigators will spend unnecessary time pursing negative avenues of investigative inquiry that otherwise would have been eliminated on the basis of forensic examination. Due to the lack of disruption of activity, violence will continue in the reservations for longer periods of time. The additional positions requested will allow the FBI to maintain an average of 60-day turnaround time for forensic examinations in Indian Country program cases, which is also desirable for prosecutorial purposes.

Funding

Base Funding

	FY 2009 Enacted				FY 2010 President's Budget				FY 2011 Current Services			
Program*	Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)
Lab	647	48	595	202,206	644	47	592	216,844	644	47	592	224,216
Total	647	48	595	202,206	644	47	592	216,844	644	47	592	224,216

Note:
. Laboratory resource totals represent the entire Laboratory program, not just the VC/Gangs-related functions.

Personnel Increase Cost Summary

Initiative	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)
Indian Country	Forensic Support	Forensic Examiner Scientist	164	2	328	72
Grand Total				2	$328	$72

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	644	47	592	$88,845	$135,371	$224,216	$ …
Increases	2	0	1	328	…	$328	72
Grand Total	646	47	593	$89,173	$135,371	$224,544	$72

Item Name: **Child Exploitation**

Budget Decision Unit(s): All
Strategic Goal(s) & Objective(s): 2.3
FBI SMS Objective: P-04, P-07, A-02
Organizational Program: Criminal, Laboratory, Operational Technology, Training
End-State Capability: Domain & Operations, Leveraging Technology, Partnerships, Workforce

Program Increase: Positions 20 Agt 4 FTE 10 Dollars $10,838,000 ($6,242,000 non-personnel)

Description of Item
The FBI requests 20 positions (4 Agents and 1 Intelligence Analyst (IA)) and $10,838,000 ($6,242,000 non-personnel) to enhance child exploitation investigations and prevent child predator advances. Resources in this request will support the FBI's Innocence Lost, Child Sex Tourism, and Innocent Images initiatives.

Justification
Threat Summary
According to the Bureau of Justice Statistics, child sex offenses were among the fastest growing offenses of the federal criminal caseload from 1994 to 2006, with an 82 percent increase. The FBI has the primary federal jurisdiction to investigate these crimes.

Child Prostitution
Everyday, 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.

These pimps portray themselves to the children as "boyfriends" and manipulate young girls and boys into trusting them and depending on them for their survival. Once they have gained control over the children, pimps force them into prostitution. One child who initially refused to work the streets, for example, was gang-raped by a pimp and his friends. The rape was videotaped, and the child was told it would be distributed on the Internet if she did not comply with the pimp's demands that she work as a prostitute for his financial gain. This type of violence is commonly inflicted on child victims. One girl, who was rescued by an Innocence Lost task force operation, reported that her pimp held her at gunpoint while he ran a potato peeler down her face to ensure she was scarred for life physically as well as emotionally. On average, a child's life expectancy is only seven years after entering into prostitution.

There are no verifiable estimates of the number of prostituted children in the United States, but one study by the University of Pennsylvania put the number as high as 300,000. Child runaways represent the greatest number of youth who are at risk to being lured into prostitution by a pimp. The National Center for Missing and Exploited Children (NCMEC) generated 10,537 endangered runaway reports in FY 2008, up significantly from previous years. In past years, 14 percent of the missing and endangered runaway reports received by NCMEC were children who were believed to be involved in prostitution. These children are viewed as some of the most vulnerable of victims of sexual exploitation in that they are often searching for safety from sexual and physical abuse.

Child Sex Tourism

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. Internet chat rooms, message boards, and online organizations have been observed giving detailed instructions on how to partake in sex tourism. United States citizens are among those from several wealthy countries who exploit children overseas. The non-government organization (NGO) known as End Child Prostitution, Child Pornography, and Trafficking of Children for Sexual Purposes (ECPAT), reports that approximately 25 percent of the sex tourists who abuse children while traveling abroad are American. From June 11, 2005 to April 10, 2006, there were 19,897 visitors to an undercover website ran by the FBI that purported to facilitate sex tourism. Internet protocol (IP) addresses from the United States accounted for over 60 percent of the total visitors to the website.

Each day, sexual predators from the United States travel abroad in order to procure children in foreign countries for sexual purposes. These offenders believe that they can commit a crime against a child with immunity abroad because they feel they are no longer subject to United States law, that they are "anonymous" while traveling abroad, that they can claim ignorance of local laws, and that the local population would be reluctant to report such crimes to law enforcement. Some offenders even rationalize that they are "helping" prostituted children by providing them with a source of income, and that sex between adults and children is socially acceptable in the victim child's culture. The victims of this crime are generally impoverished children who must join the workforce at an early age to help support their families.

Children from impoverished families are often lured away by recruiters with promises of jobs in the city; only to be forced into prostitution. These children are far away from their homes with no means of support or escape. They are entirely dependent upon their captors for sustenance. If they refuse to participate in prostitution, they are refused food and water, beaten, and possibly killed.

Numerous countries in Southeast Asia are so well-known for child sex tourism that there are entire neighborhoods which are considered brothels and open-air markets where children can be purchased for sex. The International Labour Organization reported that 2-14% of the gross domestic product of Indonesia, Malaysia, the Philippines, and Thailand derives from sex tourism. These countries have long been prime destinations for child sex tourists, but now child sex tourists are traveling to Mexico and Central America as well. Children are sold to pimps by their own families because of extreme poverty, and sex acts between adults and children can be witnessed in public places such as bars and restaurants.

ECPAT estimates that there are two million children worldwide victimized as child prostitutes. As many as one-third of the approximately 800,000 prostitutes in Cambodia are children. One indicator of the prevalence of child sex tourism is the comparative cost of an adult prostitute as opposed to a child. In Cambodia and Thailand, children are available for sex for as little as a few dollars; the same price as for adults prostitutes.

The effects of child sex tourism reach beyond the shattered lives of children overseas. In countries like Cambodia, Thailand, Philippines, Costa Rica and Mexico, where the largest child sex tourism crime problems exist, the plurality of perpetrators are from the United States. The prominence of child sexual abuse by United States citizens paints a despicable portrait of American tourists among local populations in those countries, and fosters anti-American sentiment.

Innocent Images

In 2006, child pornography made up 69 percent of the sex offenses referred to the United States Attorneys. The FBI has the primary federal jurisdiction to investigate these crimes. Computer telecommunications are one of the most prevalent techniques used by pedophiles to share illegal photographic images of minors and to lure children into illicit sexual relationships. The Internet has dramatically increased the access of the preferential sex offenders to the population they seek to victimize and provides them greater access to a community of people who validate their sexual preferences. For example, NCMEC reports that one-third of child pornography possessors were known to also distribute child pornography. The United States Postal Inspection Service (USPIS) estimates that at least 80 percent of purchasers of child pornography are also actively abusing children. According to the Association for the Treatment of Sexual Abusers, pedophiles, especially those who molest boys or both boys and girls, have the highest rate of recidivism among criminals after incarceration and/or treatment.

The Internet has become the most prevalent technique used by child predators to network with one another, to produce, purchase and share child sexual exploitation material (CSEM), and to lure children into sexual relationships. It also has dramatically increased the preferential child predator's access to the population they seek to victimize and also provides them with greater access to a like-community of people who validate their sexual preferences. The Internet has become a marketplace for child sex offenders to exchange CSEM or even children. In a recent case, a mother offered to sell her five year old daughter to child pornographers she had found on the Internet in exchange for a used

car and an apartment. Online exchanges between the child's mother and buyer discussed how, if bought, the five year old child would be forced to cut herself and bleed while performing sexual acts.

Additionally, child sex offenders have developed secret Internet networks where they discuss "best practices" on how to successfully sexually exploit children and avoid law enforcement intervention. These networks are also used to produce and share erotic stories, images, and movies involving their victims.

By far, some of the most egregious offenders are those criminal organizations who promote the production of CSEM for profit. Several countries in Eastern Europe are notorious for the proliferation of CSEM websites, which sell CSEM produced within and outside of Eastern Europe. The production and distribution of CSEM is a business for these criminal organizations, and they enter this business for profit, and as a way to steal identities of the subscribers. Children are sexually abused and images and/or videos are produced of those children, by said criminal organizations, for profit. When these websites are identified, infiltrated, and investigated by law enforcement, the majority of the subscribers are overwhelmingly identified through investigation as American citizens. The United States is the largest market for CSEM in the world. Just as with any other product, if it is a product that is in high demand, the market will provide the buyers. So it is, unfortunately, with CSEM.

In the United States, a significant number of offenders develop their own online contacts within and outside of the United States. Most groups are not well concealed, but recent and emerging trends have shown that offenders are becoming more sophisticated in their methodology and have created secretive groups in order to facilitate the distribution of CSEM, as well as the on-demand production of CSEM.

The FBI is encountering the next generation of peer-to-peer file sharing programs, which pose the highest challenge to law enforcement charged with investigating online child exploitation. One such application allows users to share entire hard drives of data (as opposed to individual files) with an invitation-only group of other users via an encrypted network. Child pornographers can have as many as 1,000 other users join their secure network and access their child abuse images and movies. There is no limit to the number of files and/or file sizes shared within such a network. The service is entirely free and accessible to anyone with an Internet-connected computer. The FBI's Innocent Images Operations Unit (IIOU) is conducting investigations of users of this service. In one phase of investigation, three of 21 subjects were found to be registered sex offenders or have had a prior sex offense against a child. These 21 subjects admitted to actively abusing 7 children. Thus, these applications are not only being used by mass distributors of child pornography, but also by producers of child pornography and repeat child sex offenders.

Justification

I.) Innocence Lost Initiative – 10 positions and $6,946,000 ($4,236,000 non-personnel)

Forensic Examiner Enhancement – 10 positions and $2,710,000 (all personnel)
The Digital Evidence Forensic Support Program requires 10 additional Computer Analysis Response Team (CART) Examiners in order to help CART keep pace with the growing number of requests for digital forensic examinations related to child exploitation investigations, the largest contributor to CART's digital forensics requests. These positions will be strategically deployed to FBI Field Offices with the largest percentage of child exploitation requests or specialty operations to ensure adequate support.

Regional Computer Forensic Laboratory (RCFL) Field Infrastructure –$4,236,000 all non-personnel)
To support the increasing demands of the law enforcement community for digital forensics services in combating child exploitation, the FBI requests additional funding to establish a new RCFL. There are two regions that have the highest risk of child exploitation that do not have an RCFL in the region to provide digital forensic support. These two regions are the Southeastern United States and Hawaii. The final decision for the RCFL will be made based on the location with the greatest risk and an evaluation of return on investment.

The following criteria were utilized to support the recommendation for one RCFL in the Southeastern United States:

- The RCFL program has a complete lack of service coverage in the Southeast, an area encompassing a total of seven states with a total population of approximately 55.6 million people.
- Numerous statistics justify the need for additional support for criminal investigations, especially for child exploitation cases in the Southeast.
- CART Examiners in the Southeast processed over 126 terabytes of data. This represents nearly 20 percent of all child exploitation exams processed by CART/RCFLs in FY 2008.

The following criteria were utilized to support the recommendation for one RCFL in Hawaii:

- In the FY 2008 RCFL site selection process conducted by the RCFL National Program Office (NPO), the Honolulu Field Office scored 4th out of the 11 proposals received. Hawaii (HI) offered a strong proposal for an RCFL with extremely strong support from their proposed participating agencies including the HI State Attorney General's office, which created the Hawaii Internet and Technology Crimes (HiTEC) unit, specifically charged with addressing child exploitation cases.
- Hawaii's unique geographic location makes it a gateway with direct access to over 40 international destinations, many of which have high incidence of child exploitation.

<u>II.) Child Sex Tourism – 8 positions (4 Agents and 1 IA) and $3,621,000 ($2,006,000 non-personnel)</u>
*Child Sex Tourism Investigations – 8 p*ositions *(4 Agents and 1 IA) $3,115,000 ($1,500,000 non-personnel)*

The requested resources are needed to address the sexual exploitation of children by United States citizens overseas. The development of intelligence and implementation of undercover operations will be utilized to combat this threat. The non-personnel funding will support case expenditures and operational travel.

The FBI has had limited success in creating domestic undercover operations to target child sex tourism offenders. The undercover operations initially generated dozens of convictions, but have experienced decreased activity as the *modus operandi* of offenders has become more sophisticated in recent years. Information on procuring children in foreign destinations is readily available on the Internet, and most offenders do not need the "services" that the domestic undercover operations offer. Like-minded offenders use chat rooms, message boards, and web sites devoted to sex tourism to exchange information on potential child sex tourism destinations. Once in the country of destination, a child sex tourist may also solicit the assistance of local taxi drivers, newspaper classified ads, bar and restaurant staff, and guesthouse and hotel workers to gain access to children in prostitution. These developments highlight the need for the FBI to devote resources to establishing in-country initiatives in child sex tourism destination countries in order to effectively combat the crime problem.

With the requested enhancements, Agents would be tasked with investigating the child sex tourism threat in countries that have been identified as main destinations for child sex tourists, specifically Cambodia, Thailand, Philippines, Honduras and Costa Rica. The Agents would form working groups with foreign law enforcement, as well as non-government organizations that conduct in-country research on child sex tourism. It is anticipated that this increase in personnel would result in 30 convictions and the identification of 50 child victims in Thailand and Cambodia.

International Training – $506,000 (all non-personnel)
The mission of the FBI's International Training and Assistance Unit (ITAU) is to develop and deliver effective law enforcement training programs for police in the international arena in order to combat and prevent, among other matters, child exploitation. The training is also designed to put FBI Agents in personal contact with their host-nation interlocutors, to increase the FBI's liaison and operational capabilities.

FBI Legal Attaché personnel across the world have worked with the ITAU to assess the abilities of the law enforcement personnel in their various jurisdictions and countries. Although foreign law enforcement personnel possess basic skills in these areas, in order to become effective investigators and team with the FBI on future cases, training courses will need to be held on an annual basis to instruct law enforcement personnel. The funding requested here would enable the FBI to increase the number of bilateral training courses that it conducts for foreign law enforcement. This includes the purchase of equipment directly used to support international training, such as translation equipment for simultaneous interpretation. Funding will also be used for the payment of FBI National Academy international re-trainers.

<u>III.) Innocent Images National Initiative (IINI) – 2 positions and $271,000 (all personnel)</u>

Forensic Evidence Analysis – 2 positions and $271,000 (all personnel)
IINI operations and investigations require forensic support from nearly every Laboratory discipline, from chemistry to DNA to trace evidence. Most examinations in support of IINI involve processing trace evidence and DNA samples collected by Field Agents during the course of their investigations. With the increase in child exploitation threats, the FBI has not been able to keep up with forensic examinations in a timely manner to support the investigation and prosecution of sexual predators. Since October 2005 the FBI Laboratory has received 443 submissions related to child exploitation investigations; to date, 62 of those submissions are still pending. The average age of a child exploitation pending submission is 303 days.

Impact on Performance (Relationship of Increase to Strategic Goals)

Failure to receive the requested enhancements will negatively impact the FBI's ability to prevent, suppress, and intervene in crimes against children. Without the requested resources, the FBI will not be able to uphold its investigatory capabilities as child exploitation offenses continue to grow. Without sufficient resources to address this threat, the FBI cannot effectively and efficiently achieve its mission of identifying and neutralizing child predators if it does not have Agents in positions to combat the threats in its domain.

Funding

Base Funding

	FY 2009 Enacted				FY 2010 President's Budget				FY 2011 Current Services			
Program*	Pos	Agt	FTE	($000)	Pos	Agt	FTE	($000)	Pos	Agt	FTE	($000)
Criminal – Child Sex Tourism	23	15	23	4,655	23	15	23	4,718	23	15	23	4,782
Lab	647	48	595	202,206	644	47	592	216,844	644	47	592	224,216
Operational Technology	69	10	69	53,323	101	10	103	59,328	124	10	129	89,183
Training	20	10	20	3,469	20	10	20	3,538	20	10	20	4,134
Total	759	83	707	$263,653	788	82	738	$284,428	811	82	764	$322,315

*Notes
1.) Laboratory resource totals represent the entire Laboratory program, not just the Child Exploitation-related functions.
2.) Operational Technology base funding is for the entire program, as OTD programs are not tracked by threat

Personnel Increase Cost Summary

Initiative	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)
Child Sex Tourism	Investigations	Clerical	$91	2	$182	$14
Child Sex Tourism	Investigations	Intelligence Analyst, HQ	164	1	164	56
Child Sex Tourism	Investigations	Investigative Support	121	1	121	31
Child Sex Tourism	Investigations	Special Agent, Field	287	4	1,148	(192)
Innocence Lost Initiative	Digital Forensics	CART Examiner	271	10	2,710	380
Innocent Images Initiative	Forensic Support	Forensic Examiner Scientist	164	1	164	36
Innocent Images Initiative	Forensic Support	Professional Staff	107	1	107	30
		Total Personnel		20	$4,596	$355

Non-Personnel Increase Cost Summary

Initiative	Non-Personnel Item	Unit Cost	Quantity	FY 2011 Request ($000)	FY 2012 Net Annualization (Change from 2011) ($000)
Child Sex Tourism	International Training	n/a	n/a	506	…
Innocence Lost Initiative	Digital Forensics	n/a	n/a	4,236	…
Innocence Lost Initiative	Investigations	n/a	n/a	1,500	…
	Total Non-Personnel			$6,242	$ …

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	811	82	764	$162,431	$159,884	$322,315	$…
Increases	20	4	10	4,596	6,242	10,838	355
Grand Total	831	86	774	$167,027	$166,126	$333,153	$355

Item Name: **Organized Crime**

Budget Decision Unit(s): All
Strategic Goal(s) & Objective(s): 1.1, 1.2, 2.2, 2.5
FBI SMS Objective: P-04, P-07, P-09
Organizational Program: Criminal Investigative, Laboratory, Intelligence
End-State Capability: Domain & Operations

Program Increase: Positions 4 Agt 3 FTE 2 Dollars $952,000 (all personnel)

Description of Item
International organized crime represents a significant challenge to the FBI due to the sophistication and diversity of criminal enterprises and the ease of communication and movement between country borders. This initiative, in cooperation with the Attorney General's Organized Crime Council, seeks additional staff to combat criminal enterprise activities that have spread to the United States from the rest of the world. To combat this problem, the FBI requests 4 positions (3 Agents, one clerical position and $952,000) to enhance the mobile investigative teams (MITs).

Justification
Threat Summary
Organized Crime in the United States, at one time associated primarily with La Cosa Nostra (LCN), has changed dramatically over the past two decades. Although the LCN remains a viable threat requiring FBI resources, International Organized Crime (IOC) groups represent a significant challenge due to their sophistication, diversity, and ease of communication and movement. These new, emerging foreign-based enterprises originate in Eurasia, Asia, and Africa and represent both a criminal and national security threat to the United States.

To combat this threat, in February 2009 the FBI developed an Organized Crime Program (OCP) Plan. It is designed to support the FBI's, as well as the Department of Justice's (DOJ) 2008 Organized Crime (OC) Threat Assessment and OC Strategy, and provides guidance to the field, supporting divisions, and other FBI entities. Supporting the OCP are the following eight DOJ International Organized Crime Threats, which were established based on analyses conducted by the FBI and the DOJ Criminal Division:

International organized criminals are penetrating the energy sector and other strategic sectors.

International organized criminals are providing support to foreign governments, intelligence services, and terrorists.

International organized criminals are subverting the integrity of national borders.

International organized criminals exploit the United States and international financial system to move illicit funds.

International organized criminals use cyberspace to target United States victims and infrastructure.

International organized criminals are manipulating securities exchanges and perpetrating sophisticated frauds.

International organized criminals corrupt and seek to corrupt public officials in the United States and abroad.

International organized criminals use violence and the threat of violence as a basis for power.

To address these threats, the FBI needs to pursue leads by opening more investigations. Cooperative foreign law enforcement organizations and FBI Legats provide a litany of information to the FBI.

The FBI's Organized Crime Section (OCS) is divided into three units (La Cosa Nostra/Italian Organized Crime, Asia/Africa Organized Crime, and Eurasian Organized Crime) which address new and emerging organized crime threats. Even though crimes are separated by region, the methods to mitigate them are relatively the same — more intelligence and more "boots on the ground."

Justification

In an effort to modernize the law enforcement approach to combating international organized crime, the Attorney General's Organized Crime Council (AGOCC) adopted a unified Law Enforcement Strategy to Combat International Organized Crime. In FY 2011, the Council seeks to implement the strategy via the FBI and other Department of Justice components. The FBI will implement its responsibilities under the strategy through the use of MITs.

Agents assigned to MITs will investigate money laundering schemes and help implement the nine goals of the 2007 National Money Laundering Strategy.

1. Continue to safeguard the banking system;
2. Enhance financial transparency in money services businesses;
3. Stem the flow of illicit bulk cash out of the United States;
4. Attack trade-based money laundering at home and abroad;
5. Promote transparency in the ownership of legal entities;
6. Examine anti-money laundering regulatory oversight enforcement at casinos;
7. Implement and enforce anti-money laundering regulations for the insurance industry;
8. Support anti-money laundering capacity building and enforcement efforts; and
9. Improve how we measure our progress.

Of particular note is the FBI's role in goal seven. The FBI developed a working group to focus on service providers that form companies on behalf of offshore criminal interests. The working group will develop leads and work with domestic and foreign law enforcement agencies to combat those criminal entities operating through shell companies.

The mobile teams will have the ability to move anywhere money laundering networks are active in the United States and abroad.

Impact on Performance (Relationship of Increase to Strategic Goals)
This request supports DOJ Strategic Goal 2: Prevent Crime, Enforce Federal Laws and Represent the Rights and Interests of the American People. These enhancements will allow the FBI to improve the quality and number of investigations against targets of strategic interest to the United States. Resources will be dedicated to identify and analyze criminal intelligence, increase investigations against key organized crime targets and will result in greater disruptions and dismantlements. In addition, finished strategic intelligence products are an FBI priority as the FBI continues to strive towards comprehensive domain threat assessments.

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

Funding

Base Funding

FY 2009 Enacted				FY 2010 President's Budget				FY 2011 Current Services			
Pos	Agt	FTE	$(000)	Pos	Agt	FTE	($000)	Pos	Agt	FTE	($000)
656	618	656	$108,686	656	618	656	$110,807	656	618	656	$114,575

Personnel Increase Cost Summary

Type of Position	Modular Cost per Position ($000)	Number of Positions Requested	FY 2011 Request ($000)	FY 2012 Net Annualization (change from 2011) ($000)
Agent	$287	3	$861	($192)
Clerical Support	91	1	91	7
Total Personnel	$378	4	$2,168	($185)

Non-personnel Increase Cost Summary

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

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	656	618	656	$111,832	$2,742	$114,574	$...
Increases	4	3	2	952	…	952	(185)
Grand Total	660	621	658	$112,784	$2,742	$115,526	($185)

VI. Program Offsets by Item

Item Name: **Travel**
Budget Decision Unit(s): All
Strategic Goal(s) & Objective(s): 2.1, 2.2
Organizational Program: Various FBI Programs

Program Reduction: Positions 0 Agt 0 FTE 0 Dollars ($10,282,000)

Description of Item
This proposal reduces FBI travel funding. This also includes travel for operational requirements as well as conferences and educational functions.

Summary Justification
The Department is continually evaluating its programs and operations with the goal of achieving across-the-board economies of scale that result in increased efficiencies and cost savings. In FY 2011, DOJ is focusing on travel as an area in which savings can be achieved. For the FBI, travel or other management efficiencies will result in offsets totaling $10.3 million.

Impact on Performance (Relationship of Reduction to Strategic Goals)
This offset will be applied in a manner that will allow the continuation of effective law enforcement program efforts in support of the Administration's goals, while minimizing the risk to health, welfare, and safety of agency personnel.

Item Name: **Cyber Education and Development**

Budget Decision Unit(s): Counterintelligence/Counterterrorism and Criminal Enterprises Federal Crimes
Strategic Goal(s) & Objective(s): 1.1, 1.2, 2.3, 2.5
Organizational Program: Cyber

Program Reduction: Positions 0 Agt 0 FTE 0 Dollars ($3,200,000)

Description of Item
The FBI seeks to expand its investigatory capabilities in order to meet projected increases in cyber intrusions as technology becomes more sophisticated and intrusions more frequent. Cyber courses educate investigators on current technologies, computer system operations, network vulnerabilities, and the methods used in intrusions, with a particular focus on intrusions with a national security nexus.

Summary Justification
Improvements in information technology and online training programs have created opportunities to reduce training costs by reducing costs of delivery. Because of this, the FBI proposes to reduce cyber training funding.

Impact on Performance (Relationship of Reduction to Strategic Goals)
The goal of protecting the American public and the private sector from cyber attacks will not be unduly compromised by this proposed decrease.

Item Name: **Vehicles**
Budget Decision Unit(s): All
Strategic Goal(s) & Objective(s): 2.1, 2.2
Organizational Program: Facilities and Logistics Services

Program Reduction: Positions 0 Agt 0 FTE 0 Dollars ($3,788,000)

Description of Item
The Energy Policy Act of 1992 requires that 75 percent of all covered light-duty vehicles acquired for Federal fleets in FY 1999 and beyond be alternative fuel vehicles (in fleets of 20 or more vehicles). Executive Order (E.O.) 13223, *"Strengthening Federal Environmental Energy, and Transportation Management"* requires the purchase of alternative fuel, hybrid, and plug-in electric vehicles when commercially available.

Summary Justification
Each year, FBI requests replacement of worn-out, old and damaged vehicles. The FBI has implemented the purchasing of fleet vehicles that are more fuel efficient and environmentally friendly in order to meet the goals of the Energy Policy Act and E.O 13223. However, in an effort to save costs in FY 2011, FBI will forego the purchase of approximately 100 hybrid vehicles.

Impact on Performance (Relationship of Reduction to Strategic Goals)
This proposed reduction will extend the time necessary for FBI to replace its current vehicle fleet with more fuel-efficient hybrids. The impact on agency performance should be minimal. Other light, medium, and heavy duty vehicles (e.g., vans, armored vehicles, etc) are not impacted by this proposal.

Item Name:	**Rescission of Prior Year TEDAC Appropriations**
Budget Decision Unit(s):	N/A
Strategic Goal(s) & Objective(s):	1.1, 1.2
FBI SMS Objective(s):	T-05, T-07
Organizational Program:	Laboratory
Program Reduction:	Positions … Agt …FTE … Dollars ($98,886,000) (all non-personnel)

Description of Item

Congress has appropriated a total of $116 million to date for the construction of a permanent facility to house the Terrorist Explosive Device Analysis Center (TEDAC). The Administration proposes to rescind $98,886,000 from unobligated construction balances. At the time of the budget transmission, the FBI was assessing final TEDAC project expenditures. Outstanding obligations may affect the amount available for rescission.

Justification

The Administration has never requested funds for TEDAC construction. The FBI is currently addressing the high priority explosives analysis needs of its primary customer, the Department of Defense (DOD). DOD is developing capabilities to analyze lower priority explosives in theater.

Impact on Performance (Relationship of Increase to Strategic Goals)

This rescission does not reduce funding for operations of the FBI's laboratory facilities in Quantico, VA. FBI labs will continue to provide explosives analysis. Additionally, the Deputy Attorney General recently coordinated a meeting between the FBI and ATF, complementing the ongoing efforts of DOJ's Joint Program Office, to improve explosives coordination, analysis, information sharing, and training between Federal, State, and local law enforcement partners. The proposed rescission will reduce funds supporting DOJ Strategic Goal 1, "Prevent Terrorism and Promote the Nation's Security."

Funding

Base Funding

FY 2009 Enacted (w/resc./supps)				FY 2010 Enacted				FY 2011 Current Services			
Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)
…	…	…	$41,000	…	…	…	$30,000	…	…	…	$...

Non-Personnel Decrease Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2011 Request ($000)	FY 2012 Net Annualization (Change from 2011) ($000)
Rescind TEDAC prior year appropriations	n/a	n/a	($98,886)	$…
Total Non-personnel			($98,886)	$…

Total Request for this Item

	Pos	Agt	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)
Current Services	…	…	…	$…	$0	$0
Decreases	…	…	…	…	($98,886)	($98,886)
Grand Total	…	…	…	$…	($98,886)	($98,886)

Initiative Name: **Operational Enablers: Facilities Infrastructure**

Strategic Goal(s) & Objective(s): 1.1, 1.4, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6
FBI SMS Objective(s): T2, T5, T7
Organizational Program: Facilities & Logistics
End-State Capability: Infrastructure

Program Increase: Positions … Agt … FTE … Dollars $73,892,000 (all non-personnel)

Threat Summary

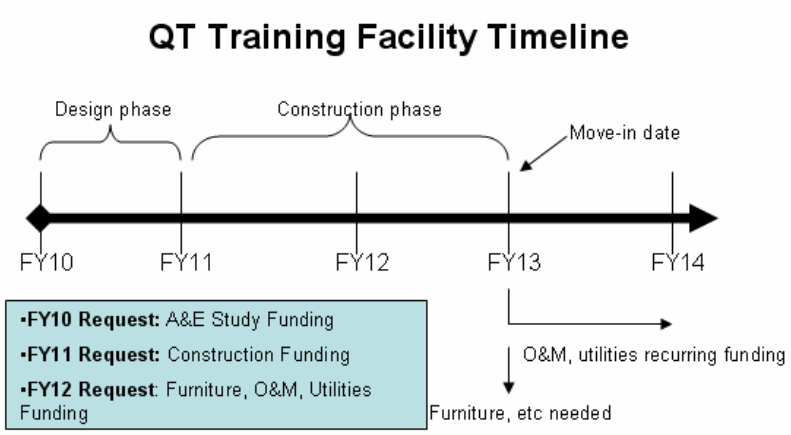
Although both the FBI Academy's role in the training of personnel and the number of personnel to be trained have greatly expanded, the required facilities have not been upgraded or enlarged to match this growth in personnel. This has caused the Academy training requirements to routinely exceed its maximum capacity and in many cases either delay or cancel critical training. The original buildings have not undergone major renovations/upgrades since their construction in 1972. The infrastructure and many structures and pieces of equipment are well past their serviceable life and are a severe burden on the Academy's modest maintenance and renovation budget.

Justification

Facilities Infrastructure – $73,892,000 (all non-personnel)
The FBI plans to expand and renovate several facilities at the FBI Academy.

The FBI Academy Training Facility - $67,605,000 (all non-personnel)
With the extensive growth of the FBI's mission and workforce since 9/11, the Academy has lacked the required training and housing capacity to accommodate this growth, thereby necessitating the use of temporary classroom structures at Quantico or in private sector space, with students being housed in local area hotels. These undesirable stop-gap arrangements come at a high price to the FBI's budget, mission, and the resultant amount and quality of training. To address this lack of capacity, the FBI requests $67,605,000 to expand its training facilities at the FBI Academy on the Quantico Marine Corps Base by constructing a new dormitory and classroom building. Expansion of the existing facilities would generate cost savings of approximately $15,187,500 per year by accommodating students on campus rather than at off-site private hotels. Housing students on campus also results in a dramatically more efficient use of student time when the daily commute to and from the campus is eliminated. In advance of official Architecture and Engineering (A&E) cost estimates, it is anticipated that this facility would include:

- 325 rooms (650 beds)
- 12 secure classrooms (50 students each)
- 200 student conference room
- 700 student cafeteria (dining hall and kitchen)

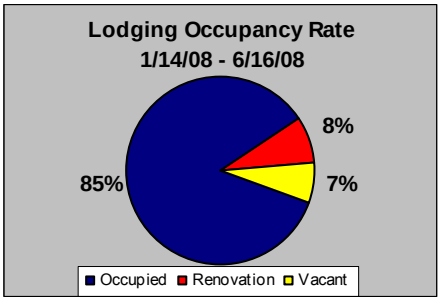


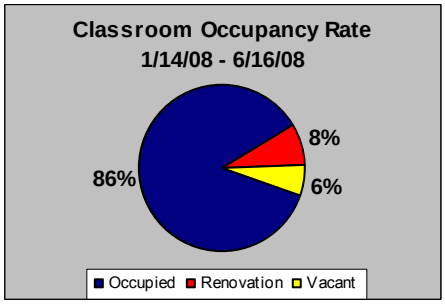
In addition to the increased number of students, the length of the training programs necessary for New Agents and IAs has been extended. This has significantly increased the total training weeks per year – by more than 90 percent since 1995 – and creates severe scheduling (classroom and lodging) constraints at the Academy. The chart below shows the combined impact of the increase in workforce size and longer classes to train New Agents and IAs:

	NEW AGENTS			IAs - IBC			
Year	# Agents Trained	Length of Training in Weeks	Training Weeks Per Year*	# IAs Trained	Length of Training in Weeks	Training Weeks Per Year*	TOTAL NAT/IA TRAINING WEEKS PER YEAR
1995	708	16	11,328	-	-	-	**11,328**
2006	728	18	13,104	365	6	2,190	**15,294**
2008	950	20	19,000	240	11	2,640	**21,640**

** Training Weeks Per year = Number trained x Length of training*

As the size and duration of FBI training grows, near full occupancy creates severe scheduling conflicts among the competing student groups and has become a significant concern at the FBI Academy. The pie charts below reflect average utilization rates for FBI Academy lodging and classroom over a five month period (1/14/08 - 6/16/08). Due to the age of the facilities, scheduled renovations and unplanned maintenance and repairs consume eight percent of space for both beds and classrooms. "Vacant" capacity is reported because 100 percent occupancy is a scheduling impossibility. In practical terms, the Academy is operating at capacity.





For example, during the week of May 5, 2008 there were eight New Agent classes, a National Academy class, and two Intelligence Basic Courses (IBCs) being trained simultaneously at the FBI Academy. These "core" requirements took up 787 of the 910 available beds; taking into

account the 81 beds not available due to renovations only 42 beds were available for other training. Because 42 beds were not enough to house an additional 50-student class (as classes are always lodged together), this class was forced to lodge at a nearby hotel. These 42 beds were counted as "vacant,", although it was not feasible to use them. For classrooms, the varying sizes/makeup of available classrooms does not always exactly match the training requirement of the current classes, thereby leaving classrooms "vacant" when in fact there is a higher demand than availability.

The 910 bed capacity at the FBI Academy is not sufficient for the training demand; therefore many training courses are pushed out onto the local economy. Adding a 650 bed dormitory and additional classrooms would ensure that core requirements would receive scheduling priority, such as entry-level training [New Agents, IBCs, Staff Operations Specialists (SOS), National Academy, and Counterintelligence] can be accommodated on-campus. The remaining balance of the beds would be used to host Career Path / regional training, most of which is currently conducted off-campus.

The data below puts the "core" (must take place at Academy) versus "non-core" (could take place at Academy) training volume into perspective, the table below (Chart A) shows the number of training weeks required by each core training area, and how these requirements result in a lack of bed space at the Academy for regional/other training (Chart B). By 2010, without the 650 bed addition, 5,692 bed weeks for the "core" requirements (i.e. new Agents) will be pushed out of the Academy and into local hotels.

FBI LODGING REQUIREMENTS

(U) Chart A.

PROGRAM	FY 2008 TOTAL STUDENTS TRAINED	FY 2008 LENGTH OF TRAINING (Weeks)	FY 2008 TOTAL BED WEEKS / YEAR	FY 2009 TOTAL STUDENTS TRAINED	FY 2009 LENGTH OF TRAINING (Weeks)	FY 2009 TOTAL BED WEEKS / YEAR	FY 2010 TOTAL STUDENTS TRAINED	FY 2010 LENGTH OF TRAINING (Weeks)	FY 2010 TOTAL BED WEEKS / YEAR
New Agent	950	20	19,000	1,200	20	24,000	1,300	20	26,000
Intel Analyst (IBC)	240	11	2,640	576	11	6,336	576	11	6,336
Staff Op. Specialist	100	4	400	300	4	1,200	450	4	1,800
National Academy	1,100	10	11,000	1,100	10	11,000	1,100	10	11,000
Counterintelligence	688	2	1,376	688	2	1,376	688	2	1,376
Renovations	80	52	4,160	80	52	4,160	80	52	4,160
Misc. (set aside)	10	52	520	10	52	520	10	52	520
Core Training Bed Weeks/Year			**39,096**			**48,592**			**51,192**

Chart B.

TRAINING WEEKS / YEAR	FY 2008 Current (910 beds)	FY 2008 Proposed (1,560)	FY 2009 Current (910 beds)	FY 2009 Proposed (1,560)	FY 2010 and beyond Current (910 beds)	FY 2010 and beyond Proposed (1,560)
Available Bed Weeks (*Beds X 50 weeks*)	45,500	78,000	45,500	78,000	45,500	78,000
Minus: Core Requirements (QT)	39,096	39,096	48,592	48,592	51,192	51,192
Available bed weeks for regional training	6,404	38,904	(3,092)	29,408	(5,692)	26,808

From 2005 to 2008, there has been a 200 percent increase in the number of regional training events (19,851 to 39,894). With the 650 bed addition, there would be 26,808 bed weeks available for regional training at the Academy, in addition to adequately housing core requirements. With the additional beds and classrooms that this proposed Training Facility will provide, it would be possible to host more of these regional training events at the FBI Academy campus.

Additional classroom space is also required. Currently, the FBI Academy has twelve 50-student, and four 24-student secure classrooms. The Academy can currently only hold nine NATs and up to three IBCs at the same time. In FY 2009, the IA-IBC doubled in class size (from 24 to 48), which has made it even more critical to provide more 50-student classrooms, in order to avoid scheduling conflicts.

The proposed facility would more than double the secure classroom capacity. This would allow the Academy to support a total of 18 NATs and up to six IBCs, which is more than double the current capacity.

The requested facility would also include a 200-student conference room equipped with dividing air-walls, allowing for up to four 50-student classrooms. This conference room is intended to draw in regional training which is currently hosted around the country due to a lack of conference space at the Academy. On average, the FBI hosts 40 100-person regional conferences per month. With more bed space and the 200-person conference room, more in-service training sessions could be held at the Academy.

The proposed training space will be equipped with more up-to-date technology and training equipment, as shown below. In particular, the proposed classrooms reflect the FBI's increased requirement for thin-client classrooms, which are secure computer rooms allowing both Trilogy and internet to run on the same monitor with switch boxes. These secure classrooms will alleviate scheduling constraints for the NAT, IBCs, and other classes that require this technology for their training.

Now		Proposed
Unsecure lecture rooms	→	Secure classrooms, and entire Secure floors
Overhead and movie projectors	→	DVD projectors
Chalkboards	→	Magnetized whiteboards
Workstation: basic computer	→	Workstation: FBInet and Unclassified Internet
Only several hours of computer training in one CBT (Computer Based Training) room	→	Secure FBInet and Internet computer training (92% IA, 56% NAT in thin-client)

The proposed cafeteria and dining hall would serve 700 students. The existing FBI Academy cafeteria was designed to serve two shifts of 360 (total of 720 students), but the addition of the 1988 Jefferson Dormitory (255 beds) forced the Academy to add an extra shift. Therefore, the cafeteria now serves three shifts of 325 (total of 975 students). The existing cafeteria is over its limit, and will not be able to serve the students from the new Training Facilities on campus. Therefore, an additional 700 person cafeteria is a fundamental structure to serve the additional students on campus.

Renovation and Abatement - $6,287,000 (all non-personnel)
Due to its 38 year age, Quantico's major buildings, systems, infrastructure, and equipment are outdated, have grossly exceeded their useful life, and do not meet current building code, fire, and life safety standards. Extensive maintenance and repairs are required to keep the old and out-dated facilities operating. Furthermore, the facilities, systems, and infrastructure were not designed to support today's technology, which is critical to incorporate into the FBI's ongoing training curriculum. To begin to alleviate these problems, the FBI requests $6,287,000.

Replacement parts for equipment are no longer available, requiring the modification of accessible parts to work with the old equipment. Estimates on how much additional funding is

required to operate a facility in poor condition run as high as 20 percent. New equipment is also more energy efficient. This efficiency will reduce the utility costs of the complex significantly.

The renovations will include interior infrastructure upgrades, a complete Fire Protection and Life Safety upgrade, including sprinkler and fire alarm systems, upgrades for compliance with all applicable building codes, compliance with the accessibility requirements of American's with Disabilities Act (ADA) and meet a minimum Leadership in Energy and Environmental Design (LEED) certified "Silver" rating in the Major Renovation Category.

All interior furnishings such as window treatments, flooring and carpeting, wall coverings, ceilings, and furniture will be upgraded. Building infrastructure for heating, ventilation, and air conditioning system; electrical system including transformers; lighting fixtures; receptacles; wall switches; panel boards; and wiring will be fully upgraded and made code compliant. The telephone and information technology systems will also be upgraded. Exterior window glazing will be replaced with thermal pane energy conserving glass. Elevators will be renovated with new equipment and the cab will be upgraded and made ADA compliant.

Funding

Base Funding

		FY 2009 Actual				FY 2010 Enacted Appropriation				FY 2011 Current Services			
		Pos	Agt	FTE	($000)	Pos	Agt	FTE	($000)	Pos	Agt	FTE	($000)
Facilities Infrastructure	FBI Academy	…	…	…	$…	…	…	…	$5,000	…	…	…	$…
Facilities Infrastructure	Renovation & Abatement	…	…	…	…	…	…	…	…	…	…	…	…
Total		…	…	…	$…	…	…	…	$5,000	…	…	…	$…

Non-Personnel Increase Cost Summary

Initiative	Non-Personnel Item	Unit Cost	Quantity	FY 2011 Request $(000)	FY 2012 Net Annualization (Change from 2011) $(000)
Facilities Infrastructure	FBI Academy	n/a	n/a	$67,605	$(49,281)
Facilities Infrastructure	Renovation & Abatement	n/a	n/a	6,287	…
	Total Non-Personnel			$73,892	$(49,281)

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	…	…	…	$…	$…	$…	$...
Increases	…	…	…	…	73,892	73,892	(49,281)
Grand Total	…	…	…	…	$73,892	$73,892	$(49,281)

A. Appropriations Language and Analysis of Appropriations Language

Appropriations Language for Construction

For [all] 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; [and] preliminary planning and design of projects; [$239,915,000] *and operation and maintenance of secure work environment facilities and secure networking capabilities; $181,202,000*, to remain available until expended. *Of the unobligated balances available under this heading, $98,886,000 are hereby permanently cancelled.* (Department of Justice Appropriations Act, 2010.)

Analysis of Appropriations Language

Adds language to authorize construction funds to be used for the operation and maintenance of secure work environment facilities and secure networking capabilities.

Adds language to permanently cancel unobligated balances of $98,886,000. At the time of the budget transmission, the FBI was assessing final TEDAC project expenditures. Outstanding obligations may affect the amount available for rescission.