U.S. Department of Justice
Federal Bureau of Investigation

FY 2016
Authorization and Budget Request to Congress

Table of Contents

VII. Exhibits

A. Organizational Chart
B. Summary of Requirements
C. FY 2016 Program Changes by Decision Unit
D. Resources by DOJ Strategic Goal/Objective
E. Justification for Technical and Base Adjustments
F. Crosswalk of 2014 Availability
G. Crosswalk of 2015 Availability
H. Summary of Reimbursable Resources
I. Detail of Permanent Positions by Category
J. Financial Analysis of Program Changes
K. Summary of Requirements by Object Class
L. Status of Congressional Requested Studies

Exhibits

B. Summary of Requirements
D. Resources by DOJ Strategic Goal/Objective
F. Crosswalk of 2014 Availability
G. Crosswalk of 2015 Availability
K. Summary of Requirements by Object Class

I. OVERVIEW FOR THE FEDERAL BUREAU OF INVESTIGATION

A. Introduction

Budget Request Summary: The Federal Bureau of Investigation's (FBI's) Fiscal Year (FY) 2016 budget request proposes a total of $8,483,607,000 in direct budget authority. The request includes a total of $8,414,625,000 for Salaries and Expenses (S&E), including 35,037 permanent positions (13,074 Special Agents (SAs), 3,083 Intelligence Analysts (IAs), and 18,880 professional staff (PS)) and 33,311 full time equivalents (FTE), and $68,982,000 for Construction to address the FBI's highest priorities. The request also includes the cancellation of $120,000,000 from excess Criminal Justice Information Services (CJIS) surcharge balances.

The request includes program increases totaling $20,000,000 to increase cyber investigative capabilities and to leverage the Intelligence Community Information Technology Enterprise (IC ITE) components and services. The request also includes a reduction of $91,368,000 in non-recurred program expenses from both the S&E ($50,350,000) and Construction ($41,018,000) accounts.

The FBI continues to strategically assess current and prospective operations to ensure that mission requirements are met at the lowest possible cost to the U.S. taxpayer. The FY 2016 budget request is a product of these assessments and provides the resources to continue the FBI's strategic vision into the future.

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

Organization of the FBI: The FBI operates Field Offices in 56 major U.S. cities and over 360 Resident Agencies (RAs) throughout the country. Resident Agencies are satellite offices that support the larger Field Offices and enable the FBI to maintain a presence in and serve a greater number of communities. FBI employees assigned to Field Offices and RAs perform the majority of the investigative and intelligence work for the FBI. Special Agents in Charge of FBI Field Offices report to the Director and Deputy Director. The FBI also operates over 60 Legal Attaché (Legat) offices and over 20 sub-offices in over 70 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 that includes the Criminal Justice Information Services (CJIS) Division and the Biometrics Technology Center; and the Hazardous Devices School and Terrorist Explosive Device Analytical Center (TEDAC) at Redstone Arsenal in Huntsville, Alabama.

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

- The National Security Branch, which includes the Counterterrorism Division, Counterintelligence Division, Terrorist Screening Center, and the Weapons of Mass Destruction Directorate.
- The newly formed Intelligence Branch, which includes the Directorate of Intelligence and the Office of Partner Engagement.

- The Criminal, Cyber, Response and Services Branch, which includes the Criminal Investigative Division, the Cyber Division, the Critical Incident Response Group, and the International Operations Division.
- The Science and Technology Branch, which includes the Criminal Justice Information Services Division, the Laboratory Division, and the Operational Technology Division.

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

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

Budget Structure: The FBI's S&E funding is appropriated among four decision units that are reflective of the FBI's key mission areas:

1. Intelligence;
2. Counterterrorism/Counterintelligence (CT/CI);
3. Criminal Enterprises and Federal Crimes (CEFC); and
4. Criminal Justice Services (CJS).

Resources are allocated to the decision units in one of three ways:

- Based on core mission function;
- Based on workload; or
- Pro-rated across all decision units.

Certain FBI divisions support one mission area exclusively and are allocated entirely to the corresponding decision unit. For example, all of the resources of the Directorate of Intelligence are allocated to the Intelligence Decision Unit while all of the resources of the CJIS Division are allocated to the CJS decision unit.

Critical investigative enablers, such as the Laboratory Division, the International Operations Division, the Critical Incident Response Group, and the Operational Technology Division, are allocated to the decision units based on workload. For example, if 25 percent of the Laboratory Division's workload is in support of counterterrorism investigations, then 25 percent of the Laboratory Division's resources are allocated to the CT/CI decision unit.

Administrative enablers, such as all three IT Divisions, the Facilities and Logistics Services Division, the Finance Division, and the Human Resources Division, are pro-rated across all four decision units since these Divisions support the entire organization.

Construction funding is not allocated to decision units.

B. Threats to the U.S. and its Interests

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

Terrorism Threat: Terrorism, in general, and al-Qa'ida and its affiliates in particular, continues to represent the most significant threat to the country's national security. Intelligence confirms that Al-Qa'ida remains committed to its goal of conducting attacks inside the U.S. and continues to adjust its tactics and tradecraft in response to U.S. security countermeasures.

Al-Qa'ida seeks to infiltrate overseas operatives who have no known nexus to terrorism into the U.S. using both legal and illegal methods of entry. Further, al-Qa'ida's access to chemical, biological, radiological, or nuclear material poses a serious threat to our Nation. Finally, al-Qa'ida's choice of targets and attack methods will 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.

In addition to the threat from al-Qa'ida, as geopolitical conflict zones continue to emerge throughout many parts of the world, terrorist groups may use this instability to recruit and incite acts of violence. The continuing violence in both Syria and Iraq, and the influx of foreign fighters who support the Islamic State of Iraq and the Levant (ISIL), threatens to destabilize an already volatile region while also heightening the threat to the West. Due to the prolonged nature and the high visibility of the Syrian conflict, the FBI is concerned that U.S. persons with an interest in committing jihad will be drawn to the region. Through law enforcement agencies like the FBI, American authorities are working with their international partners and INTERPOL to disseminate information on foreign fighters in Syria and Iraq, including individuals who have traveled from the U.S.

Another emerging issue is the threat of Homegrown Violent Extremists (HVEs). The extremists are those who reside or operate in the U.S. and become inspired by al-Qa'ida or similar groups through English-language propaganda, but do not have any ties to al-Qa'ida or any other foreign terrorist organization. In September 2014, Attorney General Eric Holder announced the launch of a series of pilot programs in cities across the country to bring together community representatives, public safety officials, and religious leaders to counter violent extremism. The new programs are being run in partnership with the White House, the Department of Homeland Security (DHS), and the National Counterterrorism Center (NCTC).

The internet is an effective terrorist recruitment tool. Through chat rooms, websites, and social media pages, one can obtain data on and make contact with radical groups without the risk of alerting authorities through overseas travel. Although the internet may provide a "below-the-radar" introduction to the radical side of Islam, many would-be terrorists still meet with their sponsors and trainers in person. U.S. citizens have traveled overseas to countries or camps with terrorist ties and then returned to the U.S. to do harm.

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

Weapons of Mass Destruction Threat: Intelligence indicates that the Weapons of Mass Destruction (WMD) threat continues to grow and pose significant danger to the U.S. and its allies. The U.S. Government has taken decisive and strategic actions to address this threat; however, the threat continues to evolve at a rapid pace as the capabilities and agility of those who would do harm to the U.S. and its international allies increase. The USIC must increase strategic and tactical intelligence and enhance partnerships to minimize WMD vulnerabilities. In an effort to provide effective risk response to the WMD threat, the FBI has identified four threat areas that constitute the greatest vulnerabilities:

- **Development and Use of Biological Weapons**, including synthetic and advanced biotechnology;
- **Domestic Acquisition of Chemical Agents**, including the vulnerability of chemical facilities in the U.S.;
- **Proliferation of WMD Materials,** including dual-use materials that have a wide range of non-nefarious and legitimate uses but could be utilized to develop a WMD capability; and
- **Smuggling and Proliferation of WMD Technology**, including foreign government interest in acquiring Chemical, Biological, Radiological, Nuclear (CBRN) materials and reduced controls over nuclear materials.

FBI WMD countermeasure, tripwire, counterproliferation, and outreach activities support policy priorities identified by the International Policy Committee on Countering Biological Threats. One example is the synthetic biology/emergent biotechnology initiative where the FBI partners with U.S. synthetic DNA providers to evaluate uncertainties or suspicious information in customer orders. Industry members follow established security protocol to vet customers prior to releasing genetic sequences of Biological Select Agents and Toxins and contact the FBI to report suspicious requests. Of concern are orders that may allow reconstruction of pathogenic organisms with synthesized DNA, circumventing the regulatory oversight that controls access to dangerous pathogens. Another example is the academic biosecurity partnership initiative where the FBI raises awareness of physical and cyber security concerns, personnel reliability and safety, exploitation of research for nefarious purposes, theft of intellectual property, and insider threat mitigation strategies.

The FBI continues to collaborate with industry, academia, public health, law enforcement, and the Intelligence Community to prevent biologic incidents and advance early detection of potential biological events that may have a terrorism nexus through the development of early warning signals and notification mechanisms and situational awareness to mitigate these risks. An example of this collaboration is the October 2014 exercise in Houston, TX to test response to a chemical attack. This exercise included participation by DHS, the Drug Enforcement Administration (DEA), other federal agencies, state and local law enforcement, and private sector representatives. In addition to testing response capabilities, this exercise also showed how private industry plays an important role in events like a chemical attack since they know their materials and vulnerabilities better than anyone else, and they are most likely to be the first to recognize suspicious activity related to their own operations.

Foreign Intelligence Threat: The foreign intelligence threat to the U.S. continues to increase as foreign powers seek to establish economic, military, and political preeminence and to position themselves to compete with the U.S. in economic and diplomatic arenas. The most desirable U.S. targets are political and military plans and intentions; technology; and economic institutions, both governmental and non-governmental. Foreign intelligence services continue to target and recruit U.S. travelers abroad to acquire intelligence and information. Foreign adversaries are increasingly employing non-traditional collectors – e.g., students and visiting scientists, scholars, and businessmen – as well as cyber-based tools to target and penetrate U.S. institutions. In 2014, the FBI launched the "Don't Be a Pawn"

campaign to help prepare U.S. college students for traveling overseas. As part of this campaign, the FBI made available publicly the film *Game of Pawns*, which was produced in partnership with the Office of National Counterintelligence Executive (ONCIX). Based on a true story, the film features Glenn Duffie Shriver, a student studying overseas who was asked by a foreign government to apply for U.S. government jobs with the goal of obtaining secret U.S. government information.

Cyber Threat: The U.S. continues to face a range of criminal, terrorist and nation-state actor threats. Their activities range from simple vandalism and lucrative organized crime rings to terrorism and nation-state intelligence collection. Terrorists seek to sabotage critical infrastructure; organized crime syndicates seek to defraud banks and corporations; and spies seek to steal defense and intelligence secrets, or Corporate America's intellectual property.

While these threats are not new, the means by which they act are changing. Today, these threats act via the Internet and other computer networks. These networks provide ample cover from attribution, making managing the broad reaching consequences of the intrusion difficult as the motive of the attacker - be it criminal, and terrorist or nation-state espionage - can remain unknown. Concurrently, just as the Internet has enabled businesses to maximize profits by inexpensively connecting with millions of customers, it has also enabled threats to amplify their impacts by inexpensively attacking millions of victims.

These circumstances have created risks to national security, global economic stability and public welfare. Despite formidable investments and concerted efforts by the private sector and government to build more secure and defensible computer networks, these risks remain high. As technology continues to proliferate into every facet of modern life - from social media and smart phones to critical infrastructure, automobiles and implanted medical devices - cybersecurity continues to be a rapidly growing concern with no easy solutions in sight.

The FBI's mission in cybersecurity is not to study computer networks to patch vulnerabilities, nor is the FBI's jurisdiction confined to only those assets owned by the U.S. government or critical infrastructure providers. Rather, the FBI's mission focuses on countering the threat by investigating intrusions to determine criminal, terrorist, and nation-state actor identities, and engaging in activities which reduce or neutralize these threats. At the same time, the FBI also collects and disseminates information significant to those responsible for defending networks, including information regarding threat actor targets and techniques. The FBI's jurisdiction is not defined by network boundaries; rather it includes all territory governed by U.S. law, whether domestic or overseas, and spans individual citizens, private industry, critical infrastructure, U.S. government, and other interests alike. Collectively, the whole-of-government approach being taken by the FBI and its federal partner agencies will serve to help deter future threats and bring closure to current threats which would otherwise continue to infiltrate and harm our network defenses.

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

> **Public Corruption:** Public Corruption, which involves the corruption of local, state, and federally elected, appointed, or contracted officials, undermines our democratic institutions and threatens public safety and national security. Government fraud affects how well U.S. borders are secured and neighborhoods protected; how verdicts are handed down in court; and the quality

of public infrastructure such as schools and roads. Taxpayer dollars wasted or lost as a result of corrupt acts by public officials represent a threat to domestic security and stability.

Border Corruption: The federal government is responsible for protecting approximately 7,000 miles of the U.S. border and 95,000 miles of shoreline. Each day, approximately 1 million persons visit the U.S. and enter through one of the 329 official Ports of Entry (POEs) located along the southwestern and northern land borders of the U.S., as well as at seaports and international airports. The documented presence of corrupt border officials facilitates a wide range of illegal activities along the northern and southern borders. Resource-rich cartels and criminal enterprises employ a variety of methods in order to target and recruit U.S. Border Patrol Agents, Customs and Border Protection Officers, and local police officers who can facilitate criminal activity. Corrupt officials assist these entities by providing intelligence and contraband across these borders. To help address this threat, the Border Corruption Initiative (BCI) was established in 2009. The BCI has developed a threat-tiered methodology, targeting border corruption in all land, air and sea ports of entry in order to mitigate the threat posed to national security. The FBI has established the National Border Corruption Task Force (NBCTF), 17 Border Corruption Task Forces (BCTFs), and 5 Border Corruption Working Groups (BCWGs) in high-risk cities along the northern and southern borders.

Corporate Fraud: As the lead agency investigating corporate fraud, the FBI focuses on cases involving complex accounting schemes, self-dealing corporate executives and obstruction of justice. The majority of cases pursued by the Bureau involve accounting schemes—deceiving investors, auditors and analysts about the true condition of a corporation. Through the manipulation of financial data, the share price of a corporation remains artificially inflated based on fictitious performance indicators provided to the investing public. In addition to significant financial losses to investors, corporate fraud has the potential to cause immeasurable damage to the U.S. economy and investor confidence. In FY 2014, the FBI had 984 pending corporate fraud cases.

Insider trading continues to pose a serious threat to the U.S. financial markets. Through national-level coordination, the FBI strives to protect the fair and orderly operation of the U.S. financial markets and help maintain public trust in the financial markets and the financial system as a whole. These efforts have led to more than a 108 percent increase in insider trading cases from FY 2010 to FY 2014, and a historic success with the recent ongoing insider trading probe.

Securities/Commodities Fraud: The FBI focuses its efforts in the securities fraud arena on schemes involving high yield investment fraud market manipulation, and commodities fraud. During and after the recent crisis, the FBI saw an unprecedented rise in the identification of Ponzi and other high yield investment fraud schemes, many of which involve thousands of victims and staggering losses. Indeed, the FBI still continues to open new Ponzi scheme cases on a weekly basis. Additionally, the development of new schemes, such as stock market manipulation via cyber intrusion, continues to indicate that securities fraud is on the rise. Since 2007, FBI securities fraud investigations have increased by 60 percent.

The FBI has adopted an intelligence-led approach to identifying and targeting the most egregious perpetrators of securities fraud, utilizing undercover operations to identify and stop perpetrators before they are able to victimize individuals and damage financial markets. Securities and Futures Industries Suspicious Activity Reports (SARs) contain some of the best intelligence available to criminal and regulatory law enforcement personnel. In 2009, the FBI established a

process to better exploit this intelligence to identify new securities fraud schemes and perpetrators. With the coordinated effort of special agents and intelligence analysts, these SARs are analyzed on a national level, leading to the creation of targeting packages which are presented to relevant Field Offices to open investigations.

Corporate fraud, along with securities and commodities fraud, remains a top priority of the FBI Financial Crimes Section and the FBI is committed to addressing this significant crime problem. Between FY 2003 and FY 2014, FBI special agent resources dedicated to corporate and securities/commodities fraud increased from 250 to 422 agents while the caseload increased at roughly the same pace, 1,216 to 2,924 cases. The impact of these resources has been significant: since 2004, the FBI has 625 information and indictments, and 516 convictions per year. These cases have resulted in billions of dollars in asset forfeitures.

Mortgage Fraud and Other Financial Institution Fraud: Mortgage fraud, a subset of financial institution fraud, continues to absorb considerable FBI resources. As long as houses are bought and sold and banks lend to consumers, mortgage fraud will continue. At the end of FY 2014, approximately 73 percent of the FBI's 1,379 mortgage fraud cases involved losses exceeding $1 million per case. In 2014, the FBI received 41,771 Mortgage Fraud Related SARs.

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

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

Health Care Fraud: National health care expenditures in the U.S. are expected to surpass the $3.2 trillion mark by 2015, representing a 58 percent increase from the 2005 $2.0 trillion expenditures. This creates an environment prevalent to fraud, as the National Health Care Anti-Fraud Association (NHCAA) estimates the financial losses due to health care fraud are in the tens of billions of dollars each year.

Today, the FBI seeks to identify and pursue investigations against the most egregious offenders involved in health care fraud and abuse, including criminal enterprises and other crime groups; corporations; companies; and providers whose schemes affect public safety. Besides federal health benefit programs such as Medicare and Medicaid, private insurance programs also lose billions of dollars each year to fraud schemes in every sector of the industry.

The FBI's increased focus on complex investigations, such as those involving criminal enterprises, is noted in the increase number of criminal organization disruptions from 269 in FY

2010 to 605 in FY 2014 and the increase of organization dismantlements from 95 in FY 2010 to 140 in FY 2014. The scope of the crime problem is also noted in that the DOJ Civil Division's Commercial Litigation Branch has obtained settlements and judgments of $2.3 billion in 2014 alone, which was the fifth straight year of recoveries of more than $2 billion in cases involving false claims against federal health care programs, a significant part of which comes from joint investigations involving the FBI and Health and Human Services (HHS).

Other Complex Financial Crimes (Insurance, Bankruptcy, and Mass Marketing Fraud): The FBI does not anticipate the trends in insurance fraud to change in the future. If insurance fraud continues to increase, this will contribute to increases in insurance premiums as well as threaten the financial viability of insurance companies. Since 2006, the year after bankruptcy laws were changed to make it more difficult for an individual to discharge all debts, bankruptcy filings have significantly increased each year according to the U.S. Bankruptcy Courts. The potential for fraud within bankruptcy is large. According to the Federal Trade Commission, complaints concerning mass marketing fraud have also increased.

Intellectual Property Rights: The FBI's overall strategy for Intellectual Property Rights (IPR) enforcement is to disrupt and dismantle international and domestic criminal organizations and individuals that manufacture or traffic in counterfeit and pirated goods and/or steal, distribute or otherwise profit from the theft of intellectual property. Investigative priorities include theft of trade secrets, counterfeit goods that pose a threat to health and safety, and copyright and trademark infringement cases having a national security, organized crime, or significant economic impact.

- The FBI is a primary partner at the DHS-led National Intellectual Property Rights Coordination Center (IPR Center). The IPR Center serves as a centralized, multiagency entity to coordinate, manage and advocate the U. S. Government's Federal criminal enforcement of intellectual property rights laws. The FBI pursues intellectual property rights enforcement by coordinating investigations with law enforcement partners at the IPR Center. This coordination includes initiating criminal initiatives based on current and emerging threats as well as coordinating intelligence components and investigative strategies with both private industry and domestic and foreign law enforcement partners.

Gang Violence: Across the country, violent street gangs operate in communities of all sizes: urban, suburban and rural areas. FBI Violent Gang Safe Streets Task Forces (VGSSTFs) report that violent street gangs, whether they are neighborhood based or national gangs, are a top threat to our communities followed by prison gangs and outlaw motorcycle gangs. The FBI's Violent Gang strategy is designed to reduce gang related violence by identifying, prioritizing, and targeting the most violent gangs whose activities constitute criminal enterprises. This is accomplished through the administration of 163 VGSSTFs.

Gangs continue to proliferate and commit violent crime and are continuing to expand to suburban and rural areas. This migration is believed to be a result of better organized urban gangs expanding their criminal networks into new market areas in suburban and rural locations, where they can absorb local unaffiliated gangs or use violence to intimidate them. As these expanding gangs encounter resistance from local gangs or other drug distributors in these communities, violent crimes such as assaults, drive-by shootings, and murders can be expected to increase.

Intelligence indicates that gangs are becoming more violent and are establishing strong alliances with drug trafficking organizations. In addition, they are also partaking in less typical gang-related crime, such as human trafficking, white-collar crime, specifically bank fraud, and cybercrime.

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

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

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

- Hate Crimes: Investigating hate crimes is the leading priority of the Civil Rights Program due to the devastating impact that the crimes have on individuals, families, and communities. Groups that preach hatred and intolerance plant the seeds of terrorism within our nation and undermine the principles on which this nation was founded. A hate crime is a traditional criminal offense, such as murder, arson, or vandalism, motivated in whole or in part by an offender's bias against a victim's actual or perceived race, religion, national origin, disability, gender, gender identify, or sexual orientation.

- Color of Law (COL): COL violations are the deprivation of any rights, privileges, or immunities secured or protected by the U.S. Constitution by someone in his/her official, governmental capacity. The FBI has investigative responsibility for federal COL matters involving local and state law enforcement and concurrent responsibility with the Office of Inspectors General for other federal agencies.

- Human Trafficking: Human trafficking is a form of modern-day slavery and 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; however, 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.

Crimes Against Children: The Violent Crimes Against Children Program has developed a nationwide capacity to 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 impacts of international parental rights disputes; and strengthen the capabilities of federal, state and local law enforcement agencies through training programs and investigative assistance. The FBI is the only federal agency with sole jurisdiction to investigate child abductions, as legislated in Title 18, U.S. Code, Section 1201. The FBI Crimes Against Children Unit supports the Child Abduction Rapid Deployment Team (CARD Team), Innocence Lost National Initiative, Innocent Images National Initiative and the Child Sex Tourism (CST) Initiative.

- Child Abductions: In FY 2014, the FBI investigated 314 pending child abduction cases. In an effort to enhance the FBI's response to abductions and the mysterious disappearance of children, the FBI's Violent Crimes Section in coordination with the Critical Incident Response Group (CIRG)/Behavior Analysis Unit III (BAU III) created regional Child Abduction Rapid Deployment (CARD) Teams. Teams are geographically distributed throughout the five regions of the U.S. The CARD Team represents 35 field divisions with each regional team comprised of 12 Supervisory Special Agents and Special Agents.

- Innocence Lost investigations address the commercial sexual exploitation of children. Investigations have identified national criminal organizations responsible for the sex trafficking of hundreds of children, some as young as nine years old. In FY 2013, 70 FBI-led Child Exploitation Task Forces designed to combat all child exploitation matters to include the commercial sexual exploitation of children through sex trafficking were established. In FY 2014, the Innocence Lost National Initiative (ILNI) investigated 1,674 pending cases, and achieved 488 informations/indictments and 424 convictions. Furthermore, subjects of these investigations are regularly sentenced to terms of 25 years or more, while ten have received life sentences.

- Child Sex Tourism (CST) initiative targets U.S. citizens who travel to foreign countries and engage in sexual activity with children under the age of 18. The initiative has also organized and participated in capacity building for foreign law enforcement, prosecutors, and non-government organizations in these countries. In FY 2014, the CST Initiative investigated 59 investigations, and achieved 6 arrests and 7 convictions.

Indian Country: The Indian Country Crimes (ICC) component of the FBI has developed and implemented strategies to address the most egregious crime problems in Indian Country (IC) where the FBI has responsibility. ICC supports joint investigative efforts with the Bureau of Indian Affairs-Office of Justice Services, tribal law enforcement, and manages 14 Safe Trails Task Forces. ICC cases are mostly reactive; however, many are cross-programmatic in nature and include public corruption and complex financial fraud.

As of January 2015, the FBI had 2,982 pending Indian Country (IC) investigations on approximately 200 reservations and 400 Indian gaming facilities throughout 28 states. Approximately 74 percent of

these investigations are in the Minneapolis, Salt Lake City, Phoenix, and Albuquerque Field Offices and the majority of the investigations involve death, sexual/physical assault of children, and/or felony assaults. Statistics indicate more than one-third of all Native American women will be raped at least once during their lifetime and nearly two-thirds will be victims of violent assaults. Financial crimes are currently an under-addressed avenue of investigation primarily due to the nature and volume of reactive violent crimes requiring the attention of the FBI. Limited internal and external oversight makes Indian Country an attractive potential target for financial crimes.

Due to jurisdictional issues, the FBI is the primary law enforcement entity in the IC. Furthermore, the Bureau of Indian Affairs has a limited number of investigators, though they are not present on every reservation. Additionally, Tribal authorities can only prosecute misdemeanors of Indians, and state/local law enforcement does not have jurisdiction within the boundaries of the reservation, with the exception of Public Law 280 states[1] and tribes. DOJ has reported that 25 percent of all violent crimes prosecuted by the U.S. Attorney Offices are related to IC. There are 14 Safe Trails Task Forces that are addressing drug/gang and violent crimes in IC.

***Fugitives*:** There are approximately 2.1 million active warrants within the National Crime Information Center (NCIC) system. The FBI is conducting investigations on more than 8,000 violent fugitives under the Unlawful Flight to Avoid Prosecution violation.[2] Further, the FBI has more than 6,500 case file fugitives outstanding and approximately 2,143 fugitives from the U.S. are believed to be in foreign countries. There are approximately 1,000 FBI red/blue notices[3] in place with Interpol for fugitives believed to have fled overseas.

Transportation Crimes: Personal and property crimes continue to be a concern within Special Jurisdiction Crimes areas such as within federal penal institutions, on other federal government properties, and in special jurisdictional areas, such as on the high seas.

Southwest Border: The volatility among Transnational Criminal Organizations (TCOs) and violent gangs (e.g., Mexican Mafia, Barrio Azteca, Los Zetas, MS-13, and 18th Street) along the Southwest Border has resulted in increased levels of drug-related violence. As rival TCOs and gangs battle for control over the lucrative drug markets, spikes in kidnappings, homicides and a myriad of other violent acts have occurred along the U.S.-Mexico border. In addition, these transnational groups are utilizing several "tools" to aid in their objectives, such as public corruption, money laundering, human trafficking, and threats to law enforcement.

To address the Southwest Border threat, the FBI has developed an intelligence-driven, cross-programmatic strategy to penetrate, disrupt and dismantle the most dangerous organizations as well as identify and target individuals in leadership roles. This strategy includes the deployment of hybrid squads in areas assessed to be particularly vulnerable to violence and criminality associated with TCOs, regardless of their physical proximity to the border. The primary goal of the hybrid squad model is to bring a threat-based domain view of these dynamic, multi-faceted enterprises, thus fusing strategic and tactical intelligence with investigative operations. In turn, this can increase the likelihood that the FBI is

[1] P.L. 280 is a federal law which transfers criminal jurisdiction of IC to the state government, but generally prohibits states from altering regulations pertaining to Native Americans regarding taxation, natural resources, and wildlife management.
[2] Title18, USC 1073, Unlawful Flight to Avoid Prosecution (UFAP) gives the FBI statutory authority to pursue criminals who have fled interstate.
[3] Red Notice - Requests to seek the location and arrest of a wanted person with a view to extradition based on an arrest warrant or court decision. Blue Notice - Collects information about, locates, or identifies a person of interest in a criminal investigation.

aware of every facet of illicit activity within the organization at all levels and can link them back to priority targets outside the U.S. To that end, hybrid squads consist of multi-disciplinary teams of Special Agents, IAs, Staff Operations Specialists (SOS), and other professionals who approach TCEs holistically. The agent composition on the squads provides different backgrounds and functional expertise, ranging from violent gangs, public corruption, and violent crimes.

C. FBI's 2016 Budget Strategy

Required Capabilities to Address National Security, Cyber, and Criminal Threats: The FBI's budget strategy is based on the FBI's knowledge of current and future national security, cyber, and criminal investigative threats. Based on this information, 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 and cyber threats and crime problems regardless of who actually perpetrates the acts.

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

FBI Strategy Management System (SMS):

The Strategy Management System (SMS) is the management tool that the FBI Director and senior leaders use to manage the FBI strategy and to test whether the strategy is working. Is the FBI headed in the right direction over the next three to five years? Are resources aligned to our highest priorities and greatest risks? Which capabilities and internal processes does the FBI need to enhance? What new training and technology must the FBI provide to its people so they can accomplish the dual mission? These are the types of questions that the SMS framework seeks to answer.

At Headquarters, the SMS process cascades from the FBI enterprise down through the FBI HQ branches and divisions to ensure that strategy is part of everyone's job. Each year, divisions, in conjunction with the SMO, assess their strategic gaps and develop measures and initiatives to close these gaps. In addition, SMS cascades to the field through the Integrated Program Management (IPM) process via the Consolidated Strategy Guide (CSG), which informs the creation of the Field Office Strategic Plan (FOSP). To remain consistent with the headquarters model, the strategy created by the FOSP cascades from the SAC down to the squad level.

Strategic Shifts

The shifts articulate the vision of what the FBI will look like in 3 to 5 years. They identify critical focus areas – known as dimensions of change – where the FBI needs to drastically improve, or shift, in order to meet its evolving mission.

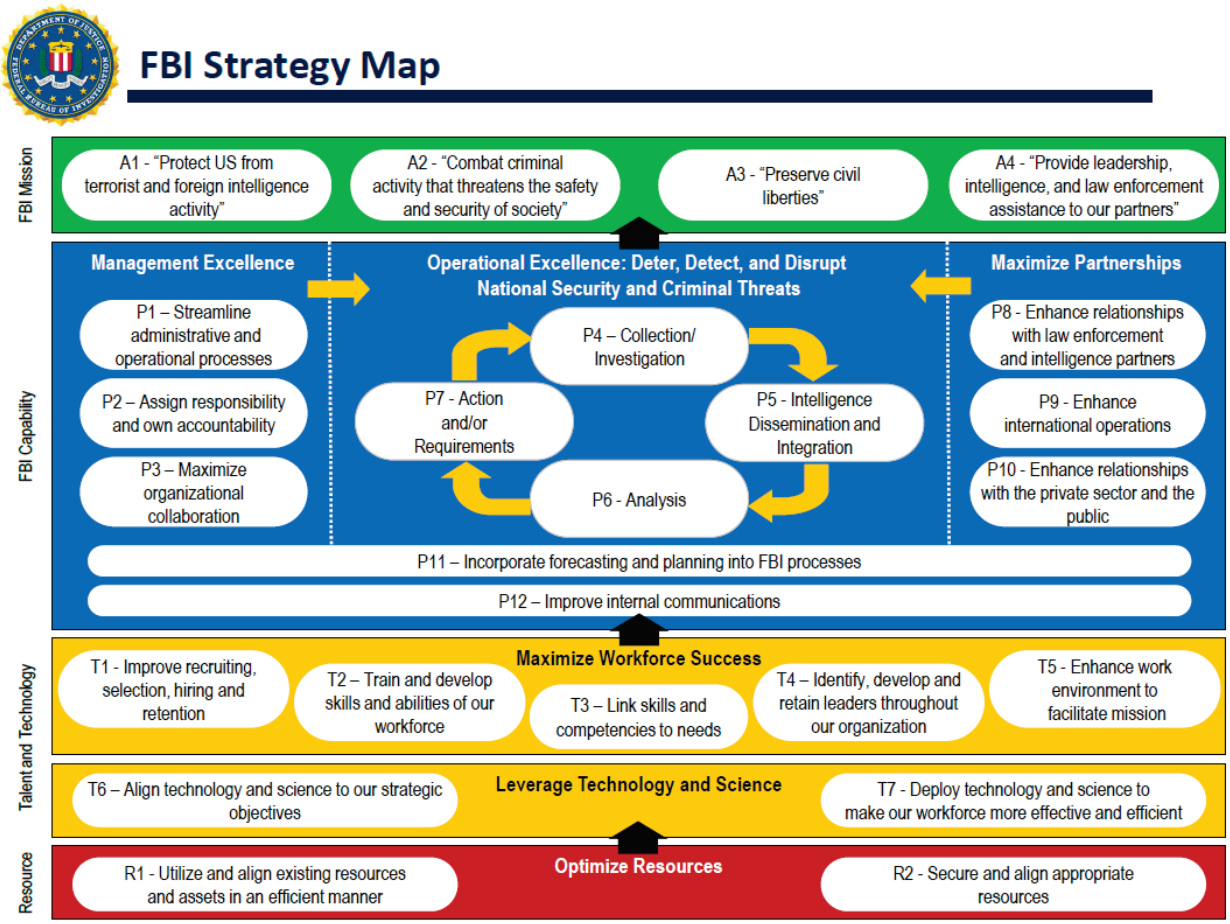
FBI Vision: Strategic Shifts

The FBI is a national security organization with intelligence and law enforcement responsibilities. The Shifts below represent continuing focus areas for the FBI over the next three to five years in order to achieve its vision.

Case-Based Program Management	*Focus*	Intelligence-Driven, Threat-Focused Program Management
Activity-Based	*Measurement of Success*	Impact-Based
"Share; restrict what you must"	*Information Sharing*	Timely, Secure, and Relevant Sharing
Partner	*Intelligence Community*	Domestic Leader
Global Presence	*Scope*	Global Impact
Tactical	*Leadership*	Strategy Drives Tactics
Unfocused and Uncoordinated	*Internal & External Communications*	Focused and Coordinated
Program-Focused	*Organization*	Integrated Teams
Process-Focused	*Human Capital*	Workforce Development Focus
Value Based on Role	*Workforce Culture*	Value Based on Contribution
Disparate IT Systems	*Information Technology*	Integrated IT Solutions
Budget Drives Strategy	*Resource Management*	Strategy Drives Resources

FBI Strategy Map

The strategy map delineates how the FBI will achieve the strategic shifts. The strategy map contains 25 objectives, each aligned to a specific perspective and theme.



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

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

SMS Profile and Initiatives

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

addition, key strategic initiatives are identified and tracked to ensure that any performance gaps are closed.

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

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

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

Intelligence-Driven Operations:

The FBI recently created an Intelligence Branch, led by an Executive Assistant Director for Intelligence (EAD-I), to provide strategic guidance for the FBI's intelligence program and priorities to ensure intelligence is more seamlessly integrated into the organization's foundation and shared between components. The current threat environment is not bound by geographic distinctions or investigative programs; instead, threats cross all existing boundaries. The new branch will ensure the FBI's organizational structure is flexible enough to effectively identify and address all threats, whether they fall within the FBI's national security or criminal missions. This collaboration and information sharing will enable the FBI to operate in accordance with one enterprise-level plan that enables intelligence to more fully drive operations.

The EAD-I serves as the FBI's Foreign Language Program Manager, to include serving as the Executive Agent for the National Virtual Translation Center (NVTC), and as the focal point for the FBI's engagement with the Office of the Director of National Intelligence (ODNI) on the National Intelligence Program (NIP).

The FBI uses intelligence to understand national security threats, and to conduct operations to dismantle or disrupt those threats. Some examples of how the FBI uses intelligence to drive its operations include:

- Field Intelligence Groups (FIGs): The FBI developed a standardized model for field intelligence that can be adjusted to the size and complexity of small, medium, and large offices. There are now 56 FIGs throughout the Nation.

- Fusion Cells: Fusion Cells are intelligence teams within operational divisions designed to integrate all aspects of the intelligence cycle for a unique threat. The Fusion Cells integrate intelligence and operations and collaborate across work roles to ensure intelligence drives and supports operations. Fusion Cells consist of Intelligence Analysts (IAs) who cover the strategic,

domain, collection, and tactical intelligence functions. The structure and process of the Fusion Cells are designed to streamline intelligence support and more directly collaborate with operations.

- The Collection Operations Requirements Environment (CORE): The CORE system is a technology solution that makes FBI and national intelligence requirements easily accessible to all Field Office personnel and improves information flow between operational squads and the FIGs.

- Threat Review and Prioritization (TRP): As the U.S. Government's lead domestic intelligence agency, the FBI is required to identify, prioritize, and mitigate a variety of threats that have an impact on national interests and public safety. Consequently, the Directorate of Intelligence spearheaded the Threat Review and Prioritization Process (TRP), which has been established as the FBI's process for assessing, triaging, and prioritizing threats. On an annual basis, operational divisions will prioritize national threat issues, determine FBI National Threat Priorities (NTPs), and develop national-level mitigation strategies. This information is then used by field offices to run the Field TRP process to prioritize the NTPs and other national and local threat issues and to develop field mitigation strategies that align with national strategies. TRP provides a standardized process whereby threat issues are uniform across the organization, inputs and outputs can be articulated and measured, and intelligence and operational components are further integrated. Using standardized criteria, TRP provides a method for cohesively prioritizing all threat issues at the Headquarters and field level for the purpose of directing work to effectively mitigate those threat issues. The TRP process's outputs are also used as the basis for the Integrated Program Management initiative, which standardizes how FBIHQ program manages the FBI's 56 field offices.

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, such as information technology refresh and vehicle fleet replacement.

An aspect of the multi-year planning effort is the Corporate Capital Planning Office within the Finance Division, which is currently examining the long-term needs of certain large-scale capital projects in the areas of facilities and information technology.

D. Environmental Accountability

The FBI is currently rolling out an organizational Environmental Management System (EMS) that provides corporate protection standards to deploy to Field Offices and major facilities (including CJIS, Quantico, and HQ). Individual facility and Field Office EMSs will follow. The FBI established an overarching environmental policy to serve as the guiding framework for developing, implementing, and continually improving the EMS. The organizational EMS is implemented through Environmental Protection Programs (EPPs) that establish policy and procedure in major environmental programmatic areas. A number of EPPs (Solid Waste & Recycling Management; Petroleum, Oil, & Lubricants (POL) Management; Hazardous Waste Management; Energy Management; Water Management; High Performance & Sustainable Green Buildings; Sustainable Acquisitions; Emergency Planning & Community Right-to-know Act (EPCRA); and Electronics Stewardship) have been developed and fully implemented. Additionally, CJIS has maintained its facility-based EMS and is currently maintaining

site-specific EPPs in accordance with the FBI's EMS policy. The FBI is also developing EPPs for implementing the National Environmental Policy Act (NEPA), scheduled to be completed in FY 2015.

The FBI has revised its safety committee policy and procedures, including the implementation of safety committees – which are in place within all FBI Divisions and major facilities. The safety committees will become "green teams" and provide a forum for discussion of environmental issues and a mechanism for EMS implementation. Additionally, the FBI has added a higher level Executive Environmental, Health and Safety Committee that meets every six months to address FBI environmental and safety policies and initiatives.

The FBI actively participates in DOJ's overall efforts to implement Executive Order 13514, "Federal Leadership in Environmental, Energy, and Economic Performance." The FBI provided data and input into the Department's Strategic Sustainability Performance Plan (SSPP) and routinely corresponds with DOJ and other government components to determine the most efficient, effective methods to protect the environment. Energy and water audit findings have been tracked for utility efficiencies and used to both prioritize facility maintenance projects and forecast future consumption and costs based on the implementation of specific ECMs and WCMs. The FBI will continue to evaluate the efficiencies garnered on an ongoing basis to ensure their effectiveness on the conservation of both financial and natural resources.

Additionally, the FBI is currently updating the sustainable building policy developed in 2008 to address requirements of Executive Orders 13423, "Strengthening Federal Environmental, Energy, and Transportation Management" and 13514, referenced above, 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 over $25 million 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, proposed updates will require that all new construction and major renovations of FBI-owned facilities meet the Federal Guiding Principles for High Performance and Sustainable Buildings, and existing buildings to work toward meeting these Guiding Principles. The FBI will obtain LEED Gold certification for the new Biometrics Technology Center (BTC) at the CJIS Complex, and is pursuing LEED certification for Laboratory Building and Collaboration Center at the new TEDAC facility in Huntsville, AL.

The FBI's Fleet Management Program integrates environmental accountability into its operations in various ways. The FBI continually incorporates hybrid vehicles, alternative fuel vehicles (E85), electric vehicles, and more fuel efficient vehicles (4 cylinders) into the 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, including degreasers, hand cleaners, and general purpose cleaners in day to day operations. Finally, facilities are ramping up hazardous waste training through pollution prevention and recycling program.

II. Summary of Program Changes

	Description	Pos.	FTE	Dollars ($000)	Page
Next Generation Cyber	To increase investigative capabilities, improve cyber collections and analysis, and extend centralized capabilities to the field.	...	…	$10,300	5-1
IT Infrastructure	To provide an updated network infrastructure and utilize the IC Information Technology Enterprise (IC ITE) components and services.	…	…	$9,700	5-7
Office of the Director of National Intelligence (ODNI) Direction	To reduce funding in accordance with ODNI priorities	…	…	($2,000)	6-1
Program Non-Recur - TEDAC	To non-recur funding provided in FY 2015.	…	…	($10,000)	6-2
Program Non-Recur - HDS	To non-recur funding provided in FY 2015.	…	…	($3,000)	6-4
Program and/or Administrative Savings	To non-recur funding provided in FY 2015. Examples of savings to be realized in 2016 include, but are not limited to, reducing the FBI's physical footprint, leveraging and extending the useful life of existing technology, bulk purchases and bundling technology procurements.	…	…	($35,350)	6-6
Total Program Changes		…	…	**($30,350)**	

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, [$8,326,569,000, of which not less than $8,500,000 shall be for the National Gang Intelligence Center, and] *$8,414,625,000,* of which not to exceed $216,900,000 shall remain available until expended: *Provided further,* That not to exceed $184,500 shall be available for official reception and representation expenses[: *Provided further,* That up to $1,000,000 shall be for a comprehensive review of the implementation of the recommendations related to the Federal Bureau of Investigation that were proposed in the report issued by the National Commission on Terrorist Attacks Upon the United States].

(CANCELLATION)

Of the unobligated balances available under this heading from fees collected to defray expenses for the automation of fingerprint identification and criminal justice information services and associated costs, $120,000,000 are hereby permanently cancelled: Provided, That no amounts may be cancelled from amounts that were designated by the Congress as an emergency requirement pursuant to the Concurrent Resolution on the Budget or the Balanced Budget and Emergency Deficit Control Act of 1985, as amended.

Analysis of Appropriations Language

- The FY 2015 Appropriation included language specifying a certain amount for the National Gang Intelligence Center. The FBI proposes to strike this language in FY 2016.
- The 9/11 Review Commission will not require funding in FY 2016, which is why this language has been deleted.
- The FY 2016 President's Budget request includes a cancellation of $120,000,000 from excess Criminal Justice Information Services (CJIS) surcharge balances.

IV. Decision Unit Justification
A. Intelligence Decision Unit

INTELLIGENCE DECISION UNIT TOTAL	Perm. Pos.	FTE	Amount ($000)
2014 Enacted	7,160	6,766	$1,647,492
2015 Enacted	7,174	6,800	1,654,977
Adjustment to Base and Technical Adjustments	5	5	32,873
2016 Current Services	7,179	6,805	1,687,850
2016 Program Increases	…	…	2,037
2016 Program Decreases	…	…	(11,439)
2016 Request	7,179	6,805	$1,678,448
Total Change 2015-2016	**5**	**5**	**$23,471**

1. Program Description
The FBI's Intelligence Decision Unit (IDU) includes the entirety of the Directorate of Intelligence (DI); the intelligence functions within the Counterterrorism, Counterintelligence, Cyber, and Criminal Investigative Divisions and the Weapons of Mass Destruction Directorate; Field Intelligence Groups (FIGs); the Office of Partner Engagement (OPE); the Terrorist Screening Center (TSC); Infrastructure and Technology (e.g., SCIFs and SCINet); and Intelligence Training. The IDU also includes a portion of the Critical Incident Response Group, Laboratory Division, and International Operations Division based on the work that those divisions do in support of intelligence activities. Additionally, to capture all resources that support these programs, a prorated share of resources from the FBI's support divisions (including Training, Finance, Facilities and Logistics Services, Information Technology (IT), and Human Resources) is calculated and allocated to the decision unit.

Recent Reprogramming and Reorganization
In FY 2014 the FBI reorganized its intelligence activities to facilitate the complete integration of intelligence and operations and ensure its structure effectively supports the organization's work to safeguard national security and public safety. This restructuring included the establishment of a new Intelligence Branch, headed by an Executive Assistant Director for Intelligence, responsible for overseeing all intelligence strategy, resources, policies, and operations. The restructuring also entailed the realignment of the Directorate of Intelligence from the National Security Branch to the new Intelligence Branch.

In addition, the restructuring included the establishment of an Office of Partner Engagement (OPE) within the Intelligence Branch to implement initiatives and strategies supporting engagement, communication, coordination, and cooperation efforts with law enforcement, intelligence, and public and private partners that enhance the FBI's domestic information-sharing capabilities. To effectively carry out its responsibilities, the OPE absorbed the resources and responsibilities of the former Office of Law Enforcement Coordination within the FBI's Criminal, Cyber, Response, and Services Branch. In addition, the FBI realigned positions from the National Security Branch to the Intelligence Branch to support the collection and prioritization of user requirements for analytical tools.

Intelligence Branch
The Intelligence Branch, under the Executive Assistant Director for Intelligence, serves as the strategic leader of the FBI's Intelligence Program and functions as a liaison to the Office of the Director of National Intelligence (ODNI). It drives collaboration to achieve the full integration of intelligence and operations throughout the FBI, proactively engages with the FBI's partners across the intelligence and

law enforcement communities, and is responsible for all FBI intelligence strategy, resources, policies, and operations. The branch provides strategic direction and oversight for all intelligence functions throughout the FBI and directly oversees the Directorate of Intelligence and Office of Partner Engagement.

Directorate of Intelligence

The Directorate of Intelligence (DI) is an essential component of the FBI's Intelligence Program, helping to drive the continued integration of intelligence and operations throughout the enterprise. The DI focuses on six core functions: cross-programmatic strategic analysis, improved finished intelligence production, refined source validation processes, oversight and support of the field intelligence program, development of the intelligence workforce, and excellence in language services. In addition, the DI manages all aspects of the intelligence cycle throughout the FBI.

Intelligence Analysts

The work performed by Intelligence Analysts (IAs) is essential to the FBI's ability to understand national security and criminal threats, and to develop a deeper understanding of tomorrow's potential threats. To safeguard national security, the FBI must focus analytic resources to analyze the threat, determine potential courses of action, and place analysis in the context of ongoing intelligence and investigative operations.

The FBI's intelligence analytic cadre covers three career paths (Tactical, Collection/Reporting and Strategic) and performs functions which include: understanding emerging threat streams to enhance domain knowledge and exploit collection opportunities; enhancing collection capabilities through the deployment of collection strategies; reporting raw intelligence in a timely manner; identifying human and technical source collection opportunities; performing domain analysis in the field to articulate the existence of a threat in the field offices' area of responsibility; performing strategic analysis at FBI HQ to ascertain the ability to collect against a national threat; serving as a bridge between intelligence and operations; performing confidential human source validation; and recommending collection exploitation opportunities at all levels. The products generated by intelligence analysis drive FBI investigative and operational strategies by ensuring they are based on an enterprise-wide understanding of the current and future threat environments.

Field Intelligence Groups

Field Intelligence Groups (FIGs) are the centralized intelligence components in the field that serve to integrate the intelligence cycle (requirements, collection, analysis, and dissemination) into field operations. In accordance with FBI policy and guidance to the field, it is the responsibility of the FIG to coordinate, guide, and support the field office's operational activities through the five core intelligence functions. These functions are: domain management; collection management; requirements-based (sometimes non-case) collection – including human intelligence (HUMINT); tactical intelligence analysis; 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 Special Agents (SAs) are required to perform one or more of the following primary functions: intelligence collection, Confidential Human Source (CHS) coordination, focused source recruitment, source development and validation, and partner relations.

All SAs assigned to the FIG work closely with IAs to report observations indicating new trends in the local environment, collect key intelligence based upon the FBI's priority threat or vulnerabilities, and spot areas and targets for source recruitment. FIG SAs serve to facilitate the handling of cross-

programmatic intelligence information obtained from CHS debriefings. To do this effectively, HUMINT collectors (SAs) on the FIG must maintain close and constant communication with other collectors (SAs) and embedded IAs on investigative squads in order to augment their collection abilities beyond reporting on the squad's investigations.

Foreign Language Program

The Foreign Language Program (FLP) provides quality language solutions, analysis, and cultural expertise to the FBI and its partners. The FBI's success at protecting the United States from future terrorist attacks, countering foreign intelligence operations and espionage, and dismantling transnational organized criminal enterprises is increasingly dependent upon maximizing the usage and deployment of its linguist workforce, language tools, and technology. The FBI workforce has certified capabilities in over 90 languages and dialects in a distributed environment spanning approximately 100 FBI domestic and overseas locations. The FLP promulgates policies and compliance requirements to ensure true fidelity of the finished English-language intelligence product. Additionally, the FLP develops the foreign language skills of the FBI employees through on-going language testing, assessments and multi-tiered training strategies designed to build and sustain a high performance intelligence workforce.

Language Analysis

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. Language analysis is a critical process in the FBI's effort to acquire and accurately process real-time, actionable intelligence to detect and prevent foreign-originated terrorist attacks against the Nation. The FBI's language analysis capabilities promptly address all of its highest priority counterterrorism intelligence translation requirements, often within 24 hours. Language Analysts and English Monitor Analysts also play a significant role in the FBI's cyber, counterintelligence and criminal investigative missions.

National Virtual Translation Center

The National Virtual Translation Center (NVTC) was established by Congress under Title IX, Section 907 of the USA Patriot Act (2001) to provide accurate and timely translations to all elements of the U.S. Intelligence Community (IC). Since its inception, NVTC has complemented foreign language translation capability and provided flexibility and agility in translation support ranging from high-volume surges to immediate needs for language translations to its customers. NVTC operates within a virtual model that connects NVTC program staff, translators, field offices and customers nationwide via a common web-based workflow management system. NVTC has achieved steady business growth since inception with an average growth for the past three years of approximately 29 percent covering customers from the IC, the Department of Defense, and non-IC. It has demonstrated its capability as a living model for inter-agency collaboration with proven effective and economical foreign language translation service that offers scalability, agility, and expansive capabilities of more than 120 foreign languages and dialects from high-priority to rare languages.

Intelligence Training

Ensuring each subset of the FBI's intelligence workforce is equipped with the necessary specialized skills and expertise is critical to the organization's ability to successfully fulfill its mission. The FBI's extensive intelligence training program leverages expertise within the organization and throughout its partners in the intelligence, academic, and industrial communities to ensure the best educational opportunities are available to the FBI's workforce. In addition, the FBI's training program identifies and coordinates the certification of adjunct faculty, communicates educational and developmental opportunities available outside the FBI, and facilitates opportunities for research related to intelligence analysis. Moreover, the FBI is pursuing an integrated approach to training that brings employees

together at the beginning of their careers to understand the importance and impact of an integrated intelligence and operational methodology—a model that continues throughout the organization's intermediate and advanced courses of instruction.

Office of Partner Engagement
The OPE implements initiatives and strategies which support engagement, communication, coordination, and cooperation efforts with law enforcement, intelligence, public and private agencies and partners in a continuous effort to enhance the FBI's capabilities in the domestic architecture for national intelligence. The OPE accomplishes this mission by establishing and maintaining methods and practices to enhance engagement, coordination, and information sharing with the U.S. Intelligence Community; intelligence commander groups; federal, state, local, and tribal law enforcement; and public and private organizations and working groups.

Exploitation Threat Section
The Exploitation Threat Section (XTS) leads law enforcement and intelligence efforts in the United States to defeat terrorism by targeting terrorist communications, and for identifying long-term, threat-related issues that may affect FBI investigative or operational strategy against terrorist targets. XTS is the focal point between the intelligence and law enforcement communities for the coordination of domestic (CONUS) threats, and the facilitation of sharing threat information with Federal, state and local authorities.

Foreign Terrorist Tracking Task Force
The Foreign Terrorist Tracking Task Force (FTTTF) provides information that prevents foreign terrorists and their supporters from entering the United States or which leads to their removal, location, detention, prosecution, or other action. FTTTF utilizes specialized analytical techniques, technologies, and data analysis to enhance terrorist identification, tracking, and risk assessments.

Terrorist Screening Center
The Terrorist Screening Center (TSC) consolidates and coordinates the U.S. Government's approach to terrorist screening, and facilitates the sharing of terrorism information to protect our Nation and foreign partners. In order to identify, prevent, deter, and disrupt potential terrorist activity, the TSC's main objective is to maintain a thorough, accurate, and current database of known and suspected terrorists, and to share this information with law enforcement, intelligence, screening, and regulatory agencies at the federal, state, local, territorial, tribal, and international levels. This effort includes direct support for the FBI, Department of Justice, Department of Homeland Security, Department of State, the ODNI, the USIC, and other major federal law enforcement, screening, and regulatory agencies. The TSC accomplishes this mission through a unique, interagency business model that incorporates information technology and information sharing, as well as operational and analytical expertise from its interagency specialists.

In May 2014, the National Security Council (NSC) tasked the TSC to conduct a Transnational Organized Crime (TOC) Actor watchlisting and screening pilot ("Pilot") using law enforcement agency information targeting three key TOC groups. The purpose of the Pilot is to assess the effectiveness of applying the proven terrorist watchlisting and screening model to TOC Actors, and potentially other threats to national security. At present, the FBI and DEA are consolidating data on approximately 2,000 persons identified for inclusion in the TOC Pilot, and will provide data to the TSC. The TSC has also completed limited technical development required to support watchlisting for the TOC Pilot and is able to ingest TOC data into TSC systems.

Infrastructure and Technology

The FBI's infrastructure and technology helps 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 classified side of the comprehensive system includes secure workspaces, or Sensitive Compartmented Information Facilities (SCIFs) and a secure information sharing capability through the Sensitive Compartmented Information Operations Network (SCION), the FBI enterprise network for processing, transmitting, storing and sharing information at the Top Secret (TS)/Sensitive Compartmented Information (SCI) level, enabling FBI analysts to connect with the USIC through a connection to the Joint Worldwide Intelligence Communication System (JWICS) and utilize powerful applications to extract and analyze intelligence data in an efficient and timely manner. 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

A Sensitive Compartmented Information Facility (SCIF) is an accredited room, group of rooms, floors, or buildings where national security professionals collect, process, exploit, analyze, disseminate, and/or store Sensitive Compartmented Information. SCIFs are outfitted with Information Technology, telecommunications, general office machines, and requisite infrastructure to process unclassified through Top Secret information. SCIFs are afforded intrusion detection and access control systems to prevent the entry of unauthorized personnel.

Sensitive Compartmented Information Operations Network (SCINet)

SCINet is a compartmented network for Top Secret information which is administered by employing increased security measures, enforcing user accountability, and enhancing information assurance methodology.

II. Decision Unit Performance and Resources

A. *Intelligence Decision Unit*

1. Performance and Resource Tables

DOJ Strategic Goal/Objective: Goal 1: Prevent Terrorism and Promote the Nation's Security Consistent with the Rule of Law (Objectives 1.1 and 1.3), Goal 2: Prevent Crime, Protect the Rights of the American People, and Enforce Federal Law (Objectives 2.1-2.5), and Goal 3: Ensure and Support the Fair, Impartial, Efficient, and Transparent Administration of Justice at the Federal, State, Local, Tribal and International Levels (Objective 3.1).											
Decision Unit: Intelligence											
RESOURCES		**Target**		**Actual**		**Projected**		**Changes**		**Requested (Total)**	
		FY 2014		**FY 2014**		**FY 2015**		**Current Services Adjustments & FY 2016 Program Changes**		**FY 2016 Request**	
Total Costs and FTE		**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		6,712	1,608,611	6,766	1,647,492	6,800	1,654,977	5	23,471	6,805	1,678,448
TYPE / STRATEGIC OBJECTIVE	**PERFORMANCE**	**FY 2014**		**FY 2014**		**FY 2015**		**Current Services Adjustments & FY 2016 Program Changes**		**FY 2016 Request**	
Performance Measure	% of Counterterrorism FISA collection reviewed by the Language Program: • Audio • Text • Electronic File		100% 100% 100%		100% 100% 100%		100% 100% 100%		- - -		100% 100% 100%
Performance Measure: ***Responsiveness***	% of IIRs citing US Intelligence Community (USIC) Priority 1 or 2 requirements		75%		81%		75%		-		80%
Data Definition, Validation, Verification, and Limitations: • Intelligence measures are provided by records maintained and verified by the FBI's Directorate of Intelligence. No known limitations exist with the available data as currently reported.											

PERFORMANCE MEASURE TABLE

Decision Unit: Intelligence

Performance Report and Performance Plan Targets		FY 2010	FY 2011	FY 2012	FY 2013	FY 2014		FY 2015	FY 2016
		Actual	Actual	Actual	Actual	Target	Actual	Target	Target
Performance Measure	% of Counterterrorism FISA collection reviewed by the Language Program:								
	• Audio	95%	83%	79%	100%	100%	100%	100%	100%
	• Text	98%	138%	56%	100%	100%	100%	100%	100%
	• Electronic File	39%	39%	82%	79%	100%	100%	100%	100%
Performance Measure: ***Responsiveness***	% of IIRs citing US Intelligence Community (USIC) Priority 1 or 2 requirements	N/A	N/A	76%	76%	75%	81%	75%	80%

2. Performance, Resources, and Strategies

The resources within the Intelligence Decision Unit contribute to all three of the DOJ strategic goals. Additionally, these resources are critical to the intelligence cycle at the heart of the FBI's strategy map in the following objectives: "Collection/Investigation;" "Intelligence Dissemination and Integration;" "Analysis;" and "Action and/or Requirements."

The mission of the FBI's Intelligence Program is to collect, produce, and disseminate actionable intelligence that enables the FBI to identify and counter current and emerging threats. The DI is responsible for managing the FBI Intelligence Program and ensuring that the prioritization of its functions comports with the formulation of budgetary requirements. DI carries out these functions through embedded intelligence elements at FBI HQ and in each field office.

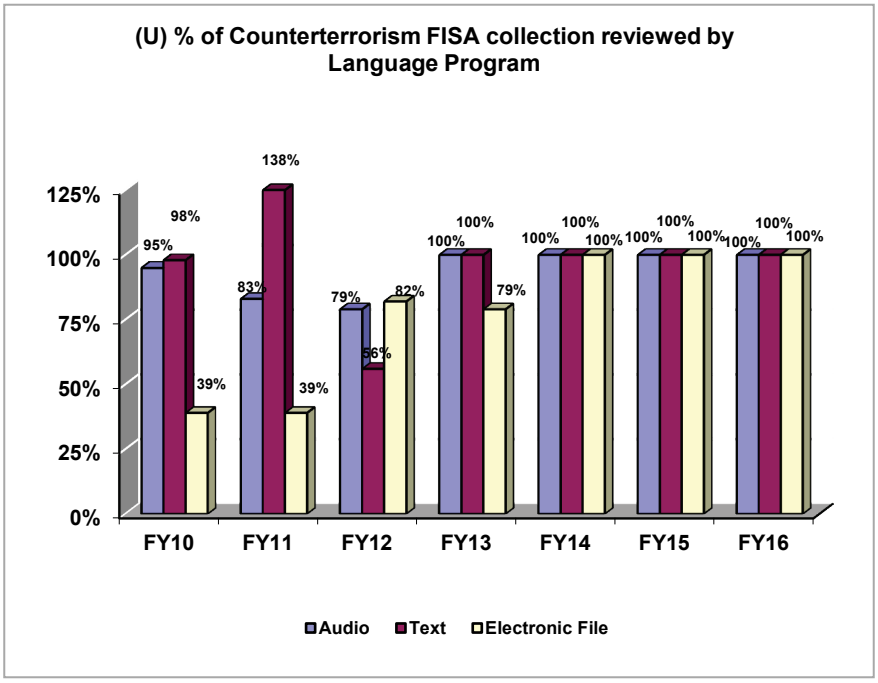
a. Performance Plan and Report for Outcomes

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

FY 2014 Targets:
Audio: *100%*
Text: *100%*
Electronic: *100%*

FY 2014 Actuals:
Audio: *100%*
Text: *100%*
Electronic: *100%*

FY 2016 Targets:
Audio: *100%*
Text: *100%*
Electronic: *100%*



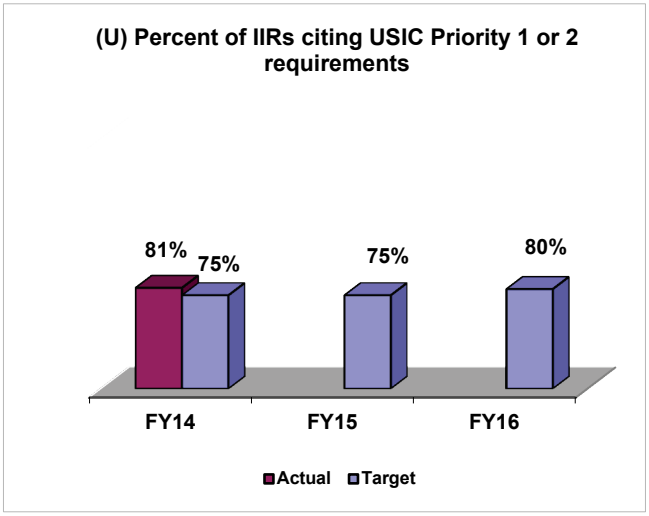
Discussion: Targets have been consistently set at 100 percent to account for technological improvements that allow for the identification of collected data that requires review and translation by the FBI's Language Program. This review rate reflects cases that have a Foreign Language component and have been marked "for translation." Language Program Resources and FISA foreign language collections have remained consistent since FY 2012. A potential challenge could occur if collection is unexpectedly high in languages for which analytic capability is extremely scarce, review rates may decrease and the target may not be met.

Performance Measure – Responsiveness: Percent of FBI Intelligence Information Reports (IIRs) citing U.S. Intelligence Community (USIC) Priority 1 or 2 requirements

FY 2014 Target: 75%
FY 2014 Actual: 80%

FY 2016 Target: 80%

Discussion: This measure was designed to determine whether the FBI is collecting and meeting the needs of the USIC by reporting against the highest priority requirements as identified externally. To link reporting to collection requirements is a foundational intelligence capability, and one which should drive collection behavior toward higher priority needs. The proposed FY 2015 and FY 2016 targets are based on current trends and recommended future performance. The target was increased from 75 percent to 80 percent in FY 2016 because the results for this measure have consistently been at or exceeding previous targets. Increasing the target to 80 percent for FY 2016 may allow for increased efforts to ensure FBI intelligence production is in alignment with ODNI priorities.



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

Please refer to the classified addendum.

b. Strategies to Accomplish Outcomes

The FBI's Intelligence Program strives 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. Moreover, the FBI is committed to fulfilling its responsibility to safeguard national security. As such, it continues to proactively adapt and improve upon collection, analysis, and dissemination capabilities while also protecting the civil liberties and rights of all Americans.

B. Counterterrorism/Counterintelligence Decision Unit

COUNTERTERRORISM/COUNTERINTELLIGENCE DECISION UNIT TOTAL	Perm. Pos.	FTE	Amount ($000)
2014 Enacted	13,074	12,295	$3,332,896
2015 Enacted	13,091	12,382	3,354,555
Adjustment to Base and Technical Adjustments	(68)	13	56,589
2016 Current Services	13,023	12,395	3,411,144
2016 Program Increases	…	…	8,842
2016 Program Decreases	…	…	(19,616)
2016 Request	13,023	12,395	$3,400,370
Total Change 2015-2016	**(68)**	**13**	**$45,815**

1. Program Description

The FBI's Counterterrorism/Counterintelligence (CT/CI) Decision Unit is comprised of most of the Counterterrorism Division (CTD)[4], the entire Weapons of Mass Destruction Directorate (WMDD), the entire Counterintelligence Division (CD), a portion of the Cyber Computer Intrusions Program within the Cyber Division, a portion of the Critical Incident Response Group (CIRG), and a portion of the Legat Program that supports the FBI's CT and CI missions overseas. 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 Divisions, administrative divisions, and staff offices) are calculated and allocated to the decision unit.

Counterterrorism Program

The mission of the FBI's CT program, which is managed by CTD, 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 by coordinating and providing operational and/or material assistance, technical expertise, research and training, negotiations and the deployment of investigative, tactical and logistical resources and materials. 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 disseminated to 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, both international and domestic terrorism investigations, are managed at FBI HQ, 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

[4] Please note that while the TSC and the FTTTF are part of the FBI's CT Program, their resources are allocated to the Intelligence Decision Unit (IDU). The Foreign Terrorist Tracking Task Force (FTTTF) and the Exploitation Threat Section, both are which are managed by the Counterterrorism Division (CTD), are allocated to the Intelligence Decision Unit (IDU) because the work that those two entities perform is intelligence-related. Similarly, the Counterterrorism Analysis Section is embedded within CTD but is allocated to the IDU. Additionally, the Terrorist Screening Center (TSC), which supports the FBI's CT mission, is also allocated to the IDU.

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, and specifically on the identification of terrorist training, fundraising, recruiting, logistical support, and pre-attack planning.

The FBI has moved aggressively to implement a comprehensive plan that has fundamentally transformed and enhanced the organization. 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. Instead, it is dedicated to disrupting terrorist plots before they are executed. The FBI's CT Program has five priorities:

- Detect, disrupt, and dismantle terrorist sleeper cells in the U.S. before they act;
- Identify and prevent acts of terrorism by individuals with a terrorist agenda acting alone;
- Detect, disrupt, and dismantle terrorist support networks, including financial support networks;
- 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
- 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 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. Additionally, 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 Terrorist Screening Center (TSC) and Foreign Terrorist Tracking Task Force (FTTTF) help identify terrorists and keep them out of the U.S. Finally, the Counterterrorism Analysis Section "connects the dots" and assesses the indicators of terrorist activity against the U.S. from a strategic perspective.

Transformation efforts are continuing to make 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 Counterterrorism operations into four branches, each of which focuses on a different aspect of the current terrorism threat facing the Nation. Operations Branch I (OPS I) within the CTD is responsible for protecting the U.S. against international terrorism. It is comprised of two sections: CONUS and OCONUS. Operations Branch II (OPS II) within the CTD supports, coordinates,

and manages terrorism-related investigations. The Operations Branch III (OPS III) within the CTD was established to devise and maintain the FBI's overall strategies against the most significant terrorism threats, and produce timely, comprehensive, and sophisticated intelligence products. This new structure with CTD ensures a threat-centric, intelligence-driven approach to operations. The fourth branch is the Operational Support Branch, which coordinates and provides operational and/or material assistance, technical expertise, research, and training to assist an on-scene commander through crisis management, negotiations, and the deployment of investigative, tactical, and logistical resources and materials. These components are staffed with SAs, IAs, and subject matter experts who work closely with investigators in the field to 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. Through the Director's daily meetings with other IC executives, the regular exchange of personnel among agencies, joint efforts in specific investigations and in the National Counterterrorism Center (NCTC), the TSC, other multi-agency entities, and the co-location of personnel at Liberty Crossing, it is clear that the FBI and its partners in the IC are now integrated at nearly 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 SAs and crime scene experts to assist in the investigation of overseas attacks. Their work has played a major role in successful international operations.

Weapons of Mass Destruction Directorate (WMDD)

The WMDD was established in FY 2006 to create a unique combination of law enforcement authorities, intelligence analysis capabilities, and technical subject matter expertise. Creation of the WMDD enabled the FBI to bring its WMD preparedness, prevention, and response capabilities into a single, focused organization, which builds a cohesive and coordinated FBI approach to WMD.

The WMDD's mission is to lead the FBI's efforts to deny state and non-state sponsored adversaries' access to WMD materials and technologies, to detect and disrupt the use of WMDs, and to respond to WMD threats and incidents. WMDD is responsible for preventing, countering, and investigating threats of terrorism or proliferation involving chemical, biological, radiological, nuclear, and explosive weapons.

The WMDD coordinates the FBI's WMD program through a multifaceted approach that addresses all areas of the WMD incident spectrum from prevention through response. This approach includes:

- *Preparedness* - This perspective incorporates the development of comprehensive plans and policies. It also implements planning, training, and practice exercises to ensure that the FBI and its USG partners are ready to respond to WMD threats.

- *Countermeasures* – Countermeasures are actions taken to counter, eliminate, or offset the WMD threat. This includes outreach activities, tripwires, and more specialized countermeasures.

- *Investigations and Operations* – The WMDD investigates the threatened, attempted, and actual use of a WMD, as well as the attempted or actual transfer of materials, knowledge, and technology needed to create a WMD. WMDD coordinates the FBI's efforts to ensure a robust capability that can collect evidence in contaminated areas, disarm hazardous devices, and provide direct command and control support in on-scene situations.

- *Intelligence* – The WMDD proactively leverages timely and relevant intelligence to drive preparedness, countermeasures, and investigative programs that are designed to prevent a threat from becoming a reality. The FBI utilizes this intelligence to combat WMD threats and events and also shares the intelligence products with the intelligence community to globally improve awareness of the WMD threat.

WMDD's case management responsibilities fall into two primary categories: WMD terrorism and WMD proliferation. The WMD terrorism cases include non-attributed instances involving the threat, attempt, or use of a WMD. Cases fall into the proliferation category, however, when an organization or nation state attempts to acquire material and expertise relevant to a WMD program.
In July 2011, the FBI combined the operational activities of the Counterintelligence Division's counterproliferation program with the subject matter expertise of the WMDD, and the analytical capabilities of the Directorate of Intelligence to create a Counterproliferation Center (CPC) in order to detect, deter, and defeat the threat posed by state-sponsored groups, individuals, and/or organizations as they attempt to obtain WMD or other sensitive technologies. All investigations concerning counterproliferation will be managed by the CPC, including all investigations directed to prevent the acquisition of information and technologies which would enhance a foreign government's abilities to create, use, share, or sell WMDs, including: Chemical, Biological, Radiological, Nuclear, Explosive, missile delivery system, space, or advanced conventional weapons or components. The Counterproliferation Center has been extremely successful in combating illegal/illicit technology transfer and proliferation. Since the stand-up of the CPC, there have been over 50 arrests stemming from CPC cases.

Counterintelligence Program
In connection with its efforts to enhance the CI Program's detection, penetration and defeat of foreign intelligence threats, the Counterintelligence Division has developed a National Strategy for Counterintelligence to delineate specific actions designed to enhance the FBI's capacity to address its counterintelligence responsibilities by providing:

- A centrally controlled and managed CI Program that guides, directs, and provides adequate resources to support an effective national CI effort.

- A shift in emphasis of the FBI's organizational culture from a reactive criminal emphasis to a proactive national security emphasis.

- An approach that emphasizes both prosecutions for espionage activity, when warranted, and other lawful neutralization techniques when espionage prosecution is not possible.

- A reinvigorated asset (human source) recruitment and validation program.

- A dynamic analytical process to assess and rank both foreign intelligence threats and, by extension, national counterintelligence priorities.

- A restructured and improved CI information management and sharing program both within the FBI and between the FBI and other IC components.

- A commitment to maintain a fully trained, highly experienced workforce of FBI agents, analysts, and professional support with recognized expertise in priority areas.

Cyber Program

The FBI's Cyber Program, which is managed by the Cyber Division, integrates Headquarters and field resources dedicated to combating national security computer intrusions. This enables 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 within the CT/CI DU are counterterrorism, counterintelligence, and national security computer intrusion investigations.

Also within the FBI Cyber Program is the FBI-led National Cyber Investigative Joint Task Force (NCIJTF). The NCIJTF serves as a multi-agency national focal point for coordinating, integrating, and sharing pertinent information relating to cybersecurity threat investigations. The NCIJTF maximizes the government's impact under a unified strategy that identifies, mitigates, and neutralizes cyber threats through the combined counterintelligence, counterterrorism, intelligence, and law enforcement authorities and capabilities of its member agencies.

Critical Incident Response Program

The 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 Federal, State, local, tribal and international law enforcement partners. CIRG personnel are on call around the clock to respond to crisis incidents.

CIRG's readiness posture provides the USG with the ability to counter a myriad of CT/CI threats—from incidents involving WMDs 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, and CIRG encompasses all of these elements.

CIRG also manages the FBI's mobile surveillance programs – the Mobile Surveillance Teams - Armed (MST-A) and the Mobile Surveillance Teams (MST) - and its Aviation Surveillance program. MST-As are comprised of armed agents who perform surveillances of targets that might have the propensity for violence; MSTs are comprised of unarmed investigative specialists who perform surveillances of targets who are unlikely to be violent. MST-As, MSTs, and Aviation Surveillance provide critical support to CT and CI investigations.

Legal Attaché (Legat) Program

Legats are the forward element of the FBI's international law enforcement effort and often provide the first response to crimes against the U.S. and its citizens that have an international nexus. The FBI's Legat Program is managed by the International Operations Division (IOD). The counterterrorism component of the Legat Program is comprised of SAs 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.

B. *Counterterrorism/Counterintelligence Decision Unit*

1. Performance and Resource Tables

DOJ Strategic Goal/Objective Goal 1: Prevent Terrorism and Promote the Nation's Security Consistent with the Rule of Law (Objectives 1.1, 1.2, 1.3 and 1.4)											
Decision Unit: Counterterrorism/Counterintelligence											
WORKLOAD/ RESOURCES		**Target**		**Actuals**		**Projected**		**Changes**		**Requested (Total)**	
		FY 2014		**FY 2014**		**FY 2015**		**Current Services Adjustments & FY2016 Program Changes**		**FY 2016 Request**	
Number of Cases: Counterterrorism, Counterintelligence, & Computer Intrusions		†				†		†		†	
Total Costs and FTE		**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		12,370	3,356,825	12,295	3,332,896	12,382	3,354,555	13	45,815	12,395	3,400,370
TYPE/ STRATEGIC OBJECTIVE	**PERFORMANCE**	**FY 2014**		**FY 2014**		**FY 2015**		**Current Services Adjustments & FY2016 Program Changes**		**FY 2016 Request**	
Program Activity/ 1.1; 1.2	**1. Counterterrorism (CT)**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		7,175	1,946,959	7,132	1,999,080	7,182	1,945,612	8	26,570	7,190	1,972,215
Workload -- # of cases investigated (pending and received)		†		6,688		†		†		†	
Performance Measure	Number of Terrorism Disruptions (2014-2015 Priority Goal)	50		190		125				125	
Program Activity/ 1.3	**2. Counterintelligence**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		4,161	1,107,752	4,136	1,099,855	4,209	1,140,549	4	15,577	4,213	1,156,126
Performance Measure	Percentage of Counterespionage Actions and Disruptions Against National Counterintelligence Priorities that Result from FBI Outreach (2014-2015 Priority Goal)	10%		7.3%		10%				10%	
Program Activity/ 1.4	**3. Cyber**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		1,034	302,114	1,027	233,961	991	268,394	1	3,668	992	272,029
Performance Measure	Number of Computer Intrusion Program Disruptions and Dismantlements (2014-2015 Priority Goal)	100		2,492		500				500	
Efficiency Measure	Cost avoidance from online Cyber training ($000)	$2,750		$2,416		$2,000		-		$2,000	

Data Definition, Validation, Verification, and Limitations:

- 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. Percentages are updated based upon the most recent field review. Cost avoidance data are based upon estimates of cost savings per student taking an online course, compared with an in-service training.
- The data source for 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. 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.

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

Performance Report and Performance Plan Targets		FY 2010	FY 2011	FY 2012	FY 2013	FY 2014		FY 2015	FY 2016
		Actual	Actual	Actual	Actual	Target	Actual	Target	Target
Performance Measure	Number of Terrorism Disruptions (2014-2015 Priority Goal)	N/A	N/A	N/A	180	50	190	125	125
Performance Measure	Percentage of Counterespionage Actions and Disruptions Against National Counterintelligence Priorities that Result from FBI Outreach (2014-2015 Priority Goal)	N/A	N/A	N/A	N/A	10%	7.3%	10%	10%
Performance Measure	Number of Computer Intrusion Program Disruptions and Dismantlements (2014-2015 Priority Goal)	N/A	N/A	N/A	N/A	100	2,942	500	500
Efficiency Measure	Cost avoidance from online Cyber training ($000)	$819	$4,987	$2,395	$3,585	$2,750	$2,416	$2,000	$2,000

2. Performance, Resources, and Strategies
The resources within the Counterterrorism/Counterintelligence Decision Unit contribute to the Department's Strategic Goal 1: Prevent Terrorism and Promote the Nation's Security Consistent with the Rule of Law, Objectives 1.1, 1.2, 1.3 and 1.4. This decision unit also ties directly to the top three FBI priorities: Priority 1 – Protect the United States from terrorist attacks; Priority 2 – Protect the United States against foreign intelligence operations and espionage; and Priority 3 – Protect the United States against cyber-based attacks and high-technology crimes.

Counterterrorism (CT)

a. Performance Plan and Report for Outcomes
The FBI must understand all dimensions of the threats facing the Nation and address them with new and innovative investigative and operational strategies. Additionally, the FBI must be able to effectively respond to the challenges posed by unconventional terrorist methods, such as the use of chemical, biological, radiological, explosive, and nuclear materials. When terrorist acts do occur, the FBI must rapidly identify, locate, and apprehend the perpetrators and their affiliates. As part of its CT mission, the FBI will continue to combat terrorism by investigating those persons and countries that finance terrorist acts.

b. Strategies to Accomplish Outcomes
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 work in this area includes improved intelligence gathering and sharing, improved analytical capabilities, and enhanced training and liaison.

c. Priority Goals
The FBI contributes to Priority Goal 1, Protect Americans from terrorism and other threats to National Security, including cyber threats.

***Performance Measure*:** Number of Terrorism Disruptions

FY 2014 data will serve as a baseline for this new measure.

FY 2014 Target:	50
FY 2014 Actual:	190
FY 2016 Target:	125

Discussion of FY 2014 Results:
The FBI exceeded its annual target for the number of terrorism disruptions effected through CT investigations. In executing the FBI's number one priority to protect the U.S. from terrorist attacks, disruptions remain a key statistic that directly speaks to its CT responsibilities. The FBI is committed to stopping terrorism of any kind at any stage as evidenced by its transformation into a proactive agency. To fulfill DOJ's mission of defeating terrorism, the FBI focused resources on targeting and disrupting terrorist threats and groups by leveraging its workforce and ensuring the use of the latest technology to

thwart emerging trends. Key to its success in terrorism disruption is CT agent training, which resumed normal levels in FY 2014 due to a restored budget.

Counterintelligence

Performance Measure: Percentage of Counterespionage Actions and Disruptions against National Counterintelligence Priorities that Result from FBI Outreach

FY 2014 data will serve as a baseline for this new measure.

FY 2014 Target:	10%
FY 2014 Actual:	7.3%
FY 2016 Target:	10%

Discussion of FY 2014 Results:
In FY 2014, espionage remained one of the CI Program's most significant threats. In addition to traditional tradecraft used to access economic, national security, and proprietary information, the FBI continued to disrupt and monitor more advanced methods to penetrate organizations. Of the CI Program's total law enforcement actions and disruption activities, espionage-related threats accounted for more than 13 percent of the FBI's total CI accomplishments against NIPF-sponsored actors or entities. These accomplishments included approximately 40 arrests, 12 convictions, and nearly 30 indictments. More than seven percent of the espionage-related accomplishments resulted from FBI outreach (as opposed to other investigative activities or intelligence production).

The FBI relies heavily on its coordination with the U.S. IC, Other Government Agencies, international partners, and public or private entities. These relationships increase intelligence collection, identify emerging threats, and disrupt priority threats. As a result of the CI Program's SPC Program, the FBI organized regular CI working group meetings, formal alliances with the academic and business sectors, and thousands of briefings to organizations vulnerable to foreign intelligence intrusions. These programs led to more than 3,600 referrals, nearly 1,300 leads, and the establishment of more than 200 tripwires.

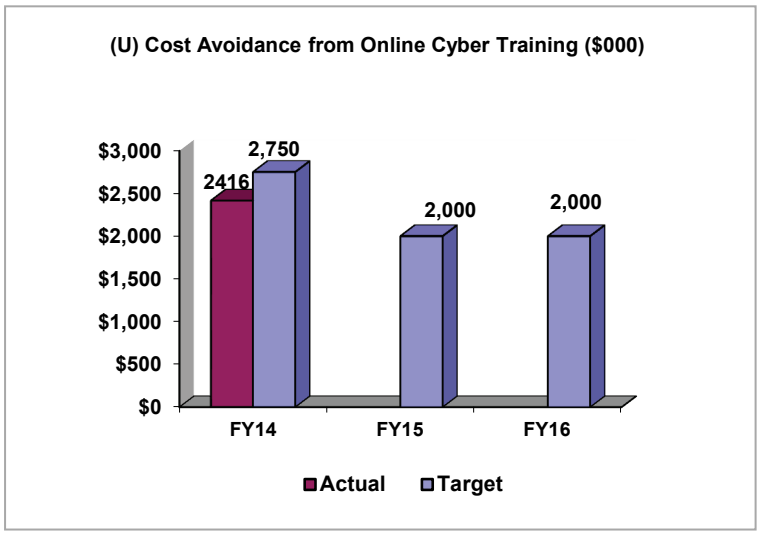
While the FBI lagged its FY 2014 target by nearly three percent, the CI Program demonstrated significant progress toward converting its outreach into productive foreign intelligence collection and investigations. In FY 2014, the SPC Program increased its outreach efforts, and approximately 10 percent of total CI investigative activities and five percent of total accomplishments were directly predicated by outreach. Also, strategic partnerships contributed to the dissemination of approximately 2,700 finished intelligence products. As hostile foreign intelligence services use more sophisticated techniques to breach key economic, national security, and technology sectors, it is essential the FBI develop more robust partnerships outside the intelligence and law enforcement communities. In FY 2015, threat-prioritized strategic outreach will remain an important initiative for the CI Program. Further, the CI Program will address the emerging threat of foreign nation states increasingly using commercial enterprises to achieve their desired intelligence collection and operational capabilities.

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.

Efficiency Measure: Cost Avoidance from Online Cyber Training

FY 2014 Target: $2,750,000
FY 2014 Actual: $2,416,000
FY 2016 Target: $2,000,000



Discussion: The FBI's Cyber Program provides online training for its introductory level courses, intermediate and advanced courses for SAs in the Cyber Career Path, and online proficiency tests ("test out") for all levels of its core curriculum. The FBI implemented multiple distance learning models in FY 2013. The student population for the introductory classes is quite broad, including FBI SAs, 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. The population for the intermediate and advanced core courses is primarily SAs in the Cyber Career Path. Intermediate and advanced courses require significant hands-on exercises with intrusion investigation software tools. For SAs in the Cyber Career Path, 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, are integrated in the program.

In addition to offering introductory level online training via the FBI Virtual Academy (the FBI's internal intranet training system), the FBI offers training over the Internet. The Cyber Division also implemented an updated distance learning system to deliver sophisticated online training in FY 2013. This system has advanced functionality to support the online delivery of intermediate and advanced level courses with hands-on exercises. The system uses virtual machines and virtual networks to mimic what the Cyber Agent will encounter in the field, and supports a number of training modalities to include teleconferenced lectures and labs, archived lectures, online live tutoring, and self-paced training and exercises. Taken together, these existing and new online training options will allow the FBI to offer improved courses to all employees, including those in remote locations, as well as state and local investigators and FBI employees who might not have been able to have access to previous training opportunities.

The FBI believes that it did not meet the FY 2014 target due to an increased demand for in-person training, and a corresponding decrease in the demand for online training. As a result of sequestration, there were limited offerings of in-person training. However, the FBI's final FY 2014 appropriation allowed the FBI to offer in-person training opportunities that were not available in FY 2014.

***Performance Measure*:** Number of Computer Intrusion Program Disruptions and Dismantlements

FY 2014 data will serve as a baseline for this new measure.

FY 2014 Target:	100
FY 2014 Actual:	2,492
FY 2016 Target:	500

Discussion of FY 2014 Results:
Throughout FY 2014, FBI CyD successfully executed its mission by identifying, pursuing, and defeating cyber adversaries targeting global U.S. interests. FBI CyD substantially exceeded its baseline performance target in disrupting and dismantling the top cyber threat actors because of significant, coordinated operational activity. For example, in May 2014, the FBI New York Field Office announced the results of the largest law enforcement cyber action in U.S. history. This takedown was of a particularly insidious computer malware known as Blackshades, which was sold and distributed to thousands of people in more than 100 countries and was used to infect more than half a million computers worldwide. As a result of this takedown, 40 FBI field offices conducted approximately 100 interviews, executed more than 100 e-mail and physical search warrants, and seized more than 1,900 domains used by Blackshades' users to control victims' computers. This year-end performance reflects the FBI's increased operational capability to interrupt and eliminate cyber actors from engaging in activities that poses a threat to our national security.

During FY 2014, FBI CyD, in coordination with other law enforcement agencies and members of the IC, gathered evidence of computer intrusion techniques, patterns of criminal activity, and copies of malicious software. When possible, the FBI notified victims of computer intrusions, which enabled them to protect themselves against such tactics. In many circumstances victims were unaware their networks had been compromised. The FBI's information sharing and analysis capabilities have ensured that computer intrusion information and other information about cyber threats are also shared with other agencies in support of their independent cyber-related missions.

Please refer to the classified addendum for additional performance measures.

C. Criminal Enterprises and Federal Crimes Decision Unit

CRIMINAL ENTERPRISES/FEDERAL CRIMES DECISION UNIT TOTAL	Perm. Pos.	FTE	Amount ($000)
2014 Enacted	12,631	12,018	$2,758,551
2015 Enacted	12,681	12,115	2,848,602
Adjustment to Base and Technical Adjustments	60	10	27,085
2016 Current Services	12,741	12,125	2,875,687
2016 Program Increases	…	…	8,539
2016 Program Decreases	…	…	(16,313)
2016 Request	12,741	12,125	$2,867,912
Total Change 2015-2016	**60**	**10**	**$19,310**

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, which are managed by the Criminal Investigative Division (CID). The DU includes:

- The FBI's Organized Crime, Gang/Criminal Enterprise (G/CE), and Criminal Intelligence programs;
- The Financial Crime, Integrity in Government/Civil Rights, and Violent Crime programs;
- The Public Corruption and Government Fraud programs, part of the Financial Crime program, 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 including, Criminal Computer Intrusions and the Internet Crime Complaint Center (IC3); and a share of the FBI's Legat program.

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

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

Financial Crime

***White Collar Crime*:** The White Collar Crime (WCC) program addresses principal threats, including: public corruption (including government fraud and border corruption); corporate fraud; securities and commodities fraud; mortgage fraud and other financial institution fraud; health care fraud; money laundering; and other complex financial crimes.

Violent Criminal Threats
The mission of the Violent Criminal Threat Section (VCTS) is to combat violent criminal threats and to disrupt and dismantle local, regional, national, and transnational cells of criminal enterprises that pose the greatest threat to the economic and national security of the U.S.

The FBI's Violent Crime (VC) component combats the most significant violent crime offenders and threats falling within the FBI's investigative jurisdiction. Violent crime continues to threaten communities within the U.S. and its citizens. Major violent crime incidents such as mass killings, school shootings, serial killings, and violent fugitives can paralyze whole communities and stretch state and local law enforcement resources to their limits. Particular emphasis is directed toward matters involving serial violent offenders and significant violence, including bank robberies, armored car robberies, fugitives, kidnappings for ransom, extortions, police killings, and assault on federal officers.

Cyber Program
Included under the purview of the Cyber Program within the CEFC DU are criminal computer intrusion investigations conducted by the Cyber Division and the FBI's Internet Crime Complaint Center.

Legal Attaché (Legat) Program
Crime-fighting in an era of increasing globalization and interconnectivity has become a truly international effort, and the people who make up the FBI's International Operations Division (IOD) and Legat Program work together to lead and direct the FBI's growing number of operations around the globe.

The FBI's Legats and their staffs work hard to combat crime, even as they partner with, and strengthen the bonds between law enforcement personnel throughout the world. Special Agents and professional staff working in IOD use their unique skill sets and knowledge to coordinate investigations large and small, by partnering with the FBI's criminal and intelligence divisions, foreign law enforcement, and U.S. and foreign intelligence and security services.

The IOD and Legat program work also includes a major training component, whether it is the support of the International Law Enforcement Academies in Budapest or Botswana, or teaching their law enforcement partners about conducting proper investigations at crime scenes or crisis management.

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

Program Objectives

White Collar Crime:

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

Cyber:

- Develop partnerships between the FBI and private sector, academia, and other public entities to support the FBI's mission and assist those institutions.
- Serve as a vehicle to receive, develop, and refer criminal complaints regarding cyber crime.
- Identify, develop, and deliver core and continuing education for Cyber investigators across all levels of the law enforcement, both domestic and international.

Civil Rights:

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

Gang Violence:

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

***Organized Crime*:**

- Combat transnational criminal organizations and collect resources supporting intelligence and investigation actions to disrupt and dismantle organized criminal activities worldwide.
- Continually assess the international organized crime threat in the country by outlining current state of FBI resources and better position the FBI to strategically direct investigatory resources to the highest threat areas.
- Execute a comprehensive strategy to disrupt and dismantle Semion Mogilevich Organization and Brothers' Circle through coordination with other agencies, including through the Threat Fusion Cells (TFCs).

Violent Crime:

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

Latin America/Southwest Border:

- Infiltrate, disrupt and dismantle Mexican and South and Central American Criminal Enterprises by targeting their center of gravity and by utilizing sensitive investigative and intelligence techniques to initiate long term proactive investigations.
- Expand and create new partnerships with the USIC and Other Government Agencies in order to better coordinate and facilitate the flow and utilization of intelligence against the threat posed by Mexican and South, and Central American Criminal Enterprises.
- Continually assess the in-country threat posed by Mexican and South and Central American Criminal Enterprises by outlining the current state of FBI resources and better positioning the FBI to strategically direct investigatory and intelligence resources to the highest threat areas.

2. PERFORMANCE/RESOURCES TABLE

Decision Unit: Criminal Enterprises and Federal Crimes

DOJ Strategic Goal/Objective Goal 2: Prevent Crime, Protect the Rights of the American People, and Enforce Federal Law. Objectives 2.1-2.5.

WORKLOAD/ RESOURCES		Target		Actual		Projected		Changes		Requested (Total)	
		FY 2014		FY 2014		FY 2015		Current Services Adjustments & FY 2016 Program Changes		FY 2016 Request	
Workload -- # of cases investigated (pending and received)		†				†		†		†	
Total Costs and FTE		**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		11,899	2,790,645	12,018	2,758,551	12,115	2,848,602	10	19,310	12,125	2,867,912
TYPE/ STRATEGIC OBJECTIVE	**PERFORMANCE**	**FY 2014**		**FY 2014**		**FY 2015**		**Current Services Adjustments & FY 2016 Program Changes**		**FY 2016 Request**	
Program Activity/ 2.3, 2.5	**1. White-Collar Crime/Cybercrime**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		5,474	1,283,697	5,528	1,268,933	5,572	1,310,357	6	8,883	5,578	1,319,240
Workload -- # of cases investigated (pending and received)		†				†		†		†	
Performance Measure	Restitutions & Recoveries / Fines ($000) • Intellectual Property Rights Violations • Public Corruption • White Collar Crimes (all other)	††		474,114 5,441,154		††		††		††	
Performance Measure	Convictions/Pre-Trial Diversions (total) • Intellectual Property Rights Violations **[Discontinued measure]** • Public Corruption • White Collar Crimes (all other)	††		1,087 2,695		†† †† ††		†† †† ††		†† †† ††	
Performance Measure	Number of Criminal Organizations Engaging in White-Collar Crimes Dismantled	368		464		368		…		368	
Efficiency Measure	% of Major Mortgage Fraud Investigations to all pending Mortgage Fraud Investigations	72%		73%		72%		…		72%	
Performance Measure	Number of Children Depicted in Child Pornography Identified by the FBI	††				††		††		††	
Performance Measure	Number of convictions for Internet fraud	††		12		††		††		††	
Performance Measure	Number of high-impact Internet fraud targets neutralized **[Discontinued measure]**	††		25		††		††		††	

TYPE/ STRATEGIC OBJECTIVE	PERFORMANCE	FY 2014		FY 2014		FY 2015		Current Services Adjustments & FY 2016 Program Changes		FY 2016 Request	
		FTE	$000	FTE	$000	FTE	$000	FTE	$000	FTE	$000
Program Activity/ 2.2, 2.4, 2.6	2. Criminal Enterprises/Civil Rights/Violent Crimes	6,425	1,506,948	6,490	1,489,618	6,543	1,538,245	4	10,427	6,547	1,548,672
Workload -- # of cases investigated (pending and received)			†				†		†		†
Performance Measure	Convictions/Pre-trial Diversions • Organized Criminal Enterprises • Gang/Criminal Enterprises • Crimes Against Children • Civil Rights		 †† †† †† ††		 723 7,338 1,570 205		 †† †† †† ††		 †† †† †† ††		 †† †† †† ††
Efficiency Measure	% of FBI OCDETF Investigations with links to CPOT-linked DTOs*		15%		20%		15%		…		N/A
Performance Measure	CPOT-Linked DTOs* • Disruptions • Dismantlements		 40 20		 150 31		 40 20		 … …		 N/A N/A
Performance Measure	Number of Organized Criminal Enterprise Dismantlements		38		82		38		…		38
Performance Measure	Number of Gang/Criminal Enterprises Dismantlements		99		167		99		…		99
Performance Measure	Number of Agents serving on Violent Crime Task Forces		†		1,121		†		†		†
Performance Measure	Average length of sentence in months Violent Crime		††				††		††		††

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 the end of the reporting period. Such changes are reflected in later reports.

– 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.

– 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.

*All CPOT related measures are proposed to be discontinued in FY 2016. The FBI does not have the ability to accurately track CPOT-linked investigative activity.

		FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013	FY 2014		FY 2015	FY 2016
		Actual	Actual	Actual	Actual	Actual	Actual	Actual	Target	Actual	Target	Target
Performance Measure	Restitutions/Recoveries/Fines ($000) • Intellectual Property Fraud • Public Corruption • White Collar Crimes (all other)	 238,832 157,440 19,516,406	 260,219 676,889 18,502,635	 5,389 220,787 15,956,528	 17,100 6,559,531 8,383,458	 4,628 1,178,976 14,027,036	 N/A N/A N/A	 N/A N/A N/A	 N/A N/A N/A	 474,114 5,441,154	 N/A N/A N/A	 N/A N/A N/A
Performance Measure	Convictions/Pre-Trial Diversions (total) • Intellectual Property Fraud • Public Corruption • White-Collar Crimes (all other)	 136 943 3,347	 116 987 3,834	 88 981 2,910	 84 954 3,357	 81 969 3,384	 N/A 924 3,529	 N/A 1,038 2,958	 N/A N/A 3,351	 1,087 2,695	 N/A N/A 3,351	 N/A N/A 3,351
Performance Measure	Number of Criminal Organizations Engaging in White Collar Crimes Dismantled	277	211	250	236	368	409	458	368	464	385	385
Efficiency Measure	% of Major Mortgage Fraud Investigations to all pending Mortgage Fraud investigations	56%	63%	66%	71%	71%	71%	72%	72%	73%	72%	72%
Performance Measure	Number of Children Depicted in Child Pornography Identified by the FBI	73	187	118	246	240	175	N/A	N/A		N/A	N/A
Performance Measure	Number of convictions for Internet fraud	N/A	N/A	N/A	N/A	27	21	22	N/A	12	N/A	N/A
Performance Measure	Number of high-impact Internet fraud targets neutralized	11	11	13	12	11	23	17	17	25	17	N/A
Performance Measure	Convictions/Pre-Trial Diversions: • Organized Criminal Enterprises • Gang/Criminal Enterprises • Crimes Against Children • Civil Rights	 693 2,218 207 207	 595 2,242 246 208	 395 2,136 270 222	 424 2,163 245 248	 812 N/A 338 268	 845 6,467 373 227	 833 N/A 1,312 238	 796 N/A 350 N/A	 723 7,338 1,570 205	 747 N/A N/A 350	 747 N/A N/A 350
Efficiency Measure	% of FBI OCDETF Investigations with links to CPOT-linked DTOs	14%	15.47%	14%	15.89%	16.35%	19%	20%	15%	20%	15%	N/A
Performance Measure	CPOT-Linked DTOs • Disruptions • Dismantlements	 45 15	 50 18	 35 20	 40 12	 54 22	 64 30	 139 40	 40 20	 150 31	 40 20	 N/A N/A
Performance Measure	Number of Organized Criminal Enterprise Dismantlements	43	38	43	39	39	47	70	38	82	38	38
Performance Measure	Number of Gang/Criminal Enterprise Dismantlements	144	114	135	124	165	163	251	99	167	99	99
Performance Measure	Number of Agents serving on Violent Crime Task Forces [Priority Goal indicator]	N/A	N/A	N/A	N/A	1,050	1,071	1,131	N/A	1,121	N/A	N/A
Performance Measure	Average length of sentence in months: Violent Crime [Priority Goal indicator]	N/A	N/A	N/A	N/A	72	74	N/A	N/A		N/A	N/A
Performance Measure	Cases Concerning Sexual Exploitation of Children	N/A	N/A	N/A	N/A	N/A	N/A	2,962	3,051	2,970	3,051	3,051
Performance Measure	Cases Concerning Human Trafficking	N/A	N/A	N/A	N/A	N/A	N/A	214	214	287	216	216

3. Performance, Resources, and Strategies

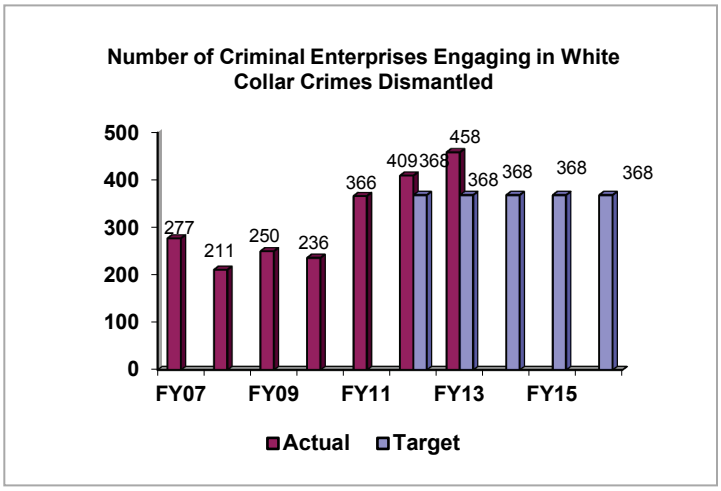
White Collar Crime

a. Performance Plan and Report for Outcomes

The White Collar Crime (WCC) program uses a suite of performance measures that concentrate on priority programs such as Corporate Fraud, Health Care Fraud, 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 Organizations Engaging in White Collar Crimes Dismantled.

FY 2014 Target: 368
FY 2014 Actual: 464
FY 2016 Target: 368

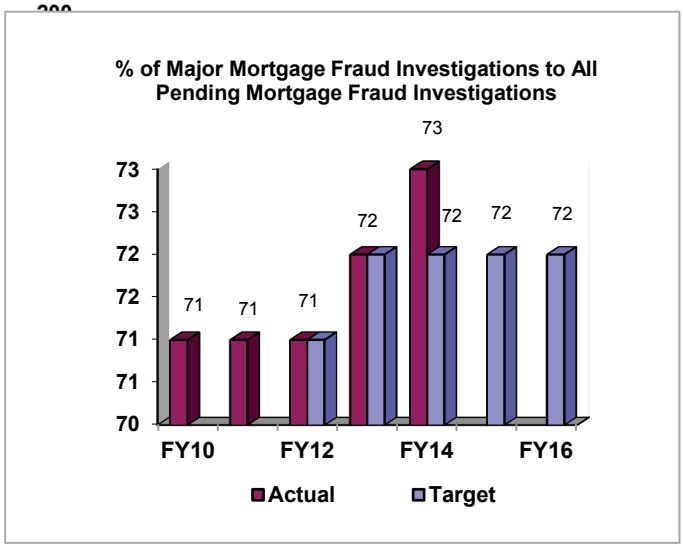


Discussion: The FBI established the FY 2016 target based on past performance and the increased activity of WCC enterprises, particularly in Health Care Fraud and Mortgage Fraud. Securities, corporate and mortgage fraud investigations are frequently long-term and resource-intensive. The impacts of resources received in one year are often not realized until several years later. Further, accomplishments in WCC can reach peaks at times when long-term cases initiated in prior years come to conclusion.

Number of Criminal Enterprises Engaging in White Collar Crimes Dismantled
500
400
300
277
211
250
236
366
409
368
458
368
368
368
368

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

FY 2014 Target: 72%
FY 2014 Actual: 73%
FY 2016 Target: 72%



Discussion: The nature of the mortgage fraud threat and recent trends indicate that high loss schemes, schemes involving industry insiders and the sophisticated criminal enterprises will persist into FY 2016. The FBI's long-term objective is to lower the incidence of mortgage fraud through detection, deterrence, and investigation so that the FBI can concentrate on neutralizing current and

emerging financial threats, as well as financial industry fraud schemes that target our Nation's financial institutions.

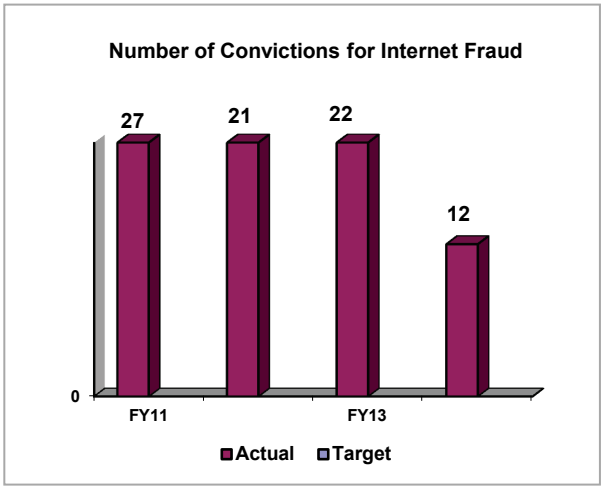
b. Strategies to Accomplish Outcomes
In FY 2016, the FBI will continue to pursue corporate fraud, securities fraud, mortgage fraud, other types of financial institution fraud, health care fraud, money laundering, and insurance fraud, which all threaten to undermine our Nation's financial infrastructure. The FBI will aggressively leverage 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.

Internet Fraud

a. Performance Plan and Report for Outcomes
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 nationwide takedowns (i.e., arrests, seizures, search warrants, indictments) to target the most significant perpetrators of on-line schemes and draw attention to identified crime problems.

Performance Measure: Number of convictions for Internet fraud

FY 2016 Target: In accordance with DOJ guidance, targeted levels of performance are not projected for this indicator.



b. Strategies to Accomplish Outcomes
The FBI will continue to aggressively pursue criminals that pose a threat to the national information infrastructure and, in the course of such endeavors, commit fraud. In cases that the Internet is but an instrumentality of a traditional fraud scheme, the FBI's Cyber Program will continue to pursue the most egregious, high-impact, and sophisticated non-intrusion schemes with an international nexus.

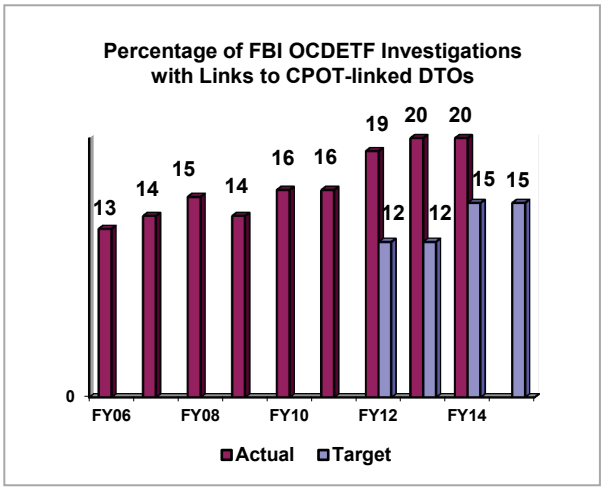
Number of Convictions for Internet Fraud
27
21
22
12
0
FY11
FY13
Actual
Target

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

a. Performance Plan and Report for Outcomes

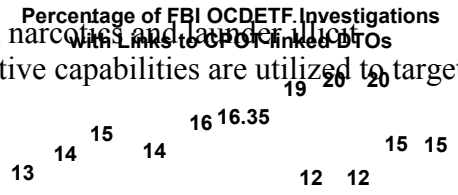
DOJ maintains a single national list of major drug trafficking and money laundering organizations. This list of targets, known as the CPOT list, reflects the most significant international narcotic supply and related money laundering organizations, poly-drug traffickers, clandestine drug manufacturers and producers, and major drug transporters supplying the U.S.

Performance Measure: Percentage of FBI OCDETF Investigations with Links to CPOT-linked Drug Trafficking Organizations (DTOs)

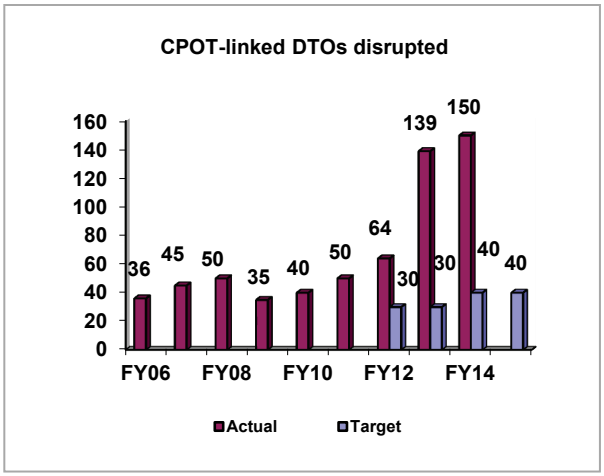


FY 2014 Target: 15%
FY 2014 Actual: 20%
FY 2016 Target: *The FBI proposes to discontinue this measure in FY 2016. This performance measure is being discontinued in FY 2016 due to the inability to accurately track these investigations.*

Discussion: CPOT-linked DTOs are identified through involved complex and coordinated intelligence, as well as analyzing drug investigative data and related financial data. Resources are focused on CPOT-linked organizations that traffic in narcotics and launder illicit proceeds. Resources, expertise and unique investigative capabilities are utilized to target their infrastructure.



Performance Measure: CPOT-linked DTOs Disrupted



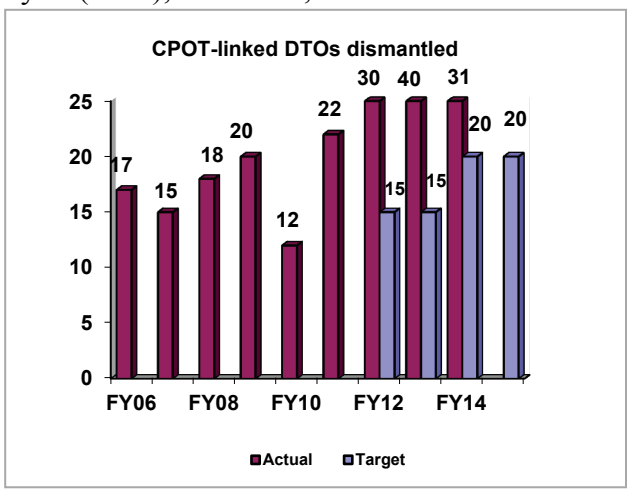
FY 2014 Target: 40
FY 2014 Actual: 150
FY 2016 Target: *The FBI proposes to discontinue this measure in FY 2016 due to the inability to track CPOT-linked investigative activity*

Discussion: CPOT-linked DTOs are disrupted through complex and coordinated intelligence-driven investigations as well as analysis of drug investigative data and related financial data. These efforts effectively alter the operations of major trafficking organizations. The FBI met and exceeded its target for this measure in FY 2014. It is anticipated that the FBI will continue to achieve greater efficiency linking cases to CPOTs which were not previously identified or documents, allowing higher documented production.

Performance Measure: CPOT-linked DTOs Dismantled

FY 2014 Target: 20
FY 2014 Actual: 31
FY 2016 Target: *The FBI proposes to discontinue this measure in FY 2016 due to the inability to track CPOT-linked investigative activity*

Discussion: To fully engage the field in support of the FBI's initiative to increase CPOT linkages, the Latin American Southwest Border Threat Section/OCDETF unit provided communications outreach and instruction to the field by utilizing the Regional OCDETF Coordinators (ROC's), OCDETF Program Analysts (PA's), as well as, the substantive units at Headquarters. In addition the OCDETF Unit continued to provide education as well as provided more funding to CPOT linked cases thereby increasing CPOT links and subsequent disruptions and dismantlements. The FBI met and exceeded its target for this measure in FY 2014. It is anticipated that the FBI will continue to achieve greater efficiency linking cases to CPOTs which were not previously identified or documented, allowing higher documented production.



CPOT-linked DTOs dismantled
25
20
15
10
5
0
17
15
18
20
12
22
30
15
40
15
31
20
20
FY06
FY08
FY10
FY12
FY14
Actual
Target

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, loan sharking, 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 Russian/Eastern European/Eurasian Criminal Enterprises (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 FBI's strategy for criminal organization investigations emphasizes the development and focusing of resources on national targets, the use of the Enterprise Theory of Investigations (which focuses investigations on the overall organization in question), 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 first established a National Gang Strategy in the 1990s to identify the gangs posing the greatest danger to American communities; combine and coordinate the efforts

of the local, state, and federal law enforcement in Violent Gang Safe Streets Task Forces throughout the U.S.; and utilize the same techniques previously used against organized criminal enterprises. The increasingly violent activity of MS-13 has prompted an FBI initiative that will assure extensive coordination between all Field Offices involved in the investigation of MS-13 matters. Additionally, due to a significant number of MS-13 gang members residing in Central America and Mexico, liaising with international law enforcement partners abroad will be a key part of the FBI's strategy against this gang threat. In FY 2006, DOJ and DHS established the National Gang Tracking Enforcement Coordination Center (GangTECC), now known as Special Operations Division/Operational Section: Gangs (SOD/OSG), a multi-agency initiative anti-gang enforcement, deconfliction, coordination and targeting center headed by a Director from the Drug Enforcement Administration (DEA) and a Deputy Director from the FBI, and staffed with representatives from Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), Bureau of Prisons (BOP), DEA, FBI, Immigration and Customs Enforcement (ICE) and the U.S. Marshals Service (USMS).

DOJ defines gangs as associations of three or more individuals whose members collectively identify themselves by adopting a group identity which they use to create an atmosphere of fear or intimidation frequently by employing one or more of the following: a common name, slogan, identifying sign, symbol, tattoo or other physical marking, style or color of clothing, hairstyle, hand sign or graffiti.[5] The association's purpose, in part, is to engage in criminal activity and the association uses violence or intimidation to further its criminal objectives. Its members engage in criminal activity or acts of juvenile delinquency that, if committed by an adult, would be crimes with the intent to enhance or preserve the association's power, reputation, or economic resources. The association may also possess some of the following characteristics: (a) the members employ rules for joining and operating within the association; (b) the members meet on a recurring basis; (c) the association provides physical protection of its members from other criminals and gangs; (d) the association seeks to exercise control over a particular location or region, or it may simply defend its perceived interests against rivals; or (e) the association has an identifiable structure. This definition is not intended to include traditional organized crime groups such as La Cosa Nostra, groups that fall within the Department's definition of "international organized crime," drug trafficking organizations or terrorist organizations.

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

Organized Criminal Enterprises & Gangs/Criminal Enterprises

a. Performance Plan and Report for Outcomes

Organized Criminal Enterprises

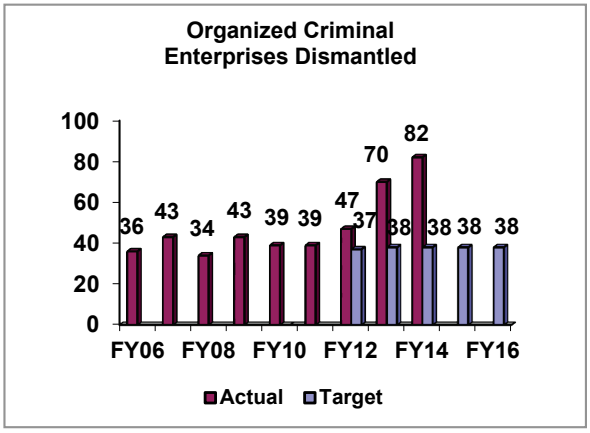
FBI investigations of criminal enterprises involved in sustained racketeering activities that are focused on those enterprises with ethnic ties to Asia, Africa, the Middle East, and Europe.

[5] http://www.justice.gov/criminal/ocgs/gangs/

Organized criminal enterprise investigations, through the use of the Racketeering Influenced Corrupt Organization statute, target the entire entity responsible for the crime problem. Each of these groups is engaged in a myriad of criminal activities.

Performance Measure: Organized Criminal Enterprises Dismantled

FY 2014 Target: 38
FY 2014 Actual: 82
FY 2016 Target: 38



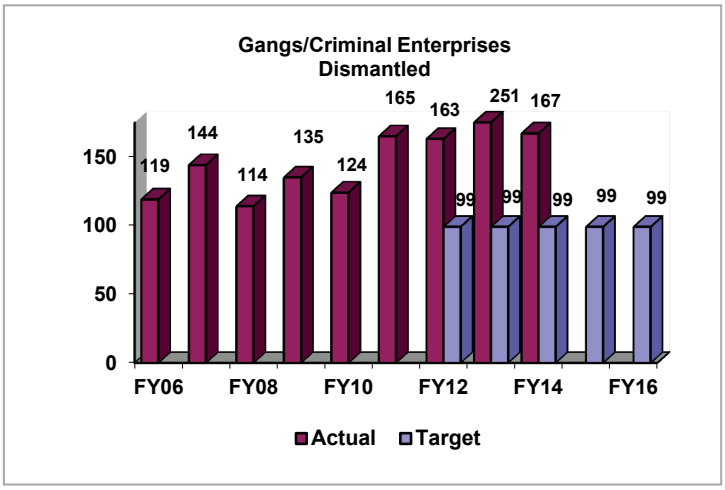
Discussion: Based on National Intelligence Estimates (NIEs) and other factors that gauge threats posed to U.S. national security by organize crime, the FBI targets high-priority organizations related to such threats.

The Organized Crime Program (OCP) anticipates additional collection, the establishment of additional cases, the development of additional confidential human sources, and an increase in IIR production. FBI efforts also include the initial targeting and operational activities against criminal bosses that support the associated thieves and members of high priority organizations, and target the financial and communications avenues of the criminal enterprises already identified as potential vulnerabilities.

<u>Gang/Criminal Enterprises</u>

The mission of the FBI's Gang/Criminal Enterprise Program is to disrupt and dismantle the domestic cells (local, regional, national, and transnational) of criminal enterprises, which pose the greatest threat to the economic and national security of the U.S. Many of these criminal enterprises have ties to North, Central, and South America. This will be accomplished through the FBI's criminal investigations, involvement in the Organized Crime Drug Enforcement Task Force Program (OCDETF), and support and leadership of HIDTA initiatives. The majority of the FBI's anti-gang efforts are directed towards the gangs that the Bureau has identified as presenting priority threats. The FBI works closely with local, state, federal, and international law enforcement agencies to accomplish this mission.

The Gang Targeting and Coordination Center (GangTECC) focuses on enhancing gang investigations of all federal agencies by acting as a deconfliction and case coordination center. GangTECC facilitates operations across agency lines and seeks to dismantle national and trans-national violent gangs.



Performance Measure: Gang/ Criminal Enterprises Dismantled

Note: This measure does not include CPOT-linked dismantlements.

FY 2014 Target: 99
FY 2014 Actual: 167
FY 2016 Target: 99

Discussion: DTOs are dismantled through complex and coordinated intelligence driven investigations that include analysis of drug investigative data and related financial data. These efforts effectively disrupt the operations of major trafficking organizations and ultimately destroy them. Resources are focused on coordinated, nationwide investigations targeting the entire infrastructure of major DTOs. DTO members who traffic in narcotics and launder illicit proceeds are targeted. Strategic initiatives are developed to effectively exploit the DTO's most vulnerable points, thus attacking its infrastructure. The FBI met and exceeded its target for this measure in FY 2014 through sustained, pro-active, coordinated investigations utilizing sophisticated techniques and technological advances. Combining short-term, street-level enforcement activity with investigative techniques such as consensual monitoring, financial analysis and Title III wire intercepts, the FBI made significant achievements against the gang and criminal enterprise threat in FY 2014.

D. Criminal Justice Services Decision Unit

CRIMINAL JUSTICE SRVICES DECISION UNIT TOTAL	Perm. Pos.	FTE	Amount ($000)
2014 Enacted	2,091	1,878	$506,863
2015 Enacted	2,091	1,983	468,435
Adjustment to Base and Technical Adjustments	3	3	1,859
2016 Current Services	2,094	1,986	470,294
2016 Program Increases	…	…	582
2016 Program Decreases	…	…	(2,982)
2016 Request	2,094	1,986	467,895
Total Change 2015-2016	**3**	**3**	**(540)**

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, as well as 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, and the administrative divisions and offices) are calculated and allocated to this decision unit.

CJIS Division

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

Next Generation Identification (NGI): NGI 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, fingerprint image comparisons, and/or other descriptors and provides criminal history records on individuals for law enforcement and civil purposes, such as requests from the Office of Personnel Management or the Department of State. NGI is designed to process criminal fingerprint submissions in 2 hours or less and civil submissions in 24 hours or less. In FY 2013, approximately 62.5 million fingerprint background checks were processed. In FY 2014, approximately 70 million fingerprint background checks were processed.

The NGI serves as the cornerstone to enable the FBI to meet its criminal justice service mission and support the intelligence community. Through incremental replacement of IAFIS, the FBI has dramatically improved system flexibility, storage capacity, accuracy and timeliness of responses, and interoperability with other systems - including the DHS and the Department of Defense biometric matching systems. The NGI is comprised of six overlapping increments. Increment 1 (Advanced Fingerprint Identification Technology [AFIT]) was achieved more than one month ahead of schedule in February 2011. Increment 2 (Repository for Individuals of Special Concern [RISC]) was deployed on schedule in August 2011. Increment 3 (Latent, Palms, Rapid DHS Response, and Full Infrastructure) was deployed on schedule on May 5, 2013. NGI achieved full operating capability with the deployment of Increment 4 in September 2014. Increment 5 remains an iris pilot, and Increment 6 is technology refreshment occurring between 2014 and 2017.

National Crime Information Center (NCIC): The NCIC is a database of criminal justice information as reported to the FBI by law enforcement and criminal justice agencies throughout the United States and internationally. The NCIC became operational on January 27, 1967, with the goal of assisting law enforcement in apprehending fugitives and locating stolen property. This goal has since expanded to include locating missing persons and further protecting law enforcement personnel and the public.

NCIC is a valuable tool that aids law enforcement officers, investigators, judges, prosecutors, correction officers, court administrators, and other law enforcement and criminal justice agency officials in the execution of their day-to-day operations. The NCIC contains over 12.8 million active records and processes an average of 11.2 million transactions a day compared to 10.9 million transactions a day in the year before. The system is available 24 hours a day, 365 days a year, and has had an average up-time of 99.77% in the last 12 months. On July 18, 2014, NCIC processed a record 14.6 million transactions with an average response time of less than 1 second.

The last major upgrade to NCIC occurred in July 1999, when the FBI and its shared-management partners envisioned a new era for the NCIC System - NCIC 2000. NCIC 2000 began operation on July 11, 1999, and enhanced the base capabilities of the legacy NCIC System as well as added important new files. These innovations enabled law enforcement to improve the safety of the communities they serve in the 21st century.

The FBI CJIS Division has implemented many enhancements to the system since 1999, in an effort to continue to meet the needs of the stakeholders. As the lifecycle of NCIC 2000 nears its end, the FBI CJIS Division is preparing for the next major upgrade to the NCIC known as NCIC 3rd Generation (N3G).

The mission of N3G is to partner with stakeholders to identify new functionality and information sharing services that will improve, modernize and expand the existing NCIC system so that it will continue to provide real time, accurate, and complete criminal justice information to support the NCIC user community.

In FY 2015, the FBI CJIS Division began conducting a N3G Requirements canvass. The purpose of the canvass is to gather and evaluate the needs of law enforcement and criminal justice communities. Subsequently, the needs of the users will be documented in concepts and scenarios that will ultimately become Concept of Operations (CONOPS) for the development of the N3G. It is vital that the new capabilities and functionality are detailed in a robust CONOPS to ensure that the system is developed to meet the current and future needs of the users. Starting in FY 2015 and continuing in FY 2016, scenarios and concept documents will be vetted and approved through the CJIS Advisory Process. In the interim while N3G development is being planned, CJIS is performing a Technical Refresh on the existing NCIC system in FY 2015. This will support three initiatives, which are DOJ Mainframe Consolidation Effort, NCIC name search COTS product upgrade (SSAName3), and the anticipated NCIC transaction growth.

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 2012, a $67 million New NICS development project began. The New NICS will refresh the current software

and hardware architecture, thereby providing continuous availability of the NICS (24/7/365) to support the NICS Section and its partners while also enabling more rapid deliveries of future improvements and/or newly legislated changes. The New NICS will utilize advances in technology, including Computer Telephony Integration, to dramatically improve user interfaces, empowering all stakeholders to more directly access information and services. In addition, the New NICS will expand business efficiencies by providing a comprehensive performance reporting capability in which real-time data can be collected and customized to more effectively and efficiently manage the workload of the NICS Section, including unanticipated spikes in system demand/transaction volumes. In FY 2013, the NICS processed almost 22 million inquiries. The FBI conducted approximately 10 million of these checks, resulting in 92,111 denials to prohibited persons. The remaining 12 million checks were conducted by individual states. In FY 2014, the NICS processed 20.8 million inquiries. The FBI conducted approximately 8.1 million of these checks, resulting in 87,160 denials to prohibited persons.

The remaining 12.7 million checks were conducted by individual states. The increased workload experienced in FY 2013 resulted from the tragic shooting at Sandy Hook Elementary School on December 14, 2012, and subsequent discussions of potential changes in gun laws. Prior to the Sandy Hook shooting, the busiest week in NICS history was the week of December 3 – 9, 2012, when 527,095 firearms checks were initiated. The week after the Sandy Hook shooting, December 17 – 23, 2012, NICS approached 1 million transactions (953,613). In FY 2013 the number of background checks increased dramatically largely as a result of the unintended consequence of the national gun safety debate. More purchases of firearms culminated in an uptick in the number of background checks processed. In FY 2014, the NICS continued to experience record high transaction volumes. On 11/28/2014, a total of 175,754 transactions were processed through the NICS in a single day. This was the second highest transaction volume day in history, only being surpassed on 12/21/2012, when the aftermath of the Sandy Hook shooting escalated the transaction volume to 177,170 background checks processed in a single day. Transaction volumes continue to increase in FY 2015. For example, during the week of December 15-21, 2014, a total of 595,201 firearm background checks were initiated, surpassing records set in FY 2012 by 13 percent. To enable the NICS Section to keep pace with the rising transaction volume, the NICS Section received $60 million and 324 positions for the NICS in FY 2014.

Uniform Crime Reporting (UCR): The FBI's UCR Program has served as the national clearinghouse for the collection of crimes reported to law enforcement since 1930. It is the CJIS Division of the FBI that collects, analyzes, reviews, and publishes the data collected from participating local, state, tribal, and federal law enforcement agencies. Information derived from the data collected within the UCR Program is the basis for the annual publications *Crime in the United States*, *Law Enforcement Officers Killed and Assaulted* (LEOKA), and *Hate Crime Statistics* that fulfill the FBI's obligations under Title 28 United States Code Section 534. The publications provide statistical compilations of crimes such as murder, forcible rape, robbery, aggravated assault, burglary, larceny-theft, motor vehicle theft, and arson; officers killed and assaulted in the line of duty; and hate crime statistics. Recognizing the need for improved statistics, law enforcement called for a thorough evaluative study to modernize the UCR Program, resulting in the National Incident-Based Reporting System (NIBRS). In the NIBRS, more detailed data are collected on each single crime occurrence made up of 49 specific offenses. In 2013, 6,328 agencies (approximately 38% of all UCR agencies) reported crime to the FBI UCR Program using the NIBRS Technical Specification. The UCR Program is actively working to increase NIBRS participation by partnering with the Bureau of Justice Statistics on the National Crime Statistics Exchange, working with advocacy groups to emphasize the importance of NIBRS data for the public and the law enforcement community, and conducting a study on transitioning the UCR Program to a NIBRS only data collection.

Currently, the UCR Program is working to complete the New UCR to manage the acquisition, development, and integration of a new information systems solution. The New UCR will decrease the time it takes to analyze data and respond sooner with data quality questions and concerns; reduce the exchange of printed materials between submitting agencies and the FBI; and implement a flexible and scalable systems framework, including industry standard interfaces that better accommodate future changes. Also, in the interest of improving crime data collections, the UCR Program is partnering with the Bureau of Justice Statistics and the National Academy of Sciences in a multi-year study to determine the relevance of current crime classifications, examine the potential for new crime data indicators, and recommend improvements on data collection and dissemination methods.

The UCR Program also conducts officer safety awareness training for the Nation's law enforcement community based on the statistics and research collected in the UCR LEOKA Program. The LEOKA Program is currently embarking on a comprehensive study "Ambushes and Unprovoked Attacks: Assault on Our Nation's Law Enforcement Officers." This two-year study, which began in March 2013, will focus on felonious killings and assaults of law enforcement officers during ambush situations.

National Data Exchange (N-DEx): The National Data Exchange (N-DEx) is the only national investigative information-sharing system that provides local, state, tribal, and federal criminal justice agencies with a mechanism for searching, linking, analyzing, sharing, and collaborating on criminal justice information. By using N-DEx as a pointer system and for data discovery, users can uncover relationships between people, crime characteristics, property, and locations; generate integrated biographies of subjects; eliminate information gaps by linking information across jurisdictions; connect the dots between non-obvious and seemingly unrelated data; and obtain contact information for criminal justice professionals working similar cases. N-DEx also promotes collaboration among agencies by allowing its users to coordinate efforts in a secure online environment.

N-DEx connects many regional and local information-sharing systems and leverages their collective power to provide access to millions of records. N-DEx complements existing state and regional systems and is positioned to fill in gaps in the many areas of the country where no information sharing system or program currently exists. N-DEx contains over 232 million records from more than 5,000 criminal justice agencies. Additionally, N-DEx provides access to an additional 94 million records from the Department of Homeland Security, the NCIC and Interpol. System records contain information on more than 1.6 billion entities (persons, places, things, and events).

During FY 2014, N-DEx added more than 25 million system records, over 300 participating agencies, and provided access to an additional 60 million leveraged records. It is projected that by the end of FY 2015, the number of criminal justice agencies sharing information via N-DEx will increase 5 percent. In addition, N-DEx expects to establish a connection with the Regional Information Sharing System (RISS) to make critical information contained within N-DEx available to more than 9,000 law enforcement agencies.

Law Enforcement On-line (LEO): LEO is a 24-hour-a-day, 7-day-a-week, on-line (real time), information-sharing system that is accredited and approved by the FBI for the transmission of sensitive but unclassified information throughout the world to the local, state, tribal, federal, and international law enforcement, criminal justice, and public safety communities. The LEO system provides a vehicle for these communities to exchange information and allows multiple agencies to share law enforcement information if they have a common interest in the same information or to store sensitive information

they may not need to share with other agencies such as building blueprints, evacuation plans, internal agency documents/forms, case information etc, also called Special Interest Groups (SIGs) or Virtual Offices (VOs). LEO provides law enforcement and criminal justice communities a secure "anytime and anywhere" national and international method to support antiterrorism, intelligence, investigative operations and provides an avenue to remotely access other law enforcement and intelligence systems and resources. LEO also offers an incident management system, the Virtual Command Center (VCC), an important component of LEO, which allows all levels of law enforcement to securely share critically needed information in real time across any Internet connection in order to provide safety and security at all major events and natural disaster areas. At the end of FY 2014, LEO supported a user base of over 70,000 active members, increased VCC new event boards created by over 1,300, and completed the addition of a new tactical tool to the VCC called Trax. This tool will complement the VCC and is designed to provide law enforcement partners with a user-friendly method for tracking multiple arrests and/or search warrant services, as encountered in "roundup" operations across the country.

The LEO system completed the merger of the CJIS Division's Enterprise Identity Management Services and the LEO re-hosted system of services, now called the Law Enforcement Enterprise Portal (LEEP), formerly known as LEO Enterprise Portal. LEEP supports and strengthens collaboration among the law enforcement, criminal justice, and public safety communities by offering a cost-effective, single sign-on capability. LEEP offers all LEO services, including VCCs, SIGs, and secure email. LEEP was created to serve as the overarching single sign-on solution from an agency's computer (or Identity Provider) to a larger suite of law enforcement hosted services. Once a user logs on to a trusted identity provider's network to access the LEEP, the user has potential access to over 20 different services such as the Regional Information Sharing System Network, National Law Enforcement Data Exchange, Joint Automated Booking System, National Gang Intelligence Center, Internet Crime Complaint Center, Intelink, MyFX, and eGuardian.

In FY 2015, work will continue on an industry portal solution which will allow an industry partner to access the services that directly support the Director's Cyber and Intelligence Initiatives that are focused on securing the nation's critical infrastructure.

Laboratory Division

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

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

The FBI Laboratory, established in 1932, is the only full-service civilian federal forensic laboratory in the U.S. The FBI Laboratory was accredited in August 2008 by the American Society of Crime Laboratory Directors – Laboratory Accreditation Board (ASCLD-LAB) for meeting or exceeding the requirements for *international* accreditation (ISO/IEC 17025). Examinations support investigations that cross all FBI investigative programs, international, federal, state, and local boundaries. Examinations of evidence for duly constituted U.S. law enforcement agencies, whether federal, state or local, and foreign law enforcement unable to perform the examinations at their own facilities are performed, free of charge. The FBI Laboratory also 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 Device Analytical Center (TEDAC), a multi-agency center that forensically and technically exploits terrorist improvised explosive devices and related materials and generates actionable investigative and intelligence information for use by the U.S. law enforcement, the Intelligence Community, the U.S. military, and other partners. In January ILEEP, the industry version of LEEP, an information sharing platform designed to integrate information sharing tools, reports, training, and platforms ILEEP, the industry version of LEEP, an information sharing platform designed to integrate information sharing tools, reports, training, and platforms 2015, as required under Public Law 113-235 and in support of the National Counter Improvised Explosive Devices (IED) Policy, Acting Deputy Attorney General Sally Quillian Yates formally designated TEDAC to serve as the single strategic level IED exploitation center and repository. This designation fulfills the requirements outlined within the 2012 Countering Improvised Explosives Report to the President and subsequent Joint Program Office for Countering Improvised Explosive Devices (JPO C-IED) Implementation Plan as envisioned by interagency partners involved in counter-IED efforts. In FY 2014, the FBI conducted approximately 545,300 forensic examinations (this included FBI, and other Federal, state and local examinations). Estimates for FY 2015 are approximately 540,000 examinations.

Training Division

In addition to training FBI agents, the FBI provides instruction for state and locals at minimal cost, both at the FBI Academy and throughout the U. S. at state, regional, and local training facilities. The principal course for state and local law enforcement officers is the FBI National Academy, a 10-week multi-disciplinary program for officers who are considered to have potential for further advancement in their careers. In FY 2014, there were 652 state and local law enforcement officers that participated in the National Academy program at the FBI Academy in Quantico, Virginia. In FY 2015, the estimated state and local law enforcement officers that will participate in the National Academy program 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 2014 97,000 criminal justice personnel received training from FBI instructors at state, regional and local training facilities. In FY 2015, the estimated criminal justice personnel to be trained by the FBI is 97,000.

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, for which the FBI is partially reimbursed by the State Department. In FY 2014, the FBI provided training to 6,304 international police officers and executives representing 96 countries. In FY 2015, the estimated number of international police officers and executives to be trained by the FBI is 6,300.

Program Objectives

- Reduce criminal activity by providing timely and qualitative 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.

D. Criminal Justice Services Decision Unit

2. PERFORMANCE/RESOURCES TABLE

Decision Unit: Criminal Justice Services

DOJ Strategic Goal/Objective Goal 3: Ensure the Fair, and Efficient Administration of Justice: Promote and strengthen innovative strategies in the administration of state and local justice systems. (Objective 3. 6)

WORKLOAD/ RESOURCES	Target	Actual	Projected	Changes	Requested (Total)
	FY 2014	FY 2014	FY 2015	Current Services Adjustments & FY 2016 Program Changes	FY 2016 Request
IAFIS fingerprint background checks	66,677,703	55,073,851	45,082,849	3,047,031	48,129,880
NCIC transactions	3,826,396,000	4,038,044,556	4,496,864,000	449,686,400	4,946,550,400
Total number of federal, state, and local investigations aided by the Combined DNA Index System (CODIS)	†		†	†	†
Total number of forensic and offender matches identified at CODIS	†		†	†	†

Total Costs and FTE	FTE	$000	FTE	$000	FTE	$000	FTE	$000	FTE	$000
	1,976	489,721	1,878	506,863	1,983	464,510	3	(540)	1,986	467,895

TYPE/ STRATEGIC OBJECTIVE	PERFORMANCE	FY 2014	FY 2014	FY 2015 Current Rate	Current Services Adjustments & FY 2016 Program Changes	FY 2016 Request
Efficiency Measures	**IAFIS/NGI: [Revived measures]** % of IAFIS/NGI routine fingerprint checks: Criminal: • Completed w/in 2 hours Civil: • Completed w/in 24 hours	95.00% 99.00%	98% 99%	95.00% 99.00%	- -	95.00% 99.00%
Performance Measure	**RISC Searches Response Time: [New Measure for FY 2014]** Average NGI response time of RISC rapid searches	<10 seconds	4.2 seconds	<10 seconds		<10 seconds
Performance Measure	**IAFIS/NGI: [Discontinued measures]** • Average daily identification searches • Average daily latent searches • Response time for routine criminal submissions • Response time for routine civil submissions	187,706 686 1 hour 12 hours		- - - -	- - - -	- - - -
Performance Measure	**NCIC:** • System availability • Downtime in minutes	99.5% 1,440	99.8% 1,313	99.5% 2,268	- -	99.5% 2,268

2. PERFORMANCE/RESOURCES TABLE						
Performance Measure	**NICS:** % of NICS system availability	98. 0%	99%	98. 0%	-	98.0%
Performance Measure	**NICS:** % of NICS checks with an Immediate Determination	90. 0%	91%	90. 0%	-	90.0%
Performance Measure	Average turnaround time for Federal DNA Sample entry in the National DNA Index System (NDIS) of submissions fulfilling the processing and upload requirements	30 days	18 days	30 days	-	30 days
Performance Measure	Student-weeks of Instruction at the Hazardous Devices School (HDS)	1,764	1,848	2,200	-	2,200
Performance Measure	**N-DEx:** Percent of population covered by N-DEx via state and local law enforcement participation	59.80%	67.72%	70.84%	-	70.84%
Performance Measure	**[Discontinued measure]** Number of products and services deployed in support of customers	210		N/A	-	N/A
Performance Measure	**LEO:** Number of active members	57,300	70,000	57,300	-	57,300
Performance Measure	**LEO:** Number of VCC new events boards open	743	1,500	831	-	831
Performance Measure	**LEO: [New Measure for FY 2014]** Number of identity or service providers on-boarded to the Law Enforcement Enterprise Portal (LEEP)	14	15	10	-	10

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 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.
- N-DEx targets are estimated based upon limited historical data. Marketing results are dependent upon executive advocacy, state policy and technical readiness for participation.

Performance Report and Performance Plan Targets		FY 2010	FY 2011	FY 2012	FY 2013	FY 2014		FY 2015	FY 2016
		Actual	Actual	Actual	Actual	Target	Actual	Target	Target
Efficiency Measures	**IAFIS/NGI: [Revived measures]** % of IAFIS/NGI routine fingerprint checks: Criminal: • Completed w/in 2 hours • DHS checks completed w/in 72 hours Civil: • Completed w/in 24 hours • DOS checks completed w/in 15 minutes	 99. 32% 99. 51% 99. 70% 99. 11%	 99. 30% 100% 99. 80% 99. 90%	 99.30% 99.83%	 N/A N/A N/A	 95.00% N/A 99.00% N/A	 98% 99%	 95.00% N/A 99.00% N/A	 95.00% N/A 99.00% N/A
Performance Measure	**RISC Searches Response Time: [New Measure for FY 2014]** Average NGI response time of RISC rapid searches	N/A	N/A	N/A	N/A	<10 seconds	4.2 seconds	<10 seconds	< 10 seconds
Performance Measure	**IAFIS/NGI: [Discontinued measures]** • Average daily identification searches • Average daily latent searches • Response time for routine criminal submissions • Response time for routine civil submissions	 132,064 682 8m 42s55m24s	 139,125 597 10 min 1 hr 5 m	157,979 700 7 min 43s 1 hr 6m 31s	 170,114 783 6.12 min 1.07 hours	 200,232 753 30 min 30 min		 N/A N/A N/A N/A	 N/A N/A N/A N/A
Performance Measure	**NICS:** % of NICS checks with an Immediate Determination	91. 36%	91. 40%	91.72	91.64%	90.00%	91%	90.00%	90.0%
Performance Measure	**NICS:** % of NICS system availability	N/A	N/A	99.93%	99.81%	98%	99%	98.%	98%
Performance Measure	**NCIC:** • System availability • Downtime in minutes	99. 79% 1,152	99. 76% 1,273	99.75% 1,351	99.81% 1,000	99. 50% 1,440	99.8% 1,313	99. 50% 2,268	99.50% 2,268
Performance Measure	Average turnaround time for Federal DNA Sample entry in the National DNA Index System (NDIS) of submissions fulfilling the processing and upload requirements	N/A	N/A	25 days	18 days	30 days	18 days	30 days	30 days
Performance Measure	**N-DEx:** Percent of population covered by N-DEx via state and local law enforcement participation	27%	35. 30%	50.00%	54%	59.80%	67.72%	70.84%	70.84%
Performance Measure	**N-DEx: : [New Measure for FY 2015]** Annual percent increase of agencies submitting data to N-DEx	N/A	N/A	N/A	N/A	N/A		15%	15%
Performance Measure: *Customer Satisfaction*	**LEO: [Discontinued measure]** % of users who visit the Law Enforcement Online (LEO) service (which provides intelligence dissemination) more than one month out of each year.	45.00%	41.00%	N/A	N/A	N/A		N/A	N/A
Performance Measure	**LEO:** Number of Active Members	N/A	55,147	58,863	56,170	57,300	70,000	57,300	57,300

Performance Measure	**LEO:** Number of VCC new events boards open	N/A	N/A	N/A	2,167	743	1,500	831	831
Performance Measure	**LEO: [New Measure for FY 2014]** Number of identity or service providers on-boarded to the Law Enforcement Enterprise Portal (LEEP)	N/A	N/A	NA	N/A	14	15	10	10
Performance Measure	Student-weeks of Instruction at the Hazardous Devices School (HDS)	2,326	2,295	2,052	2,024	1,764	1,848	2,200	2,200

3. Performance, Resources, and Strategies

The Criminal Justice Services Decision Unit contributes to the Department of Justice's Strategic Goal 3, "Ensure the Fair and Efficient Administration of Justice." Within this goal, the resources specifically support Strategic Objective 3.6, "Promote and strengthen innovative strategies in the administration of state and local justice systems." This Decision Unit ties directly to the FBI's ninth priority: Support federal, state, local, and international partners; and to the "Maximize Partnerships" theme and its related objectives on the FBI's strategy map.

a. Performance Plan and Report for Outcomes

Integrated Automated Fingerprint Identification System/Next Generation Identification

Performance Measure: REVIVED MEASURE: Percentage of IAFIS/NGI routine criminal fingerprint checks completed within 2 hours.

FY 2014 Target: 95%
FY 2014 Actual: 99%
FY 2016 Target: *95%*

Discussion: The new measure replaces the discontinued measures that follow below and may be updated once NGI is fully deployed in 2014. 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, on July 28, 1999, the FBI launched the Integrated Automated Fingerprint Identification System (IAFIS), which is managed by the FBI's CJIS Division in Clarksburg, West Virginia. The IAFIS is a national fingerprint and criminal history system that 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.

Performance Measure: REVIVED MEASURE: Percentage of IAFIS/NGI routine civil fingerprint checks completed within 24 hours.

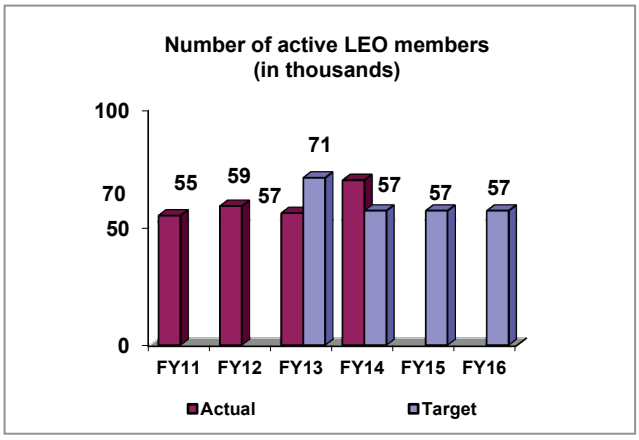
FY 2014 Target: 99%
FY 2014 Actual: 99%
FY 2016 Target: *99%*

Discussion: The FY 2016 target is based on historical data. All IAFIS segments will be replaced by NGI in 2014. Until that time, measure reporting will reflect the IAFIS system for routine criminal and civil response times. This reporting accounts for some improvements in response times which could be attributed to efficiencies gained by NGI's implementation of the new fingerprint matching segment of IAFIS. The NGI response times, and subsequent performance measures, for routine criminal and civil submissions will not be implemented until all IAFIS segments have been replaced at NGI Full Operating Capability.

Law Enforcement Online

Performance Measure: Number of active LEO members:

FY 2014 Target: 57,300
FY 2014 Actual: 70,000
FY 2016 Target: *57,300*



Discussion: This measure reports the number of total active members brought onto the LEO system from state, local, and federal law enforcement, and criminal justice entities. The target projections are based on historical system data with planned current system enhancements. With the implementation of the LEO Enterprise Portal (LEO-EP), LEO will have the ability to on-board entire law enforcement organizations as LEO users. In FY 2013, the FBI reviewed all LEO accounts and deleted those that had not been active for at least six months. The deletion of inactive accounts necessitated a significant downward revision to the target number of active LEO members in FY 2014 and FY 2015. LEO continues to increase awareness of LEO services through the FBI Field Office, and Tribal and Virtual Office initiatives. The FY 2014 target was based on rates increasing with LEO becoming a service on the LEO-EP and the addition of whole organizations/agencies.

National DNA Index System (NDIS)

Performance Measure: Average turnaround time for Federal DNA Sample entry in the National DNA Index System (NDIS) of submissions fulfilling the processing and upload requirements.

FY 2014 Target: 30 days
FY 2014 Actual: 18 days
FY 2016 Target: *30 days*

Discussion: The FBI Laboratory has established a 30-day turnaround time for processing and uploading samples based upon community expectations to receive, process, analyze, and upload samples. To reduce the turnaround time for the samples requiring re-analysis, the Federal DNA Database (FDD) Program is (1) implementing process improvements in how samples are re-analyzed/reworked to increase efficiency, and (2) specifically monitoring the turnaround time of samples that require re-analysis. For the FY 2014, the FDD program significantly exceeded their target of an average 30-day turnaround time for sample processing/upload by achieving 18 days.

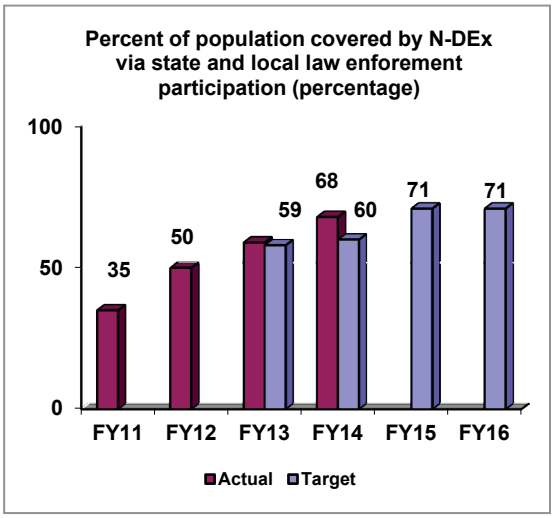
Law Enforcement National Data Exchange (N-DEx)

N-DEx provides criminal justice agencies the ability to share data and detect, deter, and disrupt criminal activity and national security threats. N-DEx is the result of collaboration among local, county, state, tribal, and federal criminal justice communities to establish a secure, national, criminal justice information sharing capability at the sensitive but unclassified level. The application of N-DEx capabilities provides the missing links and creates partnerships that lead to

more effective investigations that will help disrupt and apprehend individuals and organizations responsible for criminal activities and national security threats.

***Performance Measure**:* Percent of population covered by N-DEx via state and local law enforcement participation

FY 2014 Target: 60%
FY 2014 Actual: 68%
FY 2016 Target: 71%



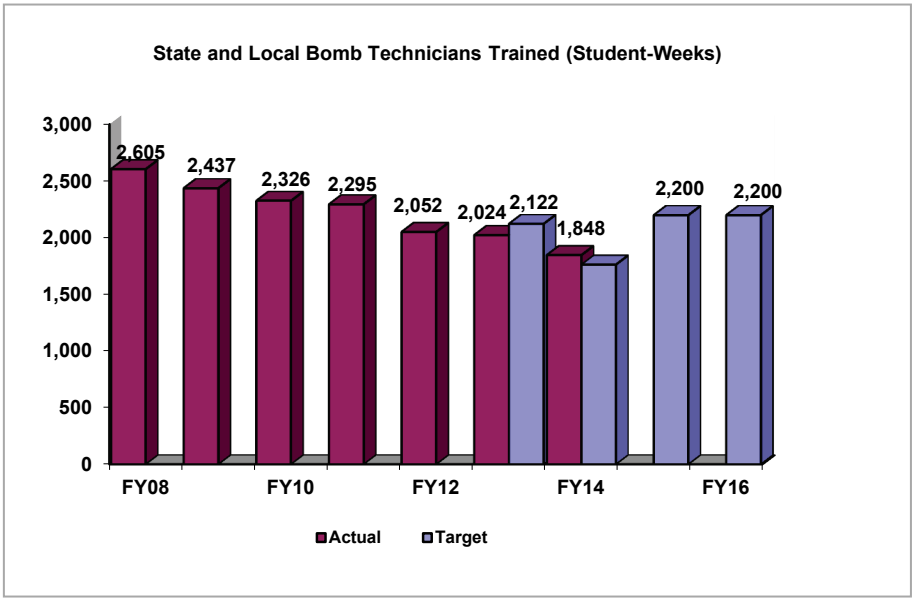
Discussion: This measure is intended to demonstrate the law enforcement agencies' desire to share its data on a national scale through participation with N-DEx. This data also indicates that N-DEx has been accepted by the law enforcement community as a major national criminal justice information sharing vehicle. Participation with N-DEx is voluntary for local, state, regional, tribal, and federal agencies. The data for this measure is defined as the portion of the U. S. population living in jurisdictions where the state or local law enforcement entities participate in N-DEx. While federal data from throughout the U. S. is contained in N-DEx, it is not included in calculating this percentage. The effectiveness of N-DEx is dependent upon widespread participation of organizations sharing their data. Annual targets are set based on historical information and planned agency participation. Marketing results are dependent upon executive advocacy, state policy, and technical readiness for participations. Continuing challenges include insufficient state and local resources, legal and policy constraints, and cultural challenges. N-DEx outreach and marketing efforts remain focused on the criminal justice community's adoption of N-DEx as the national information sharing tool.

Hazardous Devices School (HDS)

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

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

FY 2014 Target: 1,764
FY 2014 Actual: 1,848
FY 2016 Target: 2,200



Discussion: The HDS program is a reimbursable inter-service support agreement between the FBI and the U. S. Army.

The amount of projected training is based upon the amount of reimbursable funding received, which drives the frequency of training courses available, duration of training courses, and the number of courses that can be offered per fiscal year. As a result of additional resources provided in FY 2015, the FBI expects a slight increase in FY 2015 and 2016 performance.

b. Strategies to Accomplish Outcomes
The FBI's CJIS Division 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. Automation and computer technology inherently require constant upgrading and enhancement if such systems are to remain viable and flexible to accommodate changing customer requirements.

The FBI's HDS provides state-of-the-art technical intelligence to state, local, and federal first responders in courses regarding the criminal and terrorist use of improvised explosive devices (IEDs), and the tactics, techniques, and procedures to render these hazardous devices safe. Additionally, HDS provides training on emerging threats targeting the U. S. and its interests. This training includes countermeasures targeting suicide bombers, vehicle borne IEDs, stand-off weapons, WMD devices, and radio-controlled IEDs.

c. Priority Goals
The FBI contributes to Violent Crime Priority Goal 2, Protect Our Communities by Reducing Gun Violence. By September 30, 2015, the Department of Justice will increase the number of records submitted to the NICS by state and federal agencies by 10 percent, through the increase of additional non-Point of Contact State background checks.

V. Program Increases

Item Name: **Next Generation Cyber**

Strategic Goal(s) & Objective(s): 1.2, 1.4, 2.5
Budget Decision Unit(s): Counterterrorism/Counterintelligence, Criminal Enterprises and Federal Crimes

Organizational Program: Cyber, Operational Technology

Program Increase: Positions … Agt … FTE … Dollars $10,300,000 (all non-personnel)

Description of Item

The FBI requests $10,300,000 non-personnel in support of its Next Generation Cyber (NGC) initiative to enhance cyber collection and analysis and extend centralized capabilities to the field. The requested resources will foster a whole of government approach to cybersecurity, as well as address critical gaps in the FBI's current ability to investigate computer intrusions and identify, mitigate, and disrupt cyber threat actors.

The FBI's NGC initiative, launched in 2012, is aimed at enhancing the FBI's ability to address the full range of cybersecurity threats to the Nation. With an emphasis on preventing attacks before they occur, while protecting privacy, confidentiality, and civil liberties, the FBI has made significant efforts to prioritize and align existing resources to strengthen its cyber capabilities. However, given the increasing complexity and proliferation of the cyber crimes, additional resources are needed to address this threat.

Justification

Threat Summary

The U.S. faces daily computer network attacks from a range of nation-state, criminal and terrorist threats with potentially devastating consequences. Such attacks pose an urgent threat to the Nation's security and economy. Given enough time, motivation, and funding, a determined adversary will likely be able to penetrate any system accessible from the Internet. Intrusions into corporate networks, personal computers, and government systems occur daily by the thousands and range from simple vandalism and lucrative organized crime rings to terrorism and nation-state intelligence collection.

Financial crime increasingly occurs by cyber means in the online world, rather than through traditional criminal activity in the physical world. Criminals no longer need guns to rob a bank; they can use a computer to breach corporate and financial institution networks to steal credentials, account numbers, and personal information to commit a robbery. These criminal syndicates, often made up of individuals living in disparate places around the world, have already stolen billions of dollars from the financial services sector and its customers. Their crimes increase the cost of doing business, put companies at a competitive disadvantage, and create a significant drain on the U.S. economy.

While these diverse cyber-based threats are not new, the methods by which attacks occur are increasing in both volume and complexity. Today, illicit activities typically transpire over the

Internet and other computer networks. These networks hinder attribution and efforts to investigate the broad reaching consequences of the intrusion, as the identity of the attacker – be it criminal, terrorist or nation-state espionage – can remain unknown. Concurrently, just as the Internet has enabled businesses to maximize profits by inexpensively connecting with millions of customers, it has also enabled threat actors to amplify their impact by inexpensively attacking millions of victims.

These circumstances have created alarming risks to national security, global economic stability, and public welfare. Despite formidable investments and concerted efforts by the private sector and government to build more secure and defendable computer networks, these risks remain high. As technology continues to proliferate into every facet of modern life – from social media and smart phones to critical infrastructure, automobiles and implanted medical devices – cyber security continues to be a rapidly growing concern with no easy solutions in sight.

The FBI's mission focuses on contributing to a whole of government approach to cyber security. It does so by investigating intrusions to determine criminal, terrorist, and nation-state actor identities, and engaging in activities which reduce or neutralize these threats. Once an attack has been attributed to a threat actor, the FBI collects intelligence and disrupts the actor(s) using its unique combination of national security and law enforcement authorities. Working with victim companies as well as government, commercial and academic partners who own and maintain the principal data routes that make up the internet, the FBI collects intelligence and evidence to be shared with the Intelligence Community (IC), international partners and victims to neutralize the threat, whether the actor is in the U.S. or abroad. The FBI collects and disseminates information significant to those responsible for defending networks, including information regarding threat actor targets and techniques. The FBI's jurisdiction is not defined by network boundaries; rather it includes all territory governed by U.S. law, whether domestic or overseas, and spans individual citizens, private industry, critical infrastructure, U.S. Government, and other interests alike. Collectively, the efforts of the FBI, working in concert with its partners, help deter future threats and bring rapid closure to current threats which would otherwise continue to infiltrate and harm our network defenses.

Within this critical area of responsibility shared by law enforcement and intelligence community partners, the FBI has demonstrated many unprecedented successes, ranging from the take-down and arrest of the operators of "botnets" – armies of personal computers belonging to millions of unsuspecting, law-abiding citizens used to attack legitimate businesses for extortion – to attributing and arresting members of international hacking groups.

Recent successes include the FBI-led international takedown operations of the GameOver Zeus and Blackshades botnets in May and June 2014. Both botnets were prolific and led to the loss of hundreds of millions of dollars from U.S. victims. The takedowns included the shutting down of the respective botnets and the arrest of major Blackshades affiliates, including its creators and administrator. FBI also positively identified and obtained an arrest warrant for the elusive Zeus malware developer. These events represent the FBI's significant progress in international cooperation, intelligence collection and analysis since its last attempted international takedown of Zeus malware in 2010, which led to the seizure of several Zeus servers and the arrest of multiple Zeus cyber criminals, but left the developer unidentified and at large, leading to a

resurgence of the botnet. Since the 2014 takedown operations, neither botnets have been reconstituted.

The FBI has also demonstrated considerable success with the National Cyber Investigative Joint Task Force (NCIJTF) – an FBI-led multi-agency organization that has effectively leveraged collaboration to overcome information sharing challenges and successfully investigate computer intrusions while operating well within principles, authorities, and integral judicial oversight designed to protect the privacy and freedom of U.S. citizens. The NCIJTF has been instrumental in sharing information on multiple threat actors with several key partners in the private sector since 2013, facilitating victim engagement and intelligence collection. These engagements have been invaluable in the FBI effort to spread awareness of existing cyber threats to the U.S. private sector.

The FBI seeks enhancements in the following focus areas to further implement the NGC strategy. Each of these collectively builds off one another in support of this strategy and build on existing, proven areas of the FBI's program. The focus areas are:

- *Improve Cyber Collection and Analysis* to ensure the FBI and the NCIJTF is able to obtain and process essential surveillance, connect the dots, and enable actions as quickly as possible; and
- *Extend Centralized Capabilities to the Field* to gain efficiencies, improve the quality of and speed with which information is collected, and leverage talent and human capital from across the Nation.

The requested investments presented in detail below directly support the NGC strategy.

Improve Cyber Collection and Analysis – $5,000,000

As the FBI identifies indications of imminent or ongoing targeting of victim entities, consistent with Executive Order (EO) 13636, the FBI must reach out to these victims as quickly as possible to ensure that victim risks can be mitigated and losses minimized.[6] Early contact also affords the FBI with more opportunities to collect perishable evidence and plan operations that can yield significant investigative benefit.

To this end, in FY 2013 the FBI piloted the Cyber Guardian system based on an existing system developed to support counterterrorism cases. This system allows the FBI to catalog identified victims and track victim engagements, including contact information, contact history, and other pertinent details. As of January 2015, Cyber Guardian is tracking nearly 7,000 targeted victim entities. This enhancement includes $1.0 million to further develop Cyber Guardian, providing an interface with Sentinel, the FBI's case management system, to automate entry of victim data and more quickly and efficiently reach out to targeted victim entities.

The FBI's direct engagement with victims has become a staple of the FBI's investigative efforts and enables the bulk of the FBI's collection. Unlike traditional crimes, cyber crime victims can be unaware that they are targeted or their computers have been intruded upon until long after economic or national security losses have occurred. In most cases, the victims the FBI contacts have no knowledge of the crime. Identifying victims through its investigations and engaging them provides the source of much of the FBI's insight into threat actors and their identities and

[6] EO 13636 Improving Critical Infrastructure Cybersecurity, signed February 12, 2013.

opportunities for operational activities. In addition, victim engagement provides the FBI with useful insights to understand why a victim may have been targeted, what an adversary may be after, and how they may have operated. Equally important, victim engagement helps victims manage their risk by mitigating the consequences of any losses or even thwarting a compromise altogether.

When engaging victims, FBI field agents and analysts are often in direct contact with corporate executives, IT administrators and in-house incident response teams. In many cases, victims also hire outside security experts in response to the intrusion. The ability of the FBI to engage on both corporate executive concerns and highly technical details of the intrusion is critical to ensuring important evidence is preserved and collected, options for additional operations to learn more about the intruder are recognized (including establishing additional ESLUR collection). To be successful in this engagement and to carry out the investigation, FBI field agents and analysts must be technically competent, familiar with general IT and cybersecurity practices, IT hardware, software and network configurations, and the investigative tradecraft available to FBI.

While the FBI conducts its own in-house training on investigative tradecraft, holding industry-recognized certifications also facilitates FBI agents and analysts when engaging victims and when testifying in court. This request includes $1.5 million to expand training and certification under 37 different class curricula provided by the industry-recognized the SysAdmin, Audit, Networking, Security (SANS) Institute, adding approximately 225 additional seats per year of SANS Institute training.

FBI cyber agents are also cross-trained to conduct certain types of evidence extraction independent of FBI CART examiners. This cross-training improves the efficiency of the FBI's efforts, allowing CART examiners to focus on forensic analysis and allows the FBI to collect evidence concurrently with other victim engagements. This request includes $500,000 to increase the number of FBI Digital evidence Extraction Technician (DExT) training classes offered annually from 3 to 4.

This request also includes $500,000 to support the growth of the FBI Cyber Investigator Certification program developed under a partnership with the Software Engineering Institute (SEI) of Carnegie Mellon University. The certification provides customized training, knowledge assessments, and capstone cyber exercises to help state, local, tribal and territorial (SLTT) members develop, maintain, and advance their analytical skills. The program is designed around the cyber investigative process and is intended to constantly improve overall national analysis and response capabilities. It also establishes a standard certification and baseline training for all domestic law enforcement. The certification with be for SLTT, but the courses and curriculum will be dual purposed and available to FBI personnel. In FY 2015, the program expects to provide on-line training for more than 100,000 law enforcement first responders, with emphasis on the basic steps needed to preserve digital evidence at a crime scene until trained personnel arrive. Well trained SLTT law enforcement acts as a force multiplier as SLTT law enforcement provides deeper domestic coverage and increased proximity to victims.

Extend Centralized Capabilities to the Field – $5,300,000
The Operation Wide Area Network (OpWAN) provides a network where artifacts of computer intrusion investigations can be safely shared and collaboratively analyzed across the FBI enterprise. Unlike other investigations, computer intrusion investigations routinely work with evidence that includes malware – malicious software or code that can cause harm to computer networks and enable them to be compromised by adversaries. In normal situations, networks are protected from malware by using tools such as virus scanners and other cybersecurity measures. For computer intrusion investigations; however, the FBI must be able to actively handle evidence which contains malware, or even handle the malware itself in an effort to analyze it. Such practices can be exceptionally dangerous if conducted on systems not designed for these activities and normal cybersecurity measures, if in place, would interfere with the analysis. OpWAN provides such an environment that enables investigators and analysts to more easily conduct analysis, share technical evidence such as network packet capture and malware samples, and engage in technical collaboration across the FBI enterprise without subjecting traditional FBI business networks and systems to potentially dangerous malware.

Impact on Performance
As part of the NGC strategy, the FBI is developing new outcome-focused performance measures that capture the benefits of additional investments. These investments are intended to expand on capabilities that have demonstrated significant, noteworthy and cost-effective outcomes over the past several years. While the Nation's experts continue to improve the security of computerized technology, the FBI must act assertively to curtail the threats that are exploiting this technology.

The increasing need to collaborate across the FBI enterprise and safely share intrusion-related data requires the FBI to extend analytic capabilities to all FBI field offices. This enhancement will enable the capabilities demonstrated in the successful NCIJTF LIGHTHOUSE prototype to be extended to the field and shared with partners.

The cyber threat will continue to evolve and change as technology, and man's ability to exploit it, develops. The FBI's NGC strategy includes enhancing the FBI's investigative, collection, and analytic capacity to ensure the FBI can continue to provide irrefutable attribution of cyber attacks to threat actors, disrupt their efforts, and provide actionable intelligence to inform the FBI's operations, as well as those of the USIC and foreign partners. This improved capacity will ensure FBI remains nimble to effectively address emerging threats to the U.S. in the coming years.

Funding

Base Funding

FY 2014 Enacted				FY 2015 Enacted				FY 2016 Current Services			
Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)
1,485	816	1,409	$400,552	1,621	807	1,621	$417,872	1,754	894	1,754	$473,059

Non-Personnel Increase Summary

Initiative	Unit	Quantity	FY 2016 Request ($000)	FY 2017 Net Annualization (change from 2016) ($000)
Increase Field Investigations	n/a	n/a	$5,000	$…
Improve Cyber Collection and Analysis	n/a	n/a	5,300	$…
Total Non-Personnel			$10,300	$…

Total Request for this Item

	Pos	Agt	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2017 Net Annualization (change from 2016) ($000)
Current Services	1,754	894	1,754	$275,945	$197,114	$473,059	$...
Increases	…	…	…	…	10,300	10,300	…
Grand Total	1,754	894	1,754	$275,945	$207,414	$483,359	$...

Item Name: **IT Infrastructure**

Strategic Goal(s) & Objective(s): 1, 2, 3
Budget Decision Unit(s): All

Organizational Program: Information Technology

Program Change: Positions … Agt … FTE … Dollars $9,700,000 (all non-personnel)

Description of Item

The FBI requests $9,700,000 for its information technology (IT) infrastructure to increase the FBI's collaboration with the Intelligence Community (IC) by leveraging the IC Information Technology Enterprise (IC ITE) components and services.

Justification

IC ITE - $9,700,000 (all non-personnel)
The IC ITE effort is a multi-year, multi-faceted IT strategy that directly supports and leverages the Office of the Director of National Intelligence's (ODNI) strategic initiative to deliver world-class global technological solutions and services. The IC ITE strategy encompasses the policies, procedures, and strategies that support agile and efficient mission capabilities and drive responsible and secure information sharing. IC ITE lays the groundwork that will enhance the FBI's ability to share information through improved infrastructure, capabilities, business operations, governance, oversight, and strategic partnerships. The key IC ITE services will include: Applications Mall (AML), Desktop Environment (DTE), Enterprise Management Services (EMT), IC Cloud, Identity Authentication Authorization/Identity and Access Management (IAA/IdAM), Information Transport Service (ITS), Network Requirements and Engineering Service (NRES), and IC Security Coordination Center (SCC).

The IC ITE initiative will address infrastructure upgrades for existing Joint Worldwide Intelligence Communications (JWICs) nodes for increased aptitude, adapted desktop environments, migration services for the FBI's address book feature known as Active Directory (AD), data and access control systems migration, developing access rules and beginning data registry implementation. This will include supporting the provisioning of attributes and data tagging in support of access rules aligned for IC ITE requirements. These activities will require infrastructure investments and contract support services to conduct system upgrades and support services.

The FBI's 2016 IC ITE request includes:

Government Cloud (GC) Magnum support service for Cyber and Counterterrorism threats ($1.2 million)
The requested $1.2 million will provide IT services and hardware to perform system upgrades and provide contractor support to develop software in compliance with appropriate classification markings and data tagging for specific Cyber and Counterterrorism cases.

Network Demilitarized Zone (DMZ) and Circuit Enhancement ($1.3 million)
The FBI will access all IC ITE services through the DMZ, which will ensure that external network connectivity between the FBI and IC ITE service providers is dependable. This request includes the purchase of network equipment (such as load balancers, firewalls and enterprise grade routers) to support the new IC Desktop Environment (DTE) traffic load.

Digital Policy/Entity Attributes/Data Tagging ($1.4 million)
The request includes contractor support to develop access rules and guidance pertaining to the implementation of digital policies. These resources will also provision attributes and data tags associated with access rules, in support of required Smartdata tagging for data sharing in IC ITE. The resources will also support data access implementation in Secret and Unclassified enclaves, when applicable.

IC Desktop Environment (IC DTE) Adoption ($1 million)
The IC DTE service is the IC's user-facing common operating environment designed to enhance the IC's ability to improve collaborate with the IC and enhance mission performance by leveraging the DTE technologies to make services available at any IC location. IC DTE will enable IC users to use a single log-on to access e-mail, information sharing databases, desktop video teleconference capabilities, and select mission applications. The FY 2016 request will allow the deployment of IC DTE to 200 FBI users.

The requested funding will include integration and migration to support the initial expansion of the DTE pilot-based environment. Support will be required to maintain the legacy infrastructure environment while initiating the deployment of users to DTE. Network simulation and a laboratory setup will be required to measure performance and assess the impact of IC DTE on the FBI's network infrastructure

IC Identity and Access Management (IdAM) ($4.8 million)
The FBI requests $4.8 million to provide IdAM (formerly IAA) capability for the FBI's Top Secret network. Use of IC ITE IdAM Services will enable the FBI to leverage IC capabilities based on FBI mission needs. The funding will address multiple functions (i.e. hardware, software and services) related to migration, including adaptation of existing Top Secret IdAM capabilities, changes need to match IC interface specifications, adjustment of current cross-domain systems, migration services for Active Directory (AD), and access control systems migration. These activities will require contractor support services to perform system upgrades. The FY 2016 request will allow the deployment of IdAM to 200 FBI users.

IC ITE will enable the FBI to leverage existing IC capabilities and services while avoiding the cost of rebuilding the entire capability for the FBI alone. The service adoption will also provide efficiency in network Operations & Maintenance (O&M) support, and increase security.

Collaboration with other IC members is critical. The materials involved are typically subject to time constraints and content sensitivity of the information. The need for joint investigation and analysis in support of shared missions will require shared IT services. IC ITE will enable greater IC integration, information sharing, big data exploitation, safeguarding, and re-use of data and applications through a common IC architecture.

Lastly, IC ITE directly supports the President's National Strategy for Information Sharing and Safeguarding. Successful integration requires a global IT infrastructure through which the IC can rapidly and reliably share intelligence with those who need it.

Impact on Performance

Without these investments, the FBI will not be able to leverage the IC capabilities and services, and will be required to make significant capital investments in the current out-dated, aging network infrastructure and equipment. Data sharing and safeguarding will be limited. Connectivity to the IC will be sub-optimal due to the FBI's current infrastructure and network architecture not being designed to efficiently leverage the IC DTE solution and architecture.

IC ITE service interoperability and network performance will be a significant challenge for the FBI. Users' ability to access IC services supporting the FBI mission and collaboration/intelligence integration with other IC partners will be extremely limited.

Funding

Base Funding*

FY 2014 Enacted				FY 2015 Enacted				FY 2016 Current Services			
Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)
2	...	2	$804	3	...	3	$1,455	3	…	3	$640

Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2016 Request ($000)	FY 2017 Net Annualization (change from 2016) ($000)	FY 2018 Net Annualization (change from 2017) ($000)
GC Magnum Support Service	n/a	n/a	$1,200	$...	...
Network DMZ and Circuit	n/a	n/a	1,300	...	...
Digital Policy/Entity Attributes/Data Tagging	n/a	n/a	1,400	...	...
IC Desktop Environment (IC DTE)	n/a	n/a	1,000	...	...
IC Identity and Access Management (IdAM)	n/a	n/a	4,800	...	...
Total Non-Personnel	n/a	n/a	$9,700	$...	$...

Total Request for this Item

	Pos	Agt	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2017 Net Annualization (change from 2016) ($000)	FY 2018 Net Annualization (change from 2017) ($000)
Current Services	3	…	3	$640	…	$640	$…	$…
Increases	…	…	…	…	9,700	9,700	…	…
Grand Total	3	…	3	$640	$9,700	$10,340	$…	$…

* The current services amount only includes efforts directly related to the FBI's migration of IC ITE capabilities, not the Top Secret infrastructure costs the FBI pays currently to communicate with our IC partners, which is funded through Secure Work Environment (SWE) funding.

Performance Metrics

Enhancement Item	Performance Metric	FY 2016 Target
GC Magnum Support Service	Percentage of uptime for GC Magnum service through the redundant infrastructure	99%
Network DMZ and Circuit	Percentage of availability of IC ITE services	99%
Digital Policy/Entity Attributes/Data Tagging	Number of approved access rules and associated data tags	5
IC Desktop Environment (IC DTE)	Number of users migrated to IC DTE service	200
IC Identity and Access Management (IdAM)	Number of DTE users with authentication	200

VI. Program Non-recurs by Item

Item Name: **ODNI Directive**

Strategic Goal(s) & Objective(s): 1
Budget Decision Unit(s): Counterterrorism/Counterintelligence

Organizational Program: Counterintelligence

Program Change: Positions … Agt … FTE … Dollars ($2,000,000) (all non-personnel)

Description of Item
This reduction is being implemented per the direction of the Office of the Director of National Intelligence (ODNI).

Justification
Funding supported activities conducted in the FBI's National Security Recruitment Program (NSRP). The FBI discontinued the NSRP. This funding will be realigned to other IC elements.

Impact on Performance
No impact on performance.

Funding

Base Funding

FY 2014 Enacted				FY 2015 Enacted				FY 2016 Current Services			
Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)
…	…	…	$2,000	…	…	…	$2,000	…	…	…	$2,000

Non-Personnel Offset Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2016 Request ($000)	FY 2017 Net Annualization (change from 2016) ($000)	FY 2018 Net Annualization (change from 2017) ($000)
Total Non-Personnel	n/a	n/a	($2,000)	…	…

Total Offset for this Item

	Pos	Agt	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2017 Net Annualization (change from 2016) ($000)	FY 2018 Net Annualization (change from 2017) ($000)
Current Services	…	…	…	$…	$2,000	$2,000	$…	$…
Offset	…	…	…	…	(2,000)	…	…	…
Grand Total	…	…	…	$…	$…	$…	$…	$…

Item Name: **Program Non-Recur - Terrorist Explosive Device Analytical Center**

Strategic Goal(s) & Objective(s): 1
Budget Decision Unit(s): All
Organizational Program: Laboratory

Program Offset: Positions … Agt … FTE … Dollars ($10,000,000)

Description of Item
In FY 2015, the FBI received a one-time appropriation of $10,000,000 for the Terrorist Explosive Device Analytical Center (TEDAC). This funding is not recurred in FY 2016.

Justification
The FY 2015 funding was appropriated to the FBI for additional staff required to complete the activation of the new TEDAC facility in Huntsville, AL. Activation of the TEDAC facility has been delayed. Current plans are for the FBI to take delivery of the facility in early to mid-2015. Efficiency savings and the delay in delivery of the facility will allow the FBI to sustain necessary personnel.

Impact on Performance
No impact on performance.

Funding

Base Funding

FY 2014 Enacted				FY 2015 Enacted				FY 2016 Current Services			
Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)
116	13	116	$ 23,744	170	16	152	$42,691	170	16	170	$45,056

Non-Recur Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2016 Request ($000)	FY 2017 Net Annualization (change from 2016) ($000)	FY 2018 Net Annualization (change from 2017) ($000)
Total Non-Personnel	n/a	n/a	($10,000)	…	…

Total Non-Recur for this Item

	Pos	Agt	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2017 Net Annualization (change from 2016) ($000)	FY 2018 Net Annualization (change from 2017) ($000)
Current Services	170	16	170	$20,305	$24,751	$45,056	$…	$…
Non-recur	…	…	…	…	(10,000)	(10,000)	…	…
Grand Total	…	…	…	$20,305	$14,751	$35,056	$…	$…

Item Name: **Program Non-Recur – Hazardous Devices School**

Strategic Goal(s) & Objective(s): 1
Budget Decision Unit(s): All
Organizational Program: Critical Incident Response

Program Non-Recur: Positions … Agt … FTE … Dollars ($3,000,000)

Description of Item
In FY 2015, the FBI received a one-time appropriation of $3,000,000 for the Hazardous Devices School (HDS). This funding is not recurred in FY 2016.

Justification
The FY 2015 funding was appropriated to the FBI to for additional staff required to complete the activation of the HDS in Huntsville, AL. HDS is a training and certification center for bomb technicians. National standards published by the FBI for training state and local bomb squads provide the necessary foundation for an effective response to crimes involving hazardous devices, terrorist bombing campaigns, or use of a WMD. The FBI will identify efficiency savings to sustain personnel beyond 2015.

Impact on Performance
No impact on performance.

Funding

Base Funding

FY 2014 Enacted				FY 2015 Enacted				FY 2016 Current Services			
Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)
43	18	43	$18,579	56	19	50	$20,549	56	19	56	$20,859

Offset Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2016 Request ($000)	FY 2017 Net Annualization (change from 2016) ($000)	FY 2018 Net Annualization (change from 2017) ($000)
Total Non-Personnel	n/a	n/a	($3,000)	$…	$…

Total Non-Recur for this Item

	Pos	Agt	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2017 Net Annualization (change from 2016) ($000)	FY 2018 Net Annualization (change from 2017) ($000)
Current Services	56	19	56	$7,616	$13,243	$20,859	$…	$…
Non-recur	…	…	…	…	(3,000)	(3,000)	…	…
Grand Total	56	19	56	$7,616	$10,243	$17,859	$…	$…

Item Name: **Program and/or Administrative Savings**

Strategic Goal(s) & Objective(s): All
Budget Decision Unit(s): All
Organizational Program: All

Program Non-Recur: Positions … Agt … FTE … Dollars ($35,350,000) (all non-personnel)

Description of Item
The FBI has identified one-time program expenditures that will non-recur in 2016 and has captured those savings. Reductions to existing operations and services necessary to pay for increases in existing costs, including pay raises, FERS contributions, and GSA rent, among others.

Justification
Examples of savings to be realized in 2016 include, but are not limited to, reducing the FBI's physical footprint, leveraging and extending the useful life of existing technology, bulk purchases and bundling technology procurements.

Impact on Performance
None. Performance impact information is not yet available for this offset.

Funding

Base Funding

FY 2014 Enacted				FY 2015 Enacted				FY 2016 Current Services			
Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)
…	…	…	$…	…	…	…	$…	…	…	…	$…

Non-Personnel Non-Recur Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2016 Request ($000)	FY 2017 Net Annualization (change from 2016) ($000)	FY 2018 Net Annualization (change from 2017) ($000)
Total Non-Personnel	n/a	n/a	($35,350)	$...	$...

Total Non-Recur for this Item

	Pos	Agt	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2017 Net Annualization (change from 2016) ($000)	FY 2018 Net Annualization (change from 2017) ($000)
Current Services	…	…	…	$…	$3,292,967	$3,292,967	$…	$…
Non-recur	…	…	…	…	(35,350)	(35,350)	...	...
Grand Total	…	…	…	$...	$3,257,617	$3,257,617	$...	$...

VIII. Construction

Introduction

The FBI uses Construction funding for costs related to the planning, design, construction, modification or acquisition of buildings; and for the operation and maintenance of secure work environment facilities and secure networking capabilities. Construction funding supports both the national security and law enforcement missions of the FBI, though all Construction funding is presently scored to the Administration of Justice budget function. In the future, the FBI will devise a methodology to score Construction funding to both the National Defense and Administration of Justice budget functions.

Recent construction projects funded through this account include the Terrorist Explosive Device Analytical Center (TEDAC) in Huntsville, AL, as well as the expansion of the Hazardous Devices School (HDS), which is also located in Huntsville, AL. A portion of FY 2015 Construction funding is also being used for the DOJ consolidated data center initiative.

The FY 2016 request includes a total of $68,982,000 for Construction. This funding will support the Secure Work Environment (SWE) Program as well as projects at the FBI Academy in Quantico, VA. The FY 2016 request accounts for one-time expenditures associated with the activation of the TEDAC facility and the HDS and, as such represents a decrease of $41,018,000 from the FY 2015 enacted level.

Appropriations Language and Analysis of Appropriations Language

Appropriations Language for Construction

For necessary expenses, to include the cost of equipment, furniture, and information technology requirements, related to construction or acquisition of buildings, facilities and sites by purchase, or as otherwise authorized by law; conversion, modification and extension of Federally-owned buildings; preliminary planning and design of projects; and operation and maintenance of secure work environment facilities and secure networking capabilities; [$110,000,000] *$68,982,000*, to remain available until expended.

Analysis of Appropriations Language

No substantive changes.

Item Name: **Program Non-Recurs**

Strategic Goal(s) & Objective(s): All
Budget Decision Unit(s): All
Organizational Program: All

Program Non-Recur: Positions … Agt … FTE … Dollars ($41,018,000) (all non-personnel)

Description of Item
The FBI has identified one-time program expenditures that will non-recur in 2016 and has captured those savings.

Justification
The FBI received one-time construction funding in FY 2015 for the TEDAC and HDS facilities in Huntsville, AL.

Impact on Performance
None.

Funding

Base Funding

FY 2014 Enacted				FY 2015 Enacted				FY 2016 Current Services			
Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)
…	…	…	$97,482	…	…	…	$110,000	…	…	…	$68,982

Non-Personnel Non-Recur Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2016 Request ($000)	FY 2017 Net Annualization (change from 2016) ($000)	FY 2018 Net Annualization (change from 2017) ($000)
Total Non-Personnel	n/a	n/a	($41,018)	$...	$...

Total Non-Recur for this Item

	Pos	Agt	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2017 Net Annualization (change from 2016) ($000)	FY 2018 Net Annualization (change from 2017) ($000)
Current Services	…	…	…	$…	$3,292,967	$3,292,967	…	…
Non-recur	…	…	…	…	(35,350)	(35,350)	...	...
Grand Total	…	…	…	$...	$3,257,617	$3,257,617	...	...