U.S. Department of Justice
Federal Bureau of Investigation

FY 2017 Authorization and Budget Request to Congress

February 2016

Table of Contents

VII. Exhibits

A. Organizational Chart
B. Summary of Requirements
C. FY 2017 Program Changes by Decision Unit
D. Resources by DOJ Strategic Goal/Objective
E. Justification for Technical and Base Adjustments
F. Crosswalk of 2015 Availability
G. Crosswalk of 2016 Availability
H. Summary of Reimbursable Resources
I. Detail of Positions by Category
J. Financial Analysis of Program Changes
K. Summary of Requirements by Object Class
L. Status of Congressional Requests Studies, Reports, and Evaluations
M. Senior Executive Service Reporting

Exhibits
B. Summary of Requirements
C. FY 2017 Program Changes by Decision Unit
D. Resources by DOJ Strategic Goal/Objective
E. Justification for Technical and Base Adjustments
F. Crosswalk of 2015 Availability
G. Crosswalk of 2016 Availability
J. Financial Analysis of Program Changes
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) 2017 budget request proposes a total of $9,502,366,000 in direct budget authority, of which $8,718,884,000 is for Salaries and Expenses (S&E) and $783,482,000 is for Construction. The S&E request includes a total of 34,768 positions and 33,024 full time equivalents (FTE); the positions include:

- 12,892 Special Agents (SAs)
- 2,999 Intelligence Analysts (IAs)
- 18,877 professional staff (PS)

The S&E program increases total $227,785,000, 36 positions (18 SAs), and 18 FTE, for the following:

- $85,138,000 to increase cyber investigative capabilities
- $19,927,000 to support foreign intelligence and insider threat investigations and continuous evaluation
- $38,327,000 to counter the threat of Going Dark
- $6,779,000 to screen transnational organized crime (TOC) actors
- $26,997,000 to leverage the Intelligence Community Information Technology Enterprise (IC ITE) components and services
- $8,242,000 to support physical surveillance capabilities
- $7,375,000 for the Biometrics Technology Center (BTC) Operations and Maintenance (O&M) and,
- $35,000,000 to support the National Instant Criminal Background Check System (NICS).

The request also includes program offsets totaling $130,646,000, 426 positions (210 SAs), and 403 FTE. The net program change is an increase of $97,139,000, a decrease of 390 positions (192 SAs), and a decrease of 385 FTE. The FBI also proposes cancellations and balance offsets totaling $223,586,000, including $150,000,000 from Criminal Justice Information Services (CJIS) automation fund balances and cancellation of $61,586,000 in prior-year balances and $12,000,000 in GSA reimbursable work authority. Additionally, the request includes a balance transfer of $85,000,000 from S&E to Construction.

The $783,482,000 request for the Construction account includes:

- $646,000,000 for construction of the new FBI Headquarters (HQ);
- $85,000,000 from S&E prior-year balances for the Department of Justice (DOJ) Data Center Transformation Initiative;
- $50,500,000 million for the Secure Work Environment (SWE) Program; and,
- $2,000,000 for the FBI Academy at Quantico, VA.

The FBI continues to strategically assess current and prospective operations to ensure it meets mission requirements at the lowest possible cost to the U.S. taxpayer. The FY 2017 budget request is a product of these assessments and provides the resources to aggressively continue the FBI's strategic vision into the future.

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

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

The FBI contributes to the achievement of the following DOJ Strategic Goals:

- Strategic Goal 1: Prevent Terrorism and Promote the Nation's Security Consistent with the Rule of Law
- Strategic Goal 2: Prevent Crime, Protect the Rights of the American People, and Enforce Federal Law

Organization of the FBI: The FBI operates Field Offices in 56 major U.S. cities and 355 Resident Agencies (RAs) throughout the country. RAs 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.

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 CJIS Division and the BTC; and the Hazardous Devices School and Terrorist Explosive Device Analytical Center (TEDAC) at Redstone Arsenal in Huntsville, Alabama.

FBI Quantico

FBI CJIS Campus

The FBI also operates 63 Legal Attaché (Legat) offices and 27 sub-offices in 75 countries around the world.

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 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, the 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, 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)
4. Criminal Justice Services (CJS)

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

- Based on core mission function: Certain FBI divisions support one mission area exclusively and thus, 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.

- Based on workload: Critical investigative enablers, such as the Laboratory Division, the International Operations Division, and the Operational Technology Division, are allocated to the decision units based on workload. For example, 24 percent of the Laboratory Division's workload is in support of counterterrorism investigations and accordingly, 24 percent of the Laboratory Division's resources are allocated to the CT/CI decision unit. These percentage assignments may be revised upon review of workload.

- Pro-rated across all decision units: Administrative enablers, such as all three IT Divisions, the Facilities and Logistics Services Division, and the Human Resources Division, are pro-rated across all four decision units since these Divisions support the entire organization. This pro-rata spread is based on the allocation of operational divisions and critical investigative enablers.

The FBI's Construction funding is a separate funding account.

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 formulates and structures its budget according to the threats that the FBI works to deter. The FBI Director identifies these threats as the FBI's priorities and they are resourced accordingly.

Terrorism Threat: The FBI continues to identify individuals who seek to join the ranks of foreign fighters traveling in support of the Islamic State of Iraq and the Levant, commonly known as ISIL, and also homegrown violent extremists (HVE) who may aspire to attack the United States from within. These threats remain among the highest priorities for the FBI and the Intelligence Community (IC) as a whole.

Conflicts in Syria and Iraq continue to serve as the most attractive overseas theaters for Western-based extremists who want to engage in violence. As of July 2015, the FBI estimated upwards of 200 Americans had traveled or attempted to travel to Syria to participate in the conflict. The FBI closely analyzes and assesses the influence that groups, like ISIL, may have over those living in the U.S. to commit acts of violence have on individuals in the U.S. who are inspired to commit acts of violence. Whether individuals are affiliated with a foreign terrorist organization and are willing to travel abroad to fight, or are inspired by the call to arms to act in their communities, they potentially pose a significant threat to the safety of the U.S. and U.S. persons.

ISIL has proven relentless in its violent campaign to rule and has aggressively promoted its hateful message, attracting like-minded extremists including Westerners. To an even greater degree than al Qaeda and other foreign terrorist organizations, ISIL has persistently used the Internet to communicate. From a homeland security perspective, it is ISIL's widespread reach through the Internet and social media which is most concerning as ISIL has aggressively employed this technology for its nefarious strategy. ISIL blends traditional media platforms, glossy photos, in-depth articles, and social media campaigns that can go viral in a matter of seconds. No matter the format, the message of radicalization spreads faster than was imagined just a few years ago.

As a communication medium, social media is a critical tool for terror groups to exploit. One recent example occurred when an individual was arrested for providing material support to ISIL by facilitating an associate's travel to Syria to join ISIL. The arrested individual had multiple connections via a social media networking site with other like-minded individuals.

The violent extremist threat presents unique challenges because extremists do not share a typical profile, and may be self-radicalized and self-trained, and are willing to act alone, which makes them difficult to identify and stop. To address this challenge, the FBI's countering violent extremism (CVE) mission is built on four pillars: partnerships, engagement, prevention, and intervention. This approach seeks to identify threats by those who are planning, or engaged in, efforts to carry out attacks on the nation. The FBI disseminates information, intelligence, and awareness on emerging threats via engagement with community partners. For example, in July 2015, the FBI's Office of Partner Engagement (OPE) co-sponsored a summit with Rutgers University, the International Association of Chiefs of Police, and the Bipartisan Policy Center, to develop and coordinate countering violent extremism (CVE) activities. Approximately 150 people from law enforcement and academia attended this summit.

In addition, the FBI is an active participant in the Administration's recently established CVE Task Force. This task force will use a whole-of-government approach and function as a one-stop shop for federal partners, states, localities, tribal partners, academia, and the private sector to share critical

information, research, analysis, and best practices on this emerging and evolving threat. The FBI has been designated as the interagency lead in the Intervention Line of Effort in the newly established CVE task force.

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, 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.

A notable case success is the June 2015 guilty plea of Mostafa Ahmed Awwad, a Navy Civilian Engineer of Yorktown, VA, who pleaded guilty to attempted espionage for his efforts to provide schematics of the nuclear aircraft carrier USS Gerald R. Ford to Egypt. The FBI's Norfolk Field Office and Navy Criminal Investigative Service (NCIS) investigated the case, in cooperation with the Department of the Navy.

According to court documents, Awwad began working for the Department of the Navy in February 2014 as a civilian general engineer in the Nuclear Engineering and Planning Department at the Norfolk Naval Shipyard. Based on a joint investigation with the NCIS, an undercover FBI agent met with Awwad. During the meeting, Awwad claimed it was his intention to use his position with the U.S. Navy to obtain military technology for use by the Egyptian government, including but not limited to, the designs of the USS Gerald R. Ford nuclear aircraft carrier, a new Navy "supercarrier." Awwad agreed to conduct clandestine communications with the undercover FBI agent, as well as "dead drops" in a concealed location. Further, Awwad described a detailed plan to circumvent U.S. Navy computer security by installing software on his restricted computer system to copy documents without causing a security alert. Awwad provided the undercover FBI agent with four Computer Aided Drawings of a U.S. nuclear aircraft carrier downloaded from the Navy Nuclear Propulsion Information system and a thumb drive that contained more schematics of the USS Gerald R. Ford.

Former Assistant Director of Counterintelligence Division, Randall Coleman, stated "This case underscores the persistent national security threat posed by insiders stealing critical national defense information in order to benefit foreign governments. Fortunately, the aggressive counterintelligence posture of the FBI and our interagency partners enabled the identification and neutralization of Awwad's efforts before he transferred any information to a foreign power. Working together, we prevented the loss of billions of dollars in research costs and the exposure of potential vulnerabilities to our newest generation of nuclear aircraft carrier … the close collaboration between NCIS and the FBI thwarted this insider threat, and we will continue cooperative efforts to safeguard those who protect and serve in the Department of the Navy."

Cyber Threat: The U.S. continues to face a range of criminal, terrorist, and nation-state actor threats, such as organized crime syndicates seeking to defraud banks and corporations or spies seeking to steal defense and intelligence secrets.

While these threats are not new, the means by which actors implement them are changing. Today, these actors engage via the Internet and other computer networks. These networks provide ample cover from attribution, making the identification of the intrusion difficult as the motive of the attacker – be it

criminal, and terrorist or nation-state espionage – can remain unknown. 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 impacts by inexpensively attacking millions of victims. Despite formidable investments and concerted efforts by the private sector and government to build more secure and defensible computer networks, risks remain high and cybersecurity remains a rapidly growing concern with no easy solutions in sight.

The FBI's mission in cybersecurity is to counter the threat by investigating intrusions to determine criminal, terrorist, and nation-state actor identities, and engaging in activities to reduce or neutralize these threats. At the same time, 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 FBI and its federal partners take a whole-of-government approach to help deter future threats and bring closure to current threats that would otherwise continue to infiltrate and harm our network defenses.

In July 2015, the FBI, in coordination with foreign law enforcement partners, dismantled a computer hacking forum known as Darkode, which was a one-stop, high-volume shopping venue for some of the world's most prolific cyber criminals. This underground, password-protected online forum was a meeting place for those interested in buying, selling, and trading malware, botnets, stolen personally identifiable information, and other pieces of data and software that facilitated complex global cyber crimes. As the result of this multi-year investigation, called Operation Shrouded Horizon, the FBI's Cyber Division and international partner agencies took down Darkode through coordinated law enforcement action. This international takedown involved Europol and 20 cooperating countries and is believed to be the largest coordinated law enforcement operation to date against a forum based criminal enterprise. Operation Shrouded Horizon resulted in charges, arrests, and searches of 70 Darkode members and associates including indictments in the United States against 12 individuals associated with the forum including the administrator. As part of the law enforcement action, the FBI seized Darkode's domain name and servers. This operation highlighted the FBI Cyber Division's mission to identify, pursue, and defeat cyber adversaries targeting global U.S. interests through collaborative international partnerships.

***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, other complex financial crimes; and intellectual property rights enforcement.

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 U.S. border security, neighborhood safety, judicial integrity, and public infrastructure quality such as schools and roads.

Border Corruption: 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 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 FBI established the Border Corruption Initiative (BCI), which has developed a threat-tiered methodology, targeting border corruption in all land, air, and sea ports of entry to mitigate the threat posed to national security.

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 these cases involve accounting schemes – deceiving investors, auditors and analysts about the true condition of a corporation. 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.

Insider trading, which is a type of corporate fraud, 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.

Securities/Commodities Fraud: The FBI focuses our 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 an increase in securities fraud.

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. 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.

Health Care Fraud: The FBI identifies and pursues 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.

Other Complex Financial Crimes (Insurance, Bankruptcy, and Mass Marketing Fraud): The FBI also investigates other complex financial crimes that may impact the health of the U.S. economy. For example, if insurance fraud continues to increase, this will contribute to increases in insurance premiums as well as threaten the financial viability of insurance companies. Furthermore, 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, leading to higher potential for fraud within this area.

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 DOJ 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 and 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 regardless if they are 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. As of December 2015, of the FBI leads 164 VGSSTFs.

Gangs continue to proliferate, committing violent crime while expanding to suburban and rural areas. This is believed to be a result of better organized urban gangs. They are 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. Furthermore, gangs are partaking in less typical gang-related crime, such as human trafficking and white-collar crime like 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. This is 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 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 is also 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. 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. In addition, groups that preach hatred and intolerance plant the seeds of terrorism within our nation and undermine the principles on which this nation was founded.

- 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 U.S. 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, 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. 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: 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. 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.

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 where the FBI has jurisdiction. DOJ has reported that 25 percent of all violent crimes prosecuted by the U.S. Attorneys' Offices are related to Indian Country. ICC supports joint investigative efforts with the Bureau of Indian Affairs-Office of Justice Services, tribal law enforcement. ICC also manages 15 Safe Trails Task Forces that are addressing drug/gang and violent crimes in Indian Country. ICC cases are mostly reactive; however, many are cross-programmatic in nature and include public corruption and complex financial fraud.

Due to jurisdictional issues, the FBI is the primary law enforcement entity in Indian Country. The Bureau of Indian Affairs has a limited number of investigators, and 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.

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, 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 using 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 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.

C. Intelligence Driven Operations

The FBI's Intelligence Branch (IB) serves as the strategic leader of the FBI's intelligence program, driving the integration of intelligence and operations, and proactively engaging with FBI's partners across the IC and law enforcement community. The IB provides strategic direction and oversight for all aspects of the FBI's intelligence program, overseeing the implementation of our intelligence strategy and its six areas of focus: workforce success, culture and mindset, technology capabilities, information sharing, collection, and exploitation, and analysis.

The Executive Assistant Directors for Intelligence and National Security collaborate closely to manage all of the FBI's intelligence and national security operational components, including the Counterintelligence Division, Counterterrorism Division, Cyber Division, Directorate of Intelligence, High-Value Detainee Interrogation Group, Terrorist Screening Center, and Weapons of Mass Destruction Directorate. Additionally, the IB coordinates the management of the FBI's National Intelligence Program (NIP) resources, which support engagement with partners as well as intelligence-related training, technology, and secure work environments.

The Executive Assistant Director for Intelligence serves as the FBI's Foreign Language Program Manager, as well as the Executive Agent for the National Virtual Translation Center (NVTC), and is the

[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.

primary point of contact for the FBI's engagement with the Office of the Director of National Intelligence (ODNI) on NIP.

The FBI uses intelligence to understand national security threats, and to conduct operations to dismantle or disrupt those threats. Some examples 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 U.S..

- 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 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 the 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. The field offices then use this information to run the Field TRP process to prioritize the NTPs and other national and local threat issues. They also 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 FBI also uses the TRP's process outputs as the basis for the Integrated Program Management initiative, which standardizes how FBI HQ program manages the FBI's 56 Field Offices.

D. FBI's 2017 Budget Strategy

The FBI's budget strategy is based on the FBI's knowledge of current and future national security, cyber, and criminal investigative threats. The FBI has identified critical, enterprise-wide capabilities needed to perform its mission. This planning approach is necessary since to adapt to future unknown adversaries (e.g., nation, combination of nations, criminal enterprises, or individuals). In other words, the FY 2017 request designs future capabilities to address the range of expected national security, cyber threats, and crime problems regardless of who actually perpetrates the acts.

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.

E. 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 FBI implements the organizational EMS through Environmental Protection Programs (EPPs) that establish policy and procedure in major environmental programmatic areas. A number of EPPs (i.e., Solid Waste & Recycling Management; Petroleum, Oil, & Lubricants (POL) Management; Hazardous Waste Management; 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 has developed EPPs for implementing the National Environmental Policy Act (NEPA) within the FBI. The FBI is coordinating, through DOJ, the promulgation of NEPA regulations that will be an Appendix to the DOJ regulations. The completion date is subject to obtaining the Attorney General (AG)/Deputy Attorney General (DAG) signature.

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. The Bureau tracks energy and water audit findings for utility efficiencies to 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 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 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

Program	Description	Pos.	FTE	Dollars ($000)	Page
Salaries and Expenses Enhancements					
Cyber	To improve technical tools and high speed networks, and provide cyber-related training to increase the FBI's capability to combat highly sophisticated cyber threat actors.	…	…	$85,138	5-1
Foreign Intelligence and Insider Threat and Continuous Evaluation	To address threats posed by foreign intelligence and insiders. This initiative includes funding to acquire criminal activity data from multiple CJIS programs to integrate into the Continuous Evaluation (CE) Program.	...	…	19,927	5-3
Going Dark	To counter the threat of Going Dark, which includes the inability to access data because of challenges related to encryption, mobility, and anonymization. The FBI will develop and acquire tools for electronic device analysis, cryptanalytic capability, and forensic tools.	…	…	38,327	5-6
Transnational Organized Crime (TOC)	To expand existing information technology (IT) systems to create a consolidated TOC Watchlist and to formalize the TOC screening processes.	…	…	6,779	5-8
IC ITE	To increase the FBI's ability to collaborate with the IC by leveraging the IC Information Technology Enterprise (IC ITE).	…	…	26,997	5-13
Physical Surveillance	To increase the number of FBI priority targets under surveillance.	36	18	8,242	5-16
Biometrics Technology Center (BTC) Operations and Maintenance (O&M)	For O&M costs for the BTC, which will house the CJIS Divisions' Biometric Services Section with the biometric operations of the Department of Defense (DOD).	...	…	7,375	5-17
National Instant Criminal Background Check System (NICS)	To sustain investments made to NICS during FY 2016 to enable the FBI to keep up with increases in the volume of firearms background checks and to better provide for the recruitment and retention of NICS examiners.	…	…	35,000	5-20
Total, Salaries and Expenses Enhancements		**36**	**18**	**$227,785**	

Program	Description	Pos.	FTE	Dollars ($000)	Page
Salaries and Expenses Offsets					
Personnel Offset	Eliminate lower priority and unfilled positions.	(380)	(380)	($57,000)	6-1
Base Adjustment	Eliminate non-recurring one-time increases included in the FY 2016 Appropriation.	(46)	(23)	(73,646)	6-3
Total, Salaries and Expenses Offsets		**(426)**	**(403)**	**($130,646)**	
Construction Enhancements					
FBI Headquarters	Support construction of the new Headquarters (HQ) facility.	…	…	$646,000	8-3
DOJ Data Center Transformation Initiative (DCTI)	To support the Data Center consolidation project.	…	…	85,000	8-5
Total, Construction Enhancements		**…**	**…**	**$731,000**	
Construction Offsets					
Secure Work Environment (SWE) Reduction (Requirement)	This offset will reduce funding from the SWE Program, which includes Sensitive Compartmented Information Facilities (SCIF) and the Sensitive Compartmented Information Network (SCINet).	…	…	($16,500)	8-7
Total, Construction Offsets		…	…	**($16,500)**	

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, **[**$8,489,786,000**]** *$8,718,884,000*, of which not to exceed $216,900,000 shall remain available until expended: *Provided*, That not to exceed $184,500 shall be available for official reception and representation expenses.

(CANCELLATION)

Of the unobligated balances available under this heading, $223,586,000 are hereby permanently cancelled, including $150,000,000 from fees collected to defray expenses for the automation of fingerprint identification and criminal justice information services and associated costs: 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 Balances Budget and Emergency Deficit Control Act of 1985, as amended.

Analysis of Appropriations Language

- No substantive changes.

IV. Decision Unit Justification

A. Intelligence Decision Unit

INTELLIGENCE DECISION UNIT TOTAL*	Pos.	FTE	Amount ($000)
2015 Enacted	7,174	6,342	$1,654,977
2016 Enacted	7,191	6,804	1,689,100
Adjustment to Base and Technical Adjustments	1	16	55,675
2017 Current Services	7,192	6,820	1,744,775
2017 Program Increases	...	...	37,536
2017 Program Decreases	(129)	(125)	(45,345)
2017 Request	7,063	6,695	$1,736,966
Total Change 2016-2017	**(128)**	**(109)**	**$47,866**

* FY 2016 Enacted is based on FY 2016 Spend Plan submission.

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.

Intelligence Branch

As the strategic leader of the FBI's Intelligence Program, the Intelligence Branch drives collaboration to achieve the full integration of intelligence and operations throughout the organization. The branch has centralized authority and responsibility for all FBI intelligence strategy, policy, and functions, as well as for actively engaging with the FBI's partners across the intelligence and law enforcement communities.

Since its establishment in 2014, the Intelligence Branch has remained focused on facilitating the enhanced integration of intelligence and operations to enable the FBI to keep pace with the constantly evolving threat environment. To accomplish this mission, the Branch manages the planning and direction of the entire organization's intelligence work, regardless of its programmatic area or threat issue. Through a collaborative partnership and a matrix-management relationship with the operational components, the Intelligence Branch strategically directs all of the FBI's intelligence capabilities. This is accomplished by providing program management and overall guidance, while the operational components manage their workforces' day-to-day operations.

The Branch provides strategic direction and oversight for all aspects of the FBI's Intelligence Program, overseeing the implementation of the organization's intelligence strategy and its six areas of focus: workforce success, culture and mindset, technology capabilities, information sharing, collection, and exploitation and analysis. In addition, the Branch also ensures the FBI's intelligence production is objective and aligned with the organization and the Intelligence Community's intelligence priorities.

These efforts ensure intelligence is more seamlessly integrated into the FBI's work and enable the organization to operate under one enterprise-level plan so intelligence can effectively drive operations.

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 and academic communities, and the private industry 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 Office of Partner Engagement (OPE) implements initiatives and strategies that support engagement, communication, coordination, as well as cooperation efforts with law enforcement, intelligence, public and private agencies. It also 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; Fusion Centers; the Domestic Director of National Intelligence Representative program; 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 uses 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. 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 IC, 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.

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 SCIFs, and a secure information sharing capability through the SCINet. It also includes 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 IC through a connection to the Joint Worldwide Intelligence Communication System (JWICS) and use powerful applications to extract and analyze intelligence data in an efficient and timely manner. As part of the enhancements to the FBI's connection to other agencies, the FBI is adopting

initiatives through the IC ITE, which is an ODNI-led multi-year IT initiative to create an IC-wide infrastructure. IC ITE will provide shared, secure access to data, analytics, and resulting intelligence to every IC member through the following services: Applications Mall, Desktop Environment, Enterprise Management Services, IC Cloud, Identity Transport Service, Network Requirements and Engineering Services, IC Security Coordination Center, and Geospatial Intelligence Services.

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 Enterprise Portal (LEEP) system and UNet, the FBI's unclassified connection to the Internet.

Secure Work Environment (SWE)

Secure Work Environment (SWE) includes two main components - a SCIF and SCINet. A 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 equipped with intrusion detection and access control systems to prevent the entry of unauthorized personnel.

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 2015		**FY 2015**		**FY 2016**		**Current Services Adjustments & FY 2017 Program Changes**		**FY 2017 Request**	
Total Costs and FTE		**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		6,342	1,654,977	6,342	1,654,977	6,804	1,689,100	(109)	47,866	6,695	1,736,966
TYPE / STRATEGIC OBJECTIVE	**PERFORMANCE**	**FY 2015**		**FY 2015**		**FY 2016**		**Current Services Adjustments & FY 2017 Program Changes**		**FY 2017 Request**	
Performance Measure (non-NIP)	% of Counterterrorism FISA collection reviewed by the Language Program: • Audio • Text • Electronic File	 100% 100% 100%		 93% 100% 100%		 100% 100% 100%		 - - -		 100% 100% 100%	
Performance Measure: ***Responsiveness*** (NIP)	% of IIRs citing US Intelligence Community (USIC) Priority 1 or 2 requirements	75%		75.6%		80%		-		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. * FY 2016 Projected is based on FY 2016 Spend Plan submission.											

PERFORMANCE MEASURE TABLE

Decision Unit: Intelligence

Performance Report and Performance Plan Targets		FY 2011	FY 2012	FY 2013	FY 2014	FY 2015		FY 2016	FY 2017
		Actual	Actual	Actual	Actual	Target	Actual	Target	Target
Performance Measure	% of Counterterrorism FISA collection reviewed by the Language Program:								
	• Audio	83%	79%	100%	100%	100%	93%	100%	100%
	• Text	138%	56%	100%	100%	100%	100%	100%	100%
	• Electronic File (non-NIP)	39%	82%	79%	100%	100%	100%	100%	100%
Performance Measure: ***Responsiveness***	% of IIRs citing US Intelligence Community (USIC) Priority 1 or 2 requirements (NIP)	N/A	N/A	76%	76%	75%	75.6%	80%	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.

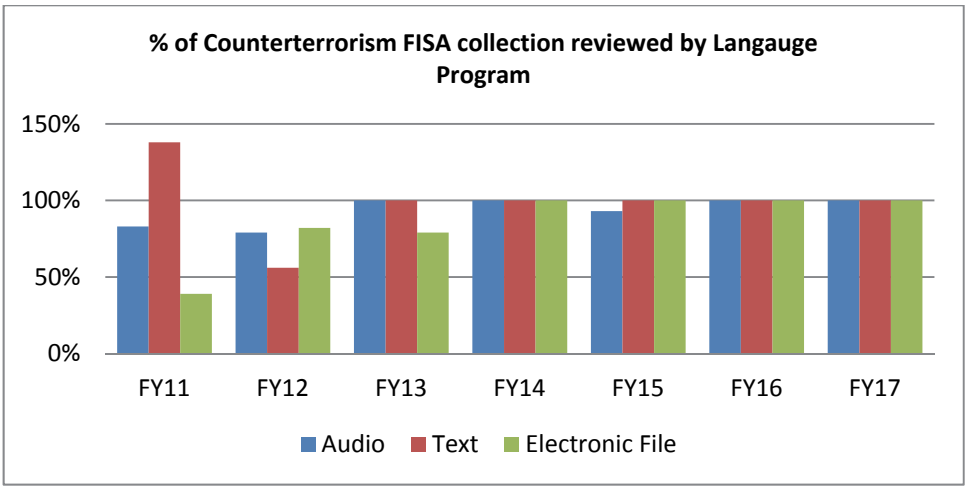
a. Performance Plan and Report for Outcomes

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

2015 Actuals:
Audio: *93%*
Text: *100%*
Electronic: *100%*

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

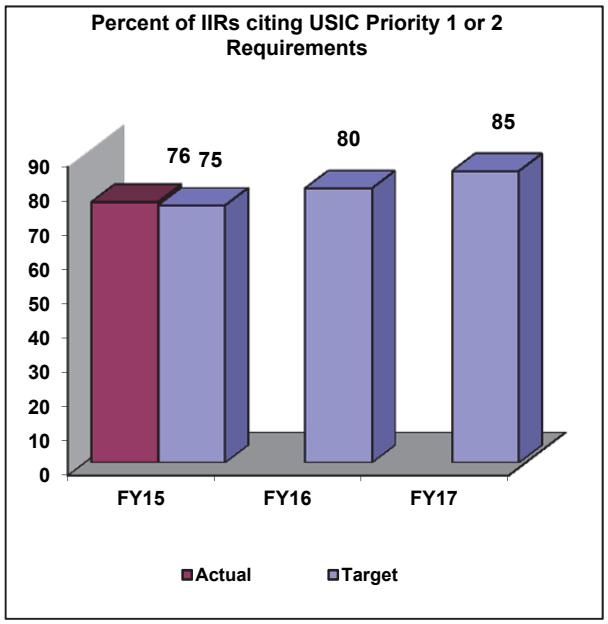
2017 Targets:
Audio: *100%*
Text: 100%
Electronic: 100%



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. However, if collection is unexpectedly high in languages for which resources are extremely scarce, review rates will decrease and the target may not be met. Conversely, it is possible to exceed the target if all materials collected in the current year, plus any unreviewed materials from the prior year, are reviewed within the current year. In the table above, FY 2011 through FY 2015 data represents actual results, while FY 2016 and FY 2017 data reflect targets.

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

2015 Actual: 76%
2016 Target: 80%
2017 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 measure will determine the FBI's responsiveness in meeting externally identified priority requirements and serving the needs of the USIC. Results on this measure will provide a better understanding of the FBI's capability to meet the given requirements and drive future collection efforts. The proposed FY 2016 and FY 2017 targets are based on current trends and projected future performance. The target will remain 80 percent in FY 2017.

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*	Pos.	FTE	Amount ($000)
2015 Enacted	13,091	11,815	$3,354,555
2016 Enacted	13,210	12,486	3,436,655
Adjustment to Base and Technical Adjustments	(6)	(3)	82,337
2017 Current Services	13,204	12,483	3,518,992
2017 Program Increases	36	18	96,478
2017 Program Decreases	(174)	(158)	(52,246)
2017 Request	13,066	12,343	$3,563,224
Total Change 2016-2017	**(144)**	**(143)**	**$126,569**

* FY 2016 Enacted is based on FY 2016 Spend Plan submission.

1. Program Description

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

Counterterrorism Program

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

The FBI is committed to stopping terrorism at any stage, from thwarting those intending to conduct an act of terrorism, to investigating the financiers of terrorist operations. All CT investigations are managed at FBI 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 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
- Enhance its overall contribution to the IC and senior policy makers in government by providing timely and accurate in-depth analysis of the terrorist threat and other information of value on an on-going basis

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

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.

[2] Please note that while the TSC and the FTTTF are part of the FBI's CT Program, their resources are scored to the Intelligence Decision Unit (IDU). Similarly, the Counterterrorism Analysis Section is embedded within CTD but is scored to the IDU.

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

The FBI has also established strong working relationships with other members of the IC. 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

The Weapons of Mass Destruction Directorate (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 uses this intelligence to combat WMD threats and events and 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. However, cases fall into the proliferation category when an organization or nation state attempts to acquire material and expertise relevant to a WMD program.

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 DI to create a Counterproliferation Center (CPC) 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. The CPC manages all investigations concerning counterproliferation, 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 CPC 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

Executive Order 12333 assigns to the Director of the FBI, under Attorney General, oversight and supervision responsibility for conducting and coordinating counterintelligence (CI) activities within the United States. The activities are designed to protect against intelligence collection conducted for, or on behalf of, foreign powers, organizations, or persons. Consequently, the FBI's CI Program mission is to identify, penetrate, and neutralize foreign-sponsored adversaries using intelligence and investigative activity. In this regard, the Counterintelligence Division (CD) uses the Threat Review and Prioritization Process (TRP) to prioritize national threat issues and develop national-level mitigation strategies. With this analytically driven process, the FBI is able to assess the activities of a foreign power against level of activity, nature of the targeting, and capability to threaten U.S. national security.

At the FBI HQ management level, the CI Program coordinates intelligence and investigative operations by providing strategic guidance, oversight, and support to field offices in connection with CI efforts in its territories. Additionally, significant efforts have been made in building

strong relationships with various IC agencies and friendly foreign intelligence services (FISs). The CI program coordinates on many interagency drafts and provides extensive input into Sense of the Community Memoranda (SOCMs), Joint Community Assessments (JCAs), and Presidential Daily Briefing (PDBs).

In connection with its efforts to enhance the CI Program's mission, CD will enhance the FBI's capacity to address its (CI) responsibilities by providing:

- A centrally controlled and managed CI Program, which 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 emphasizing 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 CI 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 integrates Headquarters and field resources to combat 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 state, local, federal, 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 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, 1.3, and 1.4)

Decision Unit: Counterterrorism/Counterintelligence

WORKLOAD/ RESOURCES		Target		Actual		Projected*		Changes		Requested (Total)	
		FY 2015		FY 2015		FY 2016		Current Services Adjustments & FY 2017 Program Changes		FY 2017 Request	
Number of Cases: Counterterrorism, Counterintelligence, & Computer Intrusions		†				†		†		†	
Total Costs and FTE		**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		11,815	3,354,555	11,815	3,354,555	12,486	3,436,655	(143)	126,569	12,343	3,563,224
TYPE/ STRATEGIC OBJECTIVE	**PERFORMANCE**	**FY 2015**		**FY 2015**		**FY 2016**		**Current Services Adjustments & FY 2017 Program Changes**		**FY 2017 Request**	
Program Activity/ 1.1	**1. Counterterrorism (CT)**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		6,853	1,945,612	6,853	1,945,612	7,242	1,993,260	(83)	73,410	7,159	2,066,670
Workload -- # of cases investigated (pending and received)		†		†		†		†		†	
Program Activity/ 1.3	**2. Counterintelligence**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		4,017	1,140,549	4,017	1,140,549	4,245	1,168,463	(49)	43,033	4,196	1,211,496
Program Activity/ 1.4	**3. Cyber Program (Intrusions)**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		945	268,394	945	268,394	999	274,932	(11)	10,126	988	285,058
Workload -- # of cases investigated (pending and received)		†				†		†		†	
Efficiency Measure	Efficiency cost savings from online cyber training ($000)	$2,750		$1,207		$2,000		-		$2,000	

Data Definition, Validation, Verification, and Limitations:

† Due to the large number of external and uncontrollable factors influencing these data, the FBI does not project numbers of cases.
* FY 2016 Projected is based on FY 2016 Spend Plan submission.

Performance Report and Performance Plan Targets		FY 2010	FY 2011	FY 2012	FY 2013	FY 2014	FY 2015	FY 2015	FY 2016	FY 2017
		Actual	Actual	Actual	Actual	Actual	Target	Actual	Target	Target
Efficiency Measure	Cost avoidance from online Cyber training ($000)	$819	$4,987	$2,395	$3,585	$2,000	$2,000	$1,207	$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, 1.3, 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.

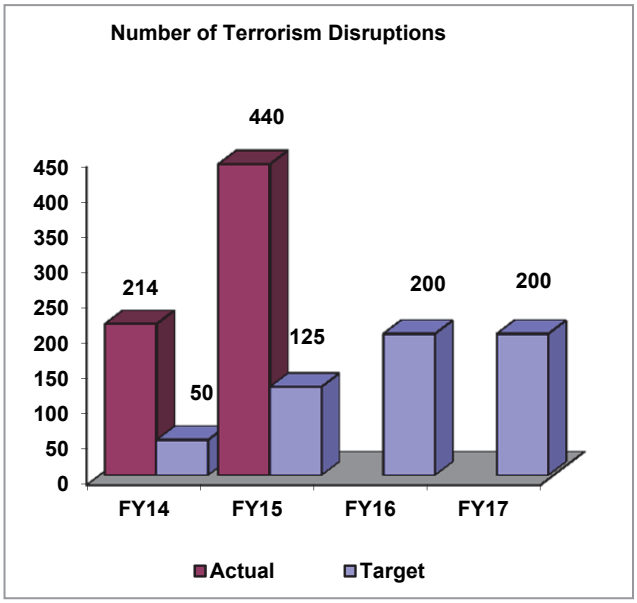
b. Strategies to Accomplish Outcomes
The FBI must be able to effectively respond to the challenges posed by unconventional terrorist methods, such as the use of chemical, biological, radiological, explosive, and nuclear materials. When terrorist acts do occur, the FBI must rapidly identify, locate, apprehend, 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 2014-2016 Priority Goal)

FY 2015 Actual:	440
FY 2016 Target:	200
FY 2017 Target:	200

Discussion: A disruption is defined as interrupting or inhibiting a threat actor from engaging in criminal or national security-related activity. A disruption is the result of direct actions and may include, but is not limited to, the arrest; seizure of assets; or impairing the operational capabilities of



key threat actors. 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.

The FBI significantly exceeded its target of 125 disruptions due to factors including increasing threats in other regions and external plotting directed at the U.S. homeland and our interests abroad. Additionally, the FBI's fusion cells continue to increase our ability to mitigate threats to the homeland by pursuing a target-centric approach with IC strategic and tactical analyses and operational capabilities. Because counterterrorism threats are constantly changing, these will have a direct impact on disruption statistics. Reported disruptions can only result from investigations predicated on potential plots, which are outside of FBI control. Forecasts for disruptions can therefore be a challenge to quantify for future years, but the target will increase by 75 to account for the success of 2015 and the outlook for future years.

Counterintelligence (CI)

a. Performance Plan and Report for Outcomes

Please refer to the Classified Addendum.

b. Strategies to Accomplish Outcomes

The FBI's Counterintelligence (CI) Program continues to execute a comprehensive National Strategy for Counterintelligence within an Integrated Program Management framework which streamlines and prioritizes the FBI's approach to threats and the execution of its strategy. This strategy is predicated on the need for centralized national direction that facilitates a focus on common priorities and specific objectives in all areas of the country. It also recognizes the need for collaboration and strategic partnerships, both within the USIC, as well as within the Business and Academic sectors. This strategy enables the program to combat effectively the intelligence threats facing the United States while effectively leveraging its available resources.

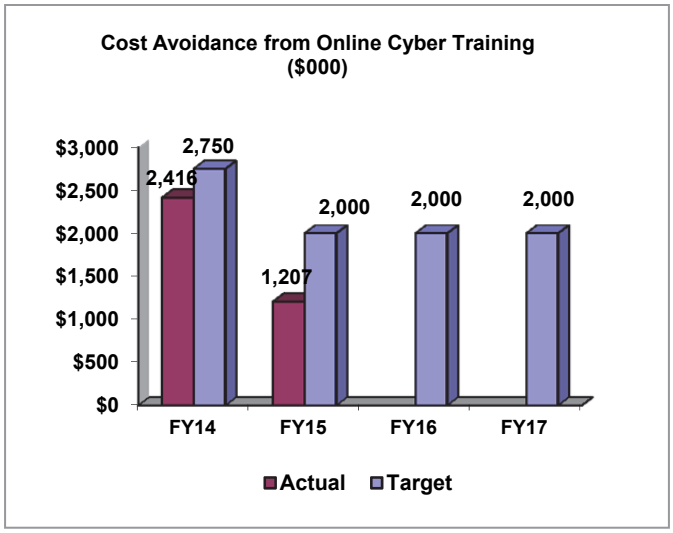
Computer Intrusions

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 2015 Actual: $1,207,000
FY 2016 Target: $2,000,000
FY 2017 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.

The FBI believes that it did not meet the FY 2015 target due to the transfer of lower level cyber training courses to the FBI's Training Division, and Cyber Division's new online courses are at a more advanced level, and therefore would be more applicable to a significantly smaller population. In addition, due to increased funding for cyber training that includes travel expenses, the expansion of in-person course offerings, and the request from the workforce and Executive Management that personnel attend in-person training, there has been a reduction in cyber online enrollment for FY 2015.

C. Criminal Enterprises Federal Crimes Decision Unit

CRIMINAL ENTERPRISES/FEDERAL CRIMES DECISION UNIT TOTAL*	Pos.	FTE	Amount ($000)
2015 Enacted	12,681	11,648	$2,848,602
2016 Enacted	12,531	12,006	2,887,249
Adjustment to Base and Technical Adjustments	1	(17)	2,457
2017 Current Services	12,532	11,989	2,889,706
2017 Program Increases	...	...	49,105
2017 Program Decreases	(118)	(115)	(26,417)
2017 Request	12,414	11,874	$2,912,394
Total Change 2016-2017	**(117)**	**(132)**	**$25,145**

* FY 2016 Enacted is based on FY 2016 Spend Plan submission.

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, 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

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 Crime and Gang Threats

The mission of the Violent Crime and Gang Section (VCGS) 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 staff 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. Legats partner 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 to support the International Law Enforcement Academies in Budapest or Botswana, or teach their law enforcement partners about proper investigation techniques 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 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 enterprise
  - 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:

- Identify cyber threats to U.S. interests posed by cyber criminal actors, provide assistance to field office investigators who are aggressively pursuing the threat, and ultimately defeat the cyber threat actors
- Develop a holistic assessment of the threat posed by cyber criminals and organizations to partner countries and launch aggressive and comprehensive mitigation strategies through joint investigations and operational partnerships with law enforcement partners, private industry, and academia
- Enable a two-way exchange of information between law enforcement and industry experts to collaborate on initiatives targeting major cyber crimes domestically and abroad
- Receive, develop, and refer Internet crime complaints, such as online fraud (in its many forms), intellectual property rights (IPR) matters, computer intrusions (hacking), economic espionage (theft of trade secrets), child pornography, international money laundering, identity theft, and a growing list of additional criminal matters

- 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 the following:
  - Race, sexuality, color, religion, or ethnic/national origin
  - Reports of abuse of authority under color of law
  - Reports of slavery and involuntary servitude
  - 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.

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 Indian Country
  - Improve the overall quality of law enforcement service in Indian Country 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 Indian Country
  - Provide training to Indian Country Special Agents, support personnel, and BIA/tribal police

- Support DOJ efforts to professionalize law enforcement operations in Indian Country, including crime statistics reporting, records management, automation, and case management.

- Provide a rapid and effective investigative response to reported federal crimes involving the following:
  - 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

  - 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 leadership and by using sensitive investigative and intelligence techniques to initiate long term proactive investigations.

- Expand and create new partnerships with the USIC and Other Government Agencies to better coordinate and facilitate the flow and use 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 position 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 2015		FY 2015		FY 2016		Current Services Adjustments & FY 2017 Program Changes		FY 2017 Request	
Workload -- # of cases investigated (pending and received)		†				†		†		†	
Total Costs and FTE		**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		11,648	2,848,602	11,648	2,848,602	12,006	2,887,249	(132)	25,145	11,874	2,912,394
TYPE/ STRATEGIC OBJECTIVE	**PERFORMANCE**	**FY 2015**		**FY 2015**		**FY 2016**		**Current Services Adjustments & FY 2017 Program Changes**		**FY 2017 Request**	
Program Activity/ 2.3, 2.5	**1. White-Collar Crime/Cybercrime**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		5,358	1,310,357	5,358	1,310,357	5,523	1,328,135	(61)	11,564	5,462	1,339,701
Workload -- # of cases investigated (pending and received)		†				†		†		†	
Performance Measure	Restitutions & Recoveries / Fines ($000) • Intellectual Property Rights Violations • Public Corruption • White Collar Crimes (all other)	††				††		††		††	
Performance Measure	Convictions/Pre-Trial Diversions (total) • Intellectual Property Rights Violations **[Discontinued measure]** • Public Corruption • White Collar Crimes (all other)	††				†† †† ††		†† †† ††		†† †† ††	
Performance Measure	Number of Criminal Organizations Engaging in White-Collar Crimes Dismantled	368		416		368		61		429	
Efficiency Measure	% of Major Mortgage Fraud Investigations to all pending Mortgage Fraud Investigations	72%		74%		72%		…		72%	
Performance Measure	Number of convictions for Internet fraud	††		19		††		††		††	

TYPE/ STRATEGIC OBJECTIVE	PERFORMANCE	FY 2015		FY 2015		FY 2016		Current Services Adjustments & FY 2017 Program Changes		FY 2017 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	6,290	1,538,245	6,290	1,538,245	6,483	1,559,114	(71)	13,578	6,412	1,572,693
Workload -- # of cases investigated (pending and received)			†				†		†		†
Performance Measure	Convictions/Pre-trial Diversions • Organized Criminal Enterprises • Gang/Criminal Enterprises • Crimes Against Children • Civil Rights		 †† †† †† ††				 †† †† †† ††		 †† †† †† ††		 †† †† †† ††
Efficiency Measure	% of FBI OCDETF Investigations with links to CPOT-linked DTOs*		15%		22%		N/A		…		N/A
Performance Measure	CPOT-Linked DTOs* • Disruptions • Dismantlements		 40 20		 136 34		 N/A N/A		 … …		 N/A N/A
Performance Measure	Number of Organized Criminal Enterprise Dismantlements		38		120		38		26		64
Performance Measure	Number of Gang/Criminal Enterprises Dismantlements		99		153		99		84		183
Performance Measure	Number of Agents serving on Violent Crime Task Forces		†		1,146		†		†		†

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 2016 Projected is based on FY 2016 Spend Plan submission.

		FY 2010	FY 2011	FY 2012	FY 2013	FY 2014	FY 2015	FY 2015	FY 2016	FY 2017
		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)	 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	 474,114 5,441,15 4	 N/A N/A N/A	 705,289 12,051,979	 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)	 84 954 3,357	 81 969 3,384	 N/A 924 3,529	 N/A 1,038 2,958	 N/A 1,087 2,695	 N/A N/A 3,351	 N/A 583 2,564	 N/A N/A 3,351	 N/A N/A 3,351
Performance Measure	Number of Criminal Organizations Engaging in White Collar Crimes Dismantled	236	368	409	458	464	385	416	385	429
Efficiency Measure	% of Major Mortgage Fraud Investigations to all pending Mortgage Fraud investigations	71%	71%	71%	72%	73%	72%	74%	72%	72%
Performance Measure	Number of convictions for Internet fraud	N/A	27	21	22	12	N/A	19	N/A	N/A
Performance Measure	Number of high-impact Internet fraud targets neutralized	12	11	23	17	25	17	23	17	17
Performance Measure	Convictions/Pre-Trial Diversions: • Organized Criminal Enterprises • Gang/Criminal Enterprises • Crimes Against Children • Civil Rights	 424 2,163 245 248	 812 N/A 338 268	 845 6,467 373 227	 833 N/A 1,312 238	 723 7,338 1,570 205	 747 N/A N/A 350	 1,455 2,445 1,401 56	 747 N/A N/A 350	 800 N/A N/A 350
Efficiency Measure	% of FBI OCDETF Investigations with links to CPOT-linked DTOs	15.89%	16.35%	19%	20%	20%	15%	22	N/A	N/A
Performance Measure	CPOT-Linked DTOs • Disruptions • Dismantlements	 40 12	 54 22	 64 30	 139 40	 150 31	 40 20	 136 34	 N/A N/A	 N/A N/A
Performance Measure	Number of Organized Criminal Enterprise Dismantlements	39	39	47	70	82	38	120	38	64
Performance Measure	Number of Gang/Criminal Enterprise Dismantlements	124	165	163	251	167	99	153	99	183
Performance Measure	Number of Agents serving on Violent Crime Task Forces	N/A	1,050	1,071	1,131	1,121	N/A	1,146	N/A	N/A

3. Performance, Resources, and Strategies

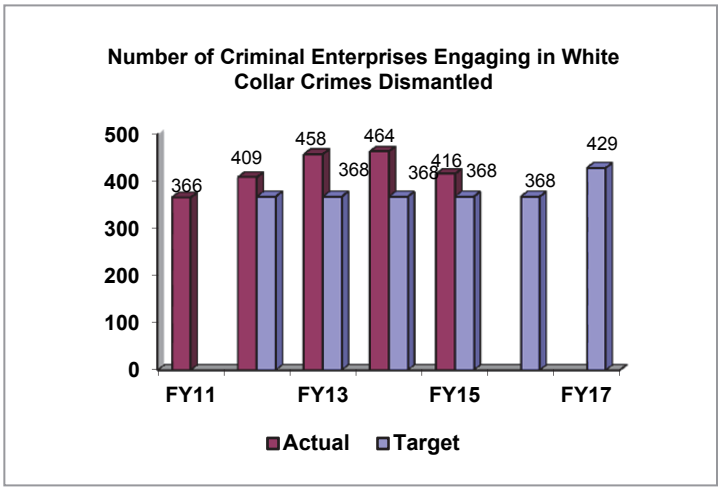
White Collar Crime

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.

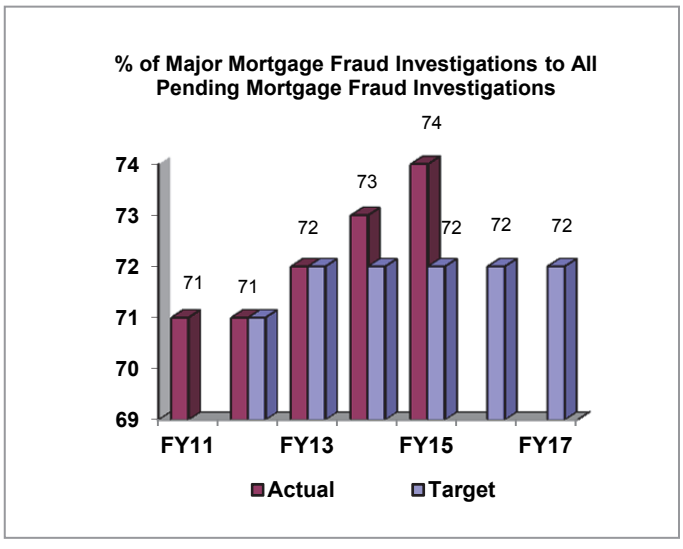
FY 2015 Actual: 416
FY 2016 Target: 368
FY 2017 Target: 429



Discussion: The FBI established the FY 2017 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.

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

FY 2015 Actual: 74
FY 2016 Target: 72
FY 2017 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 and 2017. 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.

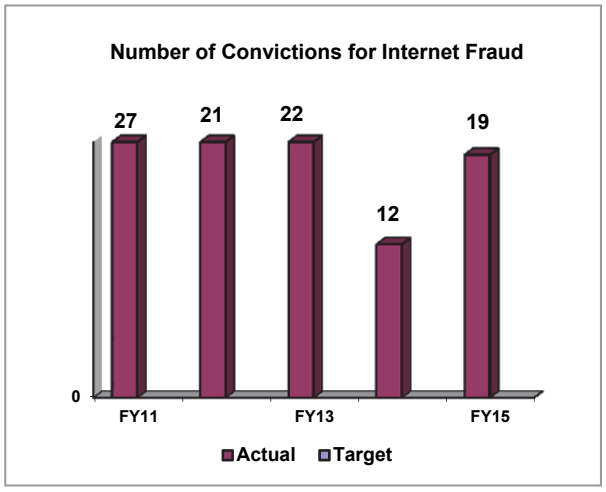
b. Strategies to Accomplish Outcomes
In FY 2017, the FBI will continue to pursue corporate fraud, securities fraud, mortgage fraud, other types of financial institution fraud, health care fraud, money laundering, and insurance fraud, which all threaten to undermine our Nation's financial infrastructure. 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 2017 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.

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.

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. Within the strategy, the FBI identifies the gangs posing the greatest danger to American communities; combines and coordinates the efforts of the local, state, and federal law enforcement in Violent Gang Safe Streets Task Forces throughout the U.S.; and uses 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). GangTECC is 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. It is 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.[3] The

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

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
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

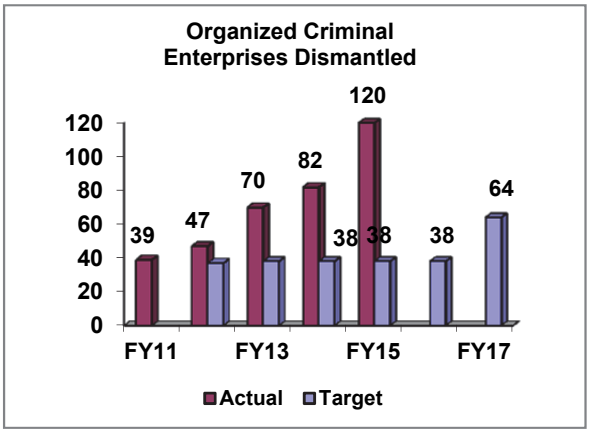
a. Performance Plan and Report for Outcomes

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. 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 2015 Actual: 120
FY 2016 Target: 38
FY 2017 Target: 64



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.

Gang/Criminal Enterprises

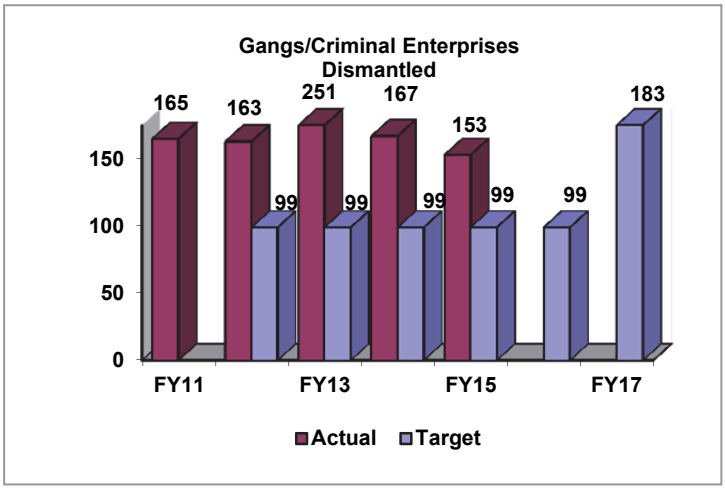
The mission of the FBI's Gang/Criminal Enterprise Program is to disrupt and dismantle the domestic cells (local, regional, national, and transnational) of criminal enterprises, which pose the greatest threat to the economic and national security of the U.S. Many of these criminal enterprises have ties to North, Central, and South America. The FBI will accomplish this through criminal investigations, involvement in the Organized Crime Drug Enforcement Task Force Program (OCDETF), and support and leadership of HIDTA initiatives. The FBI directs the majority of its anti-gang efforts 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 2015 Actual: 153
FY 2016 Target: 99
FY 2017 Target: 183



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. The FBI focuses resources on coordinated, nationwide investigations targeting the entire infrastructure of major DTOs. The Bureau also targets DTO members who traffic in narcotics and launder illicit proceeds. Strategic initiatives are developed to effectively exploit the DTO's most vulnerable points, thus attacking its infrastructure.

D. Criminal Justice Services Decision Unit

CRIMINAL JUSTICE SERVICES DECISION UNIT TOTAL*	Pos.	FTE	Amount ($000)
2015 Enacted	2,091	1,968	$468,435
2016 Enacted	2,226	2,076	476,782
Adjustment to Base and Technical Adjustments	4	41	(8,510)
2017 Current Services	2,230	2,117	468,272
2017 Program Increases	...	...	44,666
2017 Program Decreases	(5)	(5)	(6,638)
2017 Request	2,225	2,112	$506,300
Total Change 2016-2017	**(1)**	**36**	**$29,518**

* FY 2016 Enacted is based on FY 2016 Spend Plan submission.

1. Program Description

The Criminal Justice Services (CJS) Decision Unit comprises the following:

- 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
- International training program of the International Operations Division
- 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).

CJIS Division

The mission of the CJIS Division is to equip 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, seven days a week. The NGI system, which expanded and significantly enhanced the FBI's biometric identification capabilities, became fully operational in September 2014, providing the criminal justice community with the world's largest and most efficient electronic repository of biometric and criminal history information. In FY 2014, approximately 70 million fingerprint background checks were processed. In FY 2015, approximately 77 million fingerprint checks were processed.

NGI added the National Palm Print System containing over 14 million images, and the Interstate Photo System (IPS), as well as new services, such as rapid mobile searches, facial recognition, and Rap Back. NGI also improved major features such as system flexibility, storage capacity, accuracy and timeliness of responses, and the interoperability with the biometric matching systems of the Department of Homeland Security and the Department of Defense. In addition, the NGI system was designed to allow the addition of future biometric modalities; a pilot is underway to explore iris enrollment and recognition.

The Rap Back service allows authorized agencies to receive notification of activity on individuals who hold positions of trust or who are under criminal justice supervision or investigation. The IPS, through Facial Recognition, now provides ways to search over 30 million criminals' photos – data the FBI has collected for decades – and generates a list of ranked candidates to be used as potential investigative leads by authorized agencies, adding another way biometrics can be used as an investigative tool.

National Crime Information Center (NCIC): The NCIC is a computerized database of documented criminal justice information available to law enforcement agencies nationwide, 24 hours a day; 365 days a year with an average up-time of 99.7 percent in the last 12 months. 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 12.9 million transactions a day. On December 18, 2015, NCIC processed a record 15.3 million transactions with an average response time of less than .0128 seconds.

The last major upgrade to NCIC occurred in July 1999, with the NCIC 2000 project. To meet the needs of the criminal justice community, the FBI has implemented many system/technical enhancements since July 1999. However, as the lifecycle of the current technology deployed in NCIC 2000 nears its end, the FBI is preparing for the next major upgrade to the NCIC known as NCIC 3rd Generation (N3G).

The purpose of the N3G project is to identify requirements which will improve, modernize, and expand the existing NCIC system so it will continue to provide real time, accurate, and complete criminal justice information to support law enforcement and criminal justice communities.

Over the past 18 months, the FBI completed the largest User Canvass in FBI history, talking to personnel representing 500 federal, state, tribal, and local agencies. In total, users provided over 5,500 responses and suggestions for improvements, new capabilities, and changes to the NCIC system. From this user response data, the Bureau developed high level user concepts for the next generation of NCIC and review them through the Advisory Policy Board (APB). Next steps will be to develop a concept of operations, while also decomposing each of the concepts in detail and vetting topics through the APB for the third generation of NCIC to emerge.

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 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 FBI and its partners while also enabling more rapid deliveries of future improvements and/or newly legislated changes. The New NICS will use advances in technology, including Computer Telephony Integration, to dramatically improve user interfaces, thereby 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. The New NICS Program Office is collaborating with the development contractor on the revised plan/schedule that completes Phase 1 and the remainder of the contract's scope. The FBI is partnering with U.S. Digital Services to ensure that the New NICS development meets its objectives.

In FY 2015, the NICS processed 21.3 million inquiries. The FBI conducted approximately 8.5 million of these checks, resulting in 100,749 denials to prohibited persons. The remaining 12.8 million checks were conducted by individual states. On November 27, 2015, 185,345 transactions were processed through the NICS in a single day. This was the highest transaction volume day in history, surpassing December 21, 2012, when the aftermath of the Sandy Hook shooting escalated the transaction volume to 177,170 background checks processed in a single day.

Uniform Crime Reporting (UCR): The FBI's UCR Program has served as the national clearinghouse for the collection of data regarding crimes reported to law enforcement since 1930. The FBI 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, the FBI collects more detailed data on each single crime occurrence within 49 specific offenses.

Currently, the FBI is working with the APB to complete the New UCR to manage the acquisition, development, and integration of a new information systems solution. As part of this transition, in 2013 the FBI stopped accepting hard copy submissions of UCR forms. Also, in the interest of improving crime data collections, the FBI is partnering with the National Academy of Sciences (NAS) 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 NAS Panel on Modernizing the Nation's Crime Statistics was organized with a mandate to assess the landscape of national crime statistics. At its core, the concern was whether current measures provide the information that is needed. The Panel's Statement of Task identifies three main areas for assessment: substantive, methodological, and implementation. It is anticipated that the Panel will release two reports that will provide their recommendations for changes or additions to the data collections maintained by the Bureau of Justice Statistics and the FBI's UCR Program. The interim report was originally scheduled to be released December 2014, and the final report scheduled to be completed by May 2015. However, the interim report has not yet been released.

The FBI 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 has completed a comprehensive study "Ambushes and Unprovoked Attacks: Assault on Our Nation's Law Enforcement Officers." This study, which began in March 2013, focused on felonious killings and assaults of law enforcement officers during ambush situations. Upon completion of the Ambush Study, the LEOKA Program requested permission to continue research to determine whether findings from the Violent Encounters (2006) study are still relevant to today's law enforcement environment. The findings from this research and the ambush study will allow the FBI to update its Officer Safety

Awareness Training curriculum and continue to provide a professional service to our law enforcement partners.

In February 2015, the FBI Director established the need to generate a pathway to greater crime data collection and to improve the nation's crime statistics for reliability, accuracy, accessibility, and timeliness of the data. As a Director's Priority Initiative, the Bureau will achieve this effort through the completion of a five prong approach. Prong One is to transition local, state, and tribal law enforcement agencies (LEAs) from the Summary Reporting System (SRS) to the NIBRS. The FBI seeks to sunset the SRS by January 1, 2021 and replace it with the NIBRS as the national standard for crime reporting. Prong Two is to collect use of force statistics on all non-fatal/fatal police officer-involved incidents at the local, state, tribal, and federal levels to replace the current collection of justifiable homicide by law enforcement. The FBI plans to complete Prong 2 by 2018. Prong Three and Prong Four both focus on facilitating federal LEAs to comply with the Uniform Federal Crime Reporting Act of 1988, which mandates all federal agencies report their crime statistics. Prongs Three and Four will be completed between 2017 and 2021. Prong Five, which will be completed by 2018, is to develop technical efforts to ensure crime data is accessible and timely.

In 2015, 6,614 agencies (approximately 36.4 percent of all UCR agencies) reported crime to the FBI Uniform Crime Reporting (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 transitioning the UCR Program to a NIBRS only data collection within five years.

National Data Exchange (N-DEx): The National Data Exchange (N-DEx) is an unclassified national information-sharing system that enables criminal justice agencies to search, link, analyze, and share local, state, tribal, and federal records. 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; discover relationships between non-obvious and seemingly unrelated data; and obtain collaboration among agencies by allowing its users to coordinate efforts in a secure online environment.

The N-DEx connects many regional and local information-sharing systems and leverages their collective power to provide access to millions of records. The 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. The N-DEx contains over 284 million records from more than 5,500 criminal justice agencies. Additionally, N-DEx provides access to an additional 314 million records from the Department of Homeland Security, the Interstate Identification Index, the NCIC, and Interpol. System records contain information on more than 2.1 billion entities (persons, places, things, and events).

During FY 2015, N-DEx added more than 41 million system records, over 317 participating agencies, and provided access to an additional 213 million leveraged records. The FBI projects that by the end of FY 2016, an additional 200 criminal justice agencies will share information via N-DEx. Additionally, N-DEx expects to expand usage to all Regional Information Sharing System users nationwide, increase participation with the Law Enforcement Information Exchange, establish two way searching between N-DEx and the International Justice and Public Safety Network, and continue to acquire new datasets to enhance the N-DEx system.

Law Enforcement Enterprise Portal (LEEP): The Law Enforcement Enterprise Portal (LEEP) is a secure, Internet-based information sharing system for agencies around the world that are involved in law enforcement, first response, criminal justice, anti-terrorism, and intelligence. 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 Law Enforcement Online (LEO) services, including Virtual Command Centers (VCCs), Special Interest Groups (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 24 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, and eGuardian.

In FY 2016, work will continue on an industry portal solution (ILEEP) 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 American Society of Crime Laboratory Directors accredited the FBI Laboratory accredited in August 2008 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. The FBI Laboratory performs free-of-charge 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. 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. The Laboratory provides biometric identification services 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 IC, the U.S. military, and other partners. In January 2015, then 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 2015, the FBI conducted approximately 691,000 forensic examinations (this included FBI, and other Federal, state and local examinations). Of the total forensic examinations, 89.6 percent were in support of FBI-led investigations and 10.4 percent were in support of other law enforcement partner investigations. Estimates for FY 2016 are approximately 690,000 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 by their sponsoring organizations to have potential for further advancement in their careers. In FY 2015, there were 783 state and local law enforcement officers, and 95 international law enforcement officers that participated in the National Academy program at the FBI Academy in Quantico, Virginia. In FY 2016, is the FBI estimates that 900 state and local law enforcement officers and 100 international law enforcement officers will participate in the National Academy program.

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 2015, an estimated 97,000 criminal justice personnel received training from FBI instructors at state, regional and local training facilities. In FY 2016, the FBI Academy estimates it will also train 97,000 criminal justice personnel.

International Operations Division

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 State Department partially reimburses the FBI. In FY 2014, the FBI provided training to 6,304 international police officers and executives representing 96 countries. In FY 2015, the FBI estimates it will also train approximately 6,300 international police officers and executives.

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 2015	FY 2015	FY 2016	Current Services Adjustments & FY 2017 Program Changes	FY 2017 Request
IAFIS fingerprint background checks	73,831,447	77,212,843	83,743,292	-	83,743,292 +
NCIC transactions	4,496,864,000	4,558,098,730	4,946,550,400	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
	1,968	$468,435	1,968	$468,435	2,076	$476,782	132	29,518	2,208	$506,300

TYPE/ STRATEGIC OBJECTIVE	PERFORMANCE	FY 2015	FY 2015	FY 2016 Current Rate	Current Services Adjustments & FY 2017 Program Changes	FY 2017 Request
Efficiency Measures	**IAFIS/NGI:** % of IAFIS/NGI routine fingerprint checks: Criminal: • Completed w/in 2 hours Civil: • Completed w/in 24 hours	95.00% 99.00%	98.0% 97%	95.00% 99.00%	- -	95.00% 99.00%
Performance Measure	**RISC Searches Response Time:** Average NGI response time of RISC rapid searches	<10 seconds	3.94 seconds	<10 seconds	-	<10 seconds
Performance Measure	**NCIC:** • System availability • Downtime in minutes	99.5% 2,268	99.8 1,287	99.5% 2,268	- -	99.5% 2,268
Performance Measure	**NICS:** % of NICS system availability	98. 0%	99.7%	98. 0%	-	98.0%

2. PERFORMANCE/RESOURCES TABLE						
Performance Measure	**NICS:** % of NICS checks with an Immediate Determination	90. 0%	90.4%	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	13 days	30 days	-	30 days
Performance Measure	Student-weeks of Instruction at the Hazardous Devices School (HDS)	1,764		2,200	-	2,200
Performance Measure	**N-DEx:** Percent of population covered by N-DEx via state and local law enforcement participation	70.84%	NA	70.84%	-	N/A
Performance Measure	**N-DEx:** Increase in the number of N-DEx system searches – cumulative total of 5 million for FY	NA	NA	5,000,000	-	5,000,000
Performance Measure	**N-DEx: [New Measure for FY 2015]** Annual percent increase of agencies submitting data to N-DEx PROPOSED TO BE DISCONTINUED IN FY 2016.	5%	6%	NA	-	NA
Performance Measure	**LEO:** Number of VCC new events boards open	831	1,222	848	-	848
Performance Measure	**LEO:** Number of identity or service providers on-boarded to the Law Enforcement Enterprise Portal (LEEP)	10	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.

* FY 2016 Projected is based on FY 2016 Spend Plan submission.

Performance Report and Performance Plan Targets		FY 2011	FY 2012	FY 2013	FY 2014	FY 2015		FY 2016	FY 2017
		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 Civil: • Completed w/in 24 hours	99. 32% 99. 80%	99. 30% 99. 80%	N/A N/A	98.00% N/A	95.00% 99.00%	98% 97%	95.00% 99.00%	95.00% 99.00%
Performance Measure	**RISC Searches Response Time:** Average NGI response time of RISC rapid searches	N/A	N/A	N/A	4.2 seconds	<10 seconds	3.94 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	NA NA NA NA	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. 40%	91.72%	91.64%	91.00%	90.00%	90.4%	90.00%	90.0%
Performance Measure	**NICS:** % of NICS system availability	N/A	99.93%	99.81%	99%	98%	99.7%	98.%	98%
Performance Measure	**NCIC:** • System availability • Downtime in minutes	99. 76% 1,273	99.75% 1,351	99.81% 1,000	99. 50% 1,440	99.5% 2,268	99.8% 1,287	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	25 days	18 days	18 days	30 days	13 days	30 days	30 days
Performance Measure	**N-DEx:** **Increase in the number of N-DEx system searches – cumulative total of 5 million for FY**	NA	NA	NA	NA	NA	NA	5,000,000	5,000,000
Performance Measure	**N-DEx:** Percent of population covered by N-DEx via state and local law enforcement participation MEASURE PROPOSED TO BE DISCONTINUED	35. 30%	50.00%	54%	68%	70.84%	NA	70.84%	NA
Performance Measure	**N-DEx:** Annual percent increase of agencies submitting data to N-DEx	N/A	N/A	N/A	N/A	5%	6%	15%	15%
Performance Measure	**LEO:** Number of VCC new events boards open	N/A	N/A	2,167	1,500	831	1,222	848	848
Performance	**LEO:** Number of identity or service providers	N/A	N/A	NA	15	10	10	10	10

Measure	on-boarded to the Law Enforcement Enterprise Portal (LEEP)								
Performance Measure	Student-weeks of Instruction at the Hazardous Devices School (HDS)	2,295	2,052	2,024	1,848	2,200	2,286	2,350	2,500

3. Performance, Resources, and Strategies

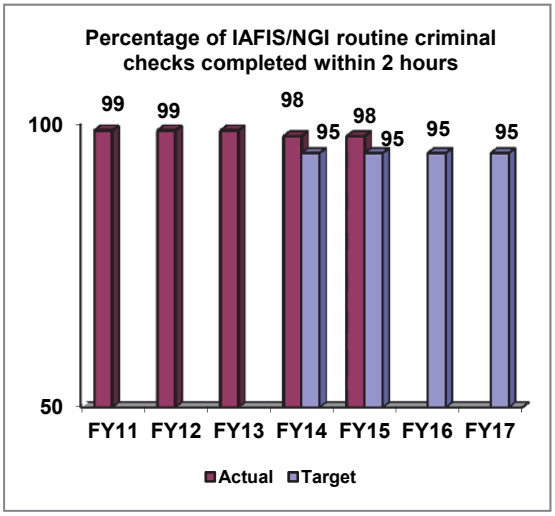
The Criminal Justice Services Decision Unit contributes to the Department of Justice's Strategic Goal 3, "Ensure the Fair and Efficient Administration of Justice." Within this goal, the resources specifically support Strategic Objective 3.6, "Promote and strengthen innovative strategies in the administration 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: Percentage of IAFIS/NGI routine criminal fingerprint checks completed within 2 hours.

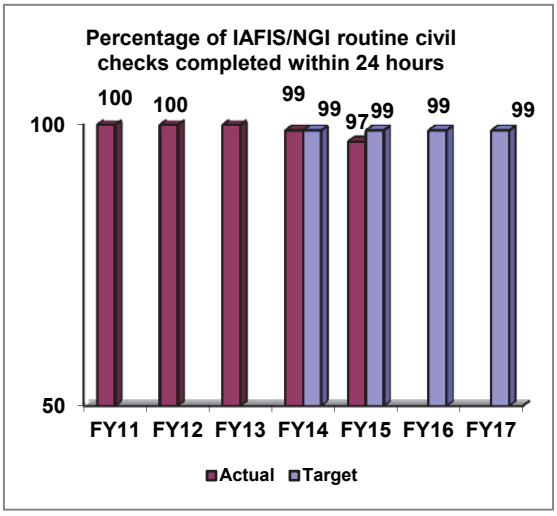
FY 2015 Actual: 98%
FY 2016 Target: *95%*
FY 2017 Target: *95%*



Discussion: 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: Percentage of IAFIS/NGI routine civil fingerprint checks completed within 24 hours.

FY 2015 Actual: 97%
FY 2016 Target: 99%
FY 2017 Target: 99%

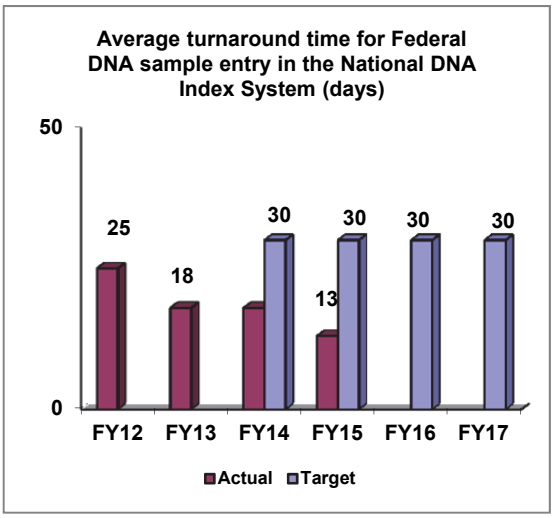


Discussion: The FY 2016 target is based on historical data. The FBI replaced all IAFIS segments by NGI in 2014. This reporting accounts for some improvements in response times which could be attributed to efficiencies gained by NGI's implementation of the new fingerprint matching segment of IAFIS. The 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.

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.



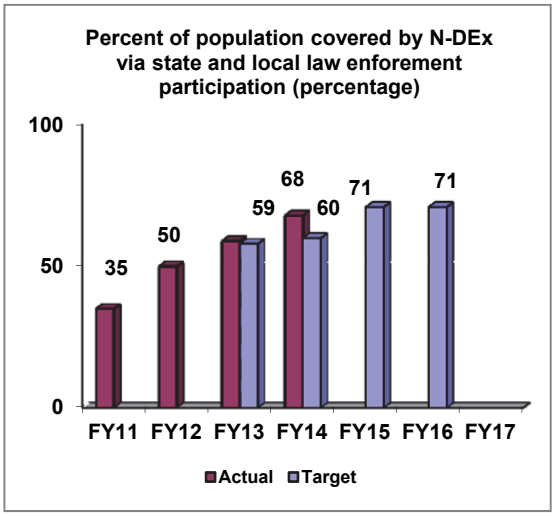
FY 2015 Actual: 13 days
FY 2016 Target: 30 days
FY 2017 Target: 30 days

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 investigations that are more effective. The objective is that the use of N-DEx 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

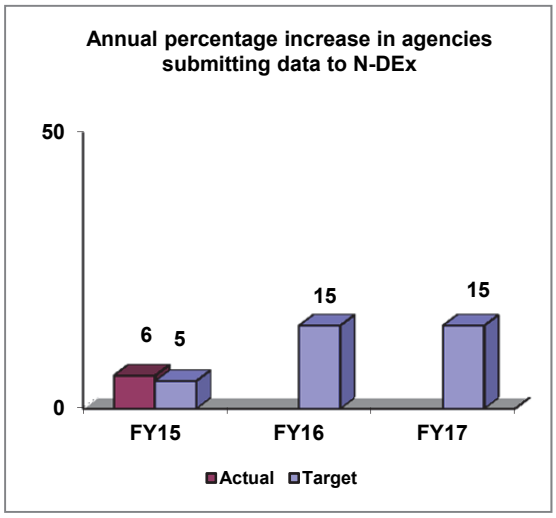


Discussion: The FBI proposes to discontinue this measure in favor of the measure "Annual percent increase of agencies submitting data to N-DEx."

***Performance Measure**:* Annual percentage increase of agencies submitting data to N-DEx

FY 2015 Actual: 6%
FY 2016 Target: 15%
FY 2017 Target: 15%

Discussion: This new measure is defined as the percent of all criminal justice agencies that have made some amount of law enforcement investigative information available through N-DEx. A 5% annual increase equates to 251 additional agencies submitting data to N-DEx.

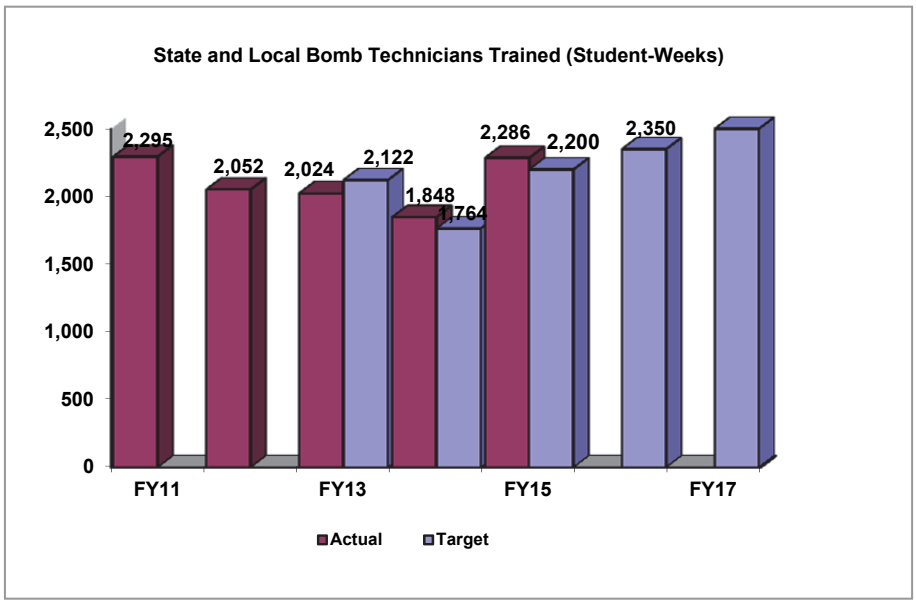


Hazardous Devices School (HDS)

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 2015 Actual: 2,286
FY 2016 Target: 2,350
FY 2017 Target: 2,500



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. Because of additional resources provided in FY 2015, the FBI expects a slight increase in FY 2016 and 2017 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.

V. Program Increases
Item Name: **Cyber**

Strategic Goal(s) & Objective(s): 1.4
Budget Decision Unit(s): All

Organizational Program: Cyber, Operational Technology

Program Increase: Positions … Agt … FTE … Dollars $85,138,000 (all non-personnel)

Description of Item

The FBI requests $85,138,000 (all non-personnel) in support of the FBI's cyber program. This initiative will support the FBI's responsibilities in defeating cyber intrusion threats through a unique combination of law enforcement and national security authorities.

The FBI's Next Generation Cyber (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 still protecting privacy, confidentiality, and civil liberties, the FBI worked to prioritize and align existing resources to strengthen its cyber capabilities. However, given the increasing complexity and proliferation of cyber crimes, the FBI requires additional resources to address this threat. This request builds on the FY 2016 enhancement.

Please refer to the classified addendum for details on this request.

Funding

Base Funding

FY 2015 Enacted				FY 2016 Enacted				FY 2017 Current Services			
Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)
1,621	807	1,447	$417,872	1,753	897	1,580	$520,049	1,753	897	1,580	$541,379

Non-Personnel Increase Summary

Non-Personnel Item	Unit	Quantity	FY 2017 Request ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
Contract – Services	n/a	n/a	$18,690	$…	$...
Equipment	n/a	n/a	7,376	…	…
Interagency Services	n/a	n/a	14,200	…	…
IT Hardware	n/a	n/a	23,775	…	…
IT Software	n/a	n/a	13,600	…	…
IT Maintenance	n/a	n/a	2,200	…	…
IT Supplies	n/a	n/a	216	…	…
Leases	n/a	n/a	625	…	…
Training	n/a	n/a	4,025	…	…
Travel	n/a	n/a	431	…	…
Total Non-Personnel			$85,138	$…	$...

Total Request for this Item

	Pos	Agt	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
Current Services	1,612	889	1,612	$279,008	$262,371	$541,379	$...	$...
Increases	…	…	…	…	85,138	85,138	…	…
Grand Total	1,931	1,050	1,772	$279,008	$347,509	$626,517	$...	$...

Item Name: **Foreign Intelligence/Insider Threat and Continuous Evaluation**

Strategic Goal(s) & Objective(s): 1.3
Budget Decision Unit(s): Counterterrorism/Counterintelligence

Organizational Program: Counterintelligence

Program Increase: Positions … Agt … FTE … Dollars $19,927,000 (all non-personnel)

Description of Item

The FBI requests $19,927,000 (all non-personnel) to address threats posed by foreign intelligence and insider threats.

Please refer to the Classified Addendum for additional details on this request. Included below is a description of the Continuous Evaluation (CE) portion of the request.

The enhancement request includes$1,700,000 in FY 2017 for technical efforts to acquire criminal activity data from the Criminal Justice Information Services (CJIS). The funds included are for architecture/engineering/system design, system development/modifications, system testing, hardware, and connectivity.

Justification

The CE Program is a federal government-wide mandate to continuously vet those with access to classified information within IC and for the Top Secret/Sensitive Compartmented Information populations across the Executive Branch of the Federal Government. The CE Program will leverage automated record checks and predefined thresholds to assist in determining an individual's eligibility for continued access to classified information. CE is only part of a larger clearance reform effort that aims to identify security risk information in a timelier manner for earlier intervention and mitigation. One of the critical components of this program is gaining access to the criminal records housed within the FBI's criminal justice information systems.

The FBI's Next Generation Identification (NGI) Rap Back program has been identified as the most effective mechanism to share criminal history information with the CE Program. The NGI Rap Back Service was deployed in September 2014, and was developed in response to a need for Non-Criminal Justice (NCJ) entities to receive notification of criminal activity on persons holding positions of trust. Enrollment into the NGI Rap Back provides continuous monitoring after the initial fingerprint-based background check. It provides several options for the subscriber to enroll persons holding positions of trust, to include Category or Person Based enrollments coupled with terms of Tier I (up to 2 years), Tier II (up to 5 years), and Tier III (Lifetime – referring to the period of time the individual holds the position of trust). The subscription consists of enrollment, maintenance and validation, subsequent criminal activity identification and notification, response generation, and billing. As designed and currently implemented, NGI Rap Back is a fee for service program that supports the local, state, tribal, and federal entities that request fingerprint-based criminal history information record checks.

Impact on Performance

ODNI is in the initial stages of developing their requirements for NCIC and NGI Rap Back data. This enhancement request will assist in providing initial/partial connectivity to support ODNI's participation in a CE program. The FBI still requires greater clarity on the scope of the CE requirements. This enhancement request does not address FBI's costs for providing ongoing CE services.

Funding

Base Funding

FY 2015 Enacted				FY 2016 Enacted				FY 2017 Current Services			
Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)
31	17	28	$25,802	31	17	28	$25,802	31	17	28	$25,802

Non-Personnel Increase Cost Summary

Non-Personnel Item	Unit	Quantity	FY 2017 Request ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
Contract Services	n/a	n/a	$2,500	$…	$…
Travel	n/a	n/a	650	…	…
IT Hardware	n/a	n/a	1,577	…	…
IT Software	n/a	n/a	1,800	…	…
Supplies	n/a	n/a	585	…	…
Case Funds	n/a	n/a	1,900	…	…
Contractors	214	43	9,215	…	…
Contracts (CE)	n/a	n/a	1,700	…	…
Total Non-Personnel			$19,927	$…	$…

Total Request for this Item

	Pos	Agt	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
Current Services	31	17	28	$6,278	$19,524	$25,802	$…	$…
Increase	…	…	…	…	19,927	19,927	…	…
Grand Total	31	17	28	$6,278	$39,451	$45,729	$…	$…

Item Name: **Going Dark**

Strategic Goal(s) & Objective(s): 1.1, 1.2, 1.3
Budget Decision Unit(s): All

Organizational Program: Operational Technology

Program Increase: Positions … Agt … FTE … Dollars $38,327,000 (all non-personnel)

Description of Item

The FBI requests $38,327,000 (all non-personnel) to counter the threat of Going Dark, which includes the inability to access data because of challenges related to encryption, mobility, anonymization, over-the-top[4] applications, and much more.

Please refer to the Classified Addendum for additional details on this request.

[4] An over-the-top (OTT) application is any app or service that provides a product over the Internet and bypasses traditional distribution. Services that come over the top are most typically related to media and communication and are generally, if not always, lower in cost than the traditional method of delivery.

Funding

Base Funding

FY 2015 Enacted				FY 2016 Enacted				FY 2017 Current Services			
Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)
39	11	39	31,011	39	11	39	31,011	39	11	39	31,011

Non-Personnel Increase Summary

Non-Personnel Item	Unit	Quantity	FY 2017 Request ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
IT Hardware	n/a	1	$17,875	($14,167)	…
Supplies	n/a	1	112	(112)	…
Contract – Services	n/a	1	10,312	…	…
IT Hardware Maintenance	n/a	1	2,219	…	…
IT Hardware/ Software	n/a	1	6,084	…	…
IT Facility Costs	n/a	1	707	…	…
IT Maintenance	n/a	1	18	…	…
Leasing Circuits	n/a		1,000	…	…
Total Non-Personnel			$38,327	($14,390)	…

(U) Total Request for this Item

	Pos	Agt	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
Current Services	39	11	39	$6,409	$24,602	$31,011	…	…
Increases	…	…	…	…	38,327	38,327	(14,390)	…
Grand Total	39	11	39	$6,409	$62,929	$69,338	($14,390)	…

Item Name: **Transnational Organized Crime (TOC)**

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

Organizational Program: Terrorist Screening, International Operations

Program Increase: Positions … Agt … FTE … Dollars $6,779,000 (all non-personnel)

Description of Item

The FBI request includes $6,330,000 (all non-personnel) for the Terrorist Screening Center (TSC) to augment its existing operations and systems to create a consolidated Transnational Organized Crime (TOC) watchlist. In addition, the request includes $449,000, the details of which are included in the Classified Addendum.

Justification

The request will increase the FBI's watchlisting, encounter management, and information sharing effort at the TSC to execute Transnational Organized Crime Watchlisting and Screening.

In FY 2014, the White House National Security Council Transborder Security Directorate Interagency Policy Committee commissioned the TSC to conduct a U.S. Government pilot to demonstrate value associated with watchlisting and screening TOC Actors. TOC Actors are defined as individuals who are reasonably suspected or known to be engaged in TOC or to be knowingly aiding, abetting, or conspiring with others engaged in TOC. On August 6, 2015, the Attorney General signed Order No. 3548-2015, which granted the TSC the authority to manage, disseminate, perform identity verification, and encounter management functions regarding TOC Actors.

In FY 2016, the TSC will transition to a broader national security screening mission for a whole-of-government approach. The TSC will augment existing information technology (IT) systems and operations to support a consolidated watchlisting effort to enable effective U.S. Government screening of TOC Actors. The addition of new watchlisting populations will increase the size of the watchlist, resulting in increased workload within the TSC and expanded coordination with existing and new interagency partners. This request assumes the FBI is solely responsible for the interagency IT capability.

During FY 2016, the TSC will conduct a TOC pilot that will include 8,000 nominations to the TOC watchlist from FBI and DEA. The FBI must integrate and expand the TSC IT systems to accomodate the full execution of TOC Watchlisting and Screening. The FBI estimates that $3,046,280 is required for short-term contractor support for the TSC IT Systems. Key IT development areas include:

- **IT Infrastructure-** Develop new network-to-network and system-to-system engineering infrastructure to support network communication and system compatibility to support new TOC partners.
- **Semi-Automated Ingest-** Develop a semi-automated TOC Actor ingest capability akin to what currently exists for Known or Suspected Terrorists (KST).
- **Biometrics Ingest/Housing Capability-** Develop biometric (e.g., fingerprint, iris) ingest, storage, and export capabilities that are compatible with screener-systems to support operational TOC Watchlisting and Screening requirements.

- **Scaling of Database -** Provide the necessary data storage and develop the IT infrastructure to accommodate full operational TOC Actor Watchlisting and Screening.

TOC poses a significant and growing threat to national and international security with implications for public safety, public health, democratic institutions, and economic stability across the globe. On July 19, 2011, the President issued the "Strategy to Combat Transnational Organized Crime" with the goal to "build, balance, and integrate the tools of American power to combat transnational organized crime and related threats to national security." Currently, U.S. Government efforts to screen against persons associated with TOC are not consolidated and coordinated; no single agency supports TOC screening across all U.S. Government screening systems. Application of the terrorism watchlisting and screening enterprise leverages existing infrastructure in an efficient and cost-effective manner, adding a new tool to the U.S. Government's counter-TOC efforts. The U.S. Government does not currently have a central, TS/SCI repository of TOC Actor derogatory and source information. Therefore, the FBI requires additional IT augmentation to provide the TSC the ability to store the derogatory information of TOC Actors on behalf of the community whose supporting derogatory information is classified at the SECRET level or above.

TOC Mexico (including the Sinaloa drug cartel), identified as a high FBI National Threat Priority for FY 2015, will be a population included in the TSC's TOC watchlisting pilot. The Sinaloa drug cartel serves as just one of many examples of the impact of TOC activity on the U.S. Sinaloa's annual revenues are estimated at $3 billion, equivalent to several large U.S. corporations. The Sinaloa organization is transnational, with an observed presence in over 100 U.S. cities and at least 47 countries. Other significant Transnational Criminal Organizations (TCOs) exhibit a similar span of volume and threat.

The TSC's current operations and infrastructure are ideally suited to lead the U.S. Government's TOC watchlisting efforts. The FBI established the TSC in 2003 to provide the U.S. Government and select international partners with a consolidated and comprehensive solution for known or suspected terrorist watchlisting, identity resolution, and information and intelligence sharing. The TSC is a multi-agency organization staffed with assignees and detailees from the Departments of Homeland Security, Justice, and State; the Office of the Director of National Intelligence; and other federal departments and agencies that the TSC supports. Over the past eleven years, the TSC's Terrorist Screening Database ("the Terrorist Watchlist") has grown to include over 879,000 watchlisted persons and has been successfully used by screening agencies to positively match over 230,000 individuals to persons on the watchlist.

The Terrorist Screening Database is populated with identity information through a formal nomination process. The TSC receives international terrorism nominations from the U.S. IC, through the NCTC, and receives domestic terrorism nominations directly from the FBI. Identity information contained within the Terrorist Screening Database is provided to over 70 domestic and international law enforcement, intelligence, and regulatory agencies to support screening activities. The Terrorist Screening Database is an established data platform that the FBI can optimally use for the watchlisting of TOC Actors.

To support screeners, the TSC operates a 24/7/365 operations center that conducts real-time identity resolution, coordinates operational responses to positive encounters with watchlisted persons, and assists the FBI and partner agencies with critical operational support services. In FY 2015, the TSC processed 99,007 encounters with potentially watchlisted persons. Encounter management at the TSC is an established screening support system ideal for use during the screening of TOC Actors. The TSC will expand this screening support to include 24/7/365 operations services for TOC screeners.

In addition to the watchlisting and screening capabilities at the TSC, the TOC initiative will likely leverage the TSC's information sharing network. The TSC disseminates encounter notifications to the appropriate government entities if an encounter with a potentially watchlisted person is deemed to be a match to a watchlisted person's identity. The TSC coordinates with hundreds of individual organizations every month, both domestically and internationally, to ensure the FBI properly disseminates critical KST encounter information. For example, the TSC will set investigative leads when necessary which inform FBI field offices of previously unknown watchlisted persons that were encountered in their area of responsibility. In FY 2015, the TSC set 224 of these investigative leads.

Watchlisting

The TSC will provide the U.S. Government's watchlisting function for TOC populations by building upon its successful operational and IT framework for watchlisting KSTs. Additionally, the TSC will expand its redress program to resolve concerns from individuals experiencing travel delays or difficulties that may be related to watchlisting. The process of watchlisting incorporates a multi-layered, enterprise approach that allows the TSC to share appropriate information from investigative and intelligence agencies through a quality control process. The TSC then shares information to law enforcement and homeland security components conducting screening operations. The TSC will serve as the organization responsible for consolidating, maintaining, and sharing watchlist information on TOC populations.

As Pilot phase nominators (FBI and DEA) institutionalize TOC Watchlisting and Screening by implementing policies that will set forth circumstances, criteria, and processes for ongoing TOC Actor nominations, a significant increase in TSC watchlisting operations is anticipated. In addition, the FBI expects that ICE, CBP, CIA, DOD, NSA, ATF, and Treasury will submit TOC Watchlisting Nominations. To mitigate adverse impacts on counterterrorism watchlisting activities and minimize TOC Actor daily residuals, the FBI estimates that it requires $1,956,290 for contractor support to augment watchlisting capabilities to include TOC.

Encounter Management

The TSC will provide 24/7/365 operations support to screening agencies that will potentially encounter watchlisted TOC Actors. This operation support will include providing real-time identity resolution, coordinating operational responses to positive encounters, and providing specialized operational support services to partner agencies. Since 2003, the TSC has been providing 24/7/365 operations support services to agencies screening known or suspected terrorists.

Persons watchlisted in the Terrorist Screening Database are encountered through a variety of screening activities, including, but not limited to: visa application, border crossing, pre-flight manifest checks, and law enforcement encounters through the National Criminal Information Center. The anticipated increase in the number of watchlisted TOC Actors will lead to at least a commensurate increase in encounters requiring TSC provided identity resolution and encounter management support. A sizable portion of the TOC Actor population could be geographically based in the Americas and, based on their illicit activities (e.g., drug, money, weapons, and human trafficking), could be frequent travelers. This is likely to result in a greater watchlist-to-encounter ratio than observed in the KST population, resulting in an increased total level of effort per TOC Actor than historically observed for KSTs. For FY2014, there was an 8/1 watchlist-to-encounter KST ratio. To mitigate adverse impacts on counterterrorism encounter management activities and provide adequate coverage for TOC Actor encounters, is the FBI estimates that it requires $663,715 for contractor support.

The IT development will include: capability to provide real-time encounter "alerts" to external stakeholders and updates to existing data structure to support TOC record encounters. Upon a TOC Actor encounter, the encountering agency will contact the TSC to verify the TOC Actor's identity. Once confirmed, the TSC will immediately contact the applicable Case Agent, ask for special instructions, and convey those instructions to the encountering agency. Once the encounter is over, the TSC will send an encounter summary and details to the Case Agent, as well as post it to various Task Force web forums. The Bureau will also expand the TSC's operational response framework to support additional TOC populations and additional reporting agencies.

Impact on Performance

Absent the requested funding, the TSC will continue to develop, albeit at a reduced pace, the capability to screen TOC Actors and information. The intent of the requested increase for TOC Watchlisting and Screening is to provide a whole-of-government solution to the problems of intermittent and incomplete TOC Actor information sharing across the government and missed interdiction, intelligence gathering, and investigative opportunities.

Funding

Base Funding

FY 2015 Enacted				FY 2016 Enacted				FY 2017 Current Services			
Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)
184	14	181	$83,749	184	14	181	$83,749	184	14	181	$83,749

Non-Personnel Increase Cost Summary

Non-Personnel Item	Unit	Quantity	FY 2017 Request ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
Travel	n/a	n/a	$88	$…	$…
Training	n/a	n/a	$70	$…	$…
Other	n/a	n/a	$291	$…	$…
IT Contractor Support	$249	25	$6,330	($4,350)	$…
Total Non-Personnel			$6,779	($4,350)	$…

Total Request for this Item

	Pos	Agt	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
Current Services	184	14	181	$21,209	$62,540	$83,749	$…	$…
Increase	…	…	…	…	6,779	6,779	(4,350)	…
Grand Total	184	14	181	$21,209	$69,319	$90,528	($4,350)	$…

Item Name: **Intelligence Community Information Technology Enterprise (IC ITE)**

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

Organizational Program: Information Technology

Program Increase: Positions … Agt … FTE… Dollars $26,997,000 (all non-personnel)

Description of Item

The FBI requests $26,997,000 (all non-personnel) for its IT infrastructure to increase the FBI's collaboration with the IC by leveraging the IC ITE technology and services.

Justification

The IC ITE effort is a multi-year investment and 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 at the top secret level 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 Services (NRES)
- IC Security Coordination Center (SCC),
- Geospatial Intelligence (GEOINT) Services

The FBI's 2017 IC ITE request includes:

IT Consulting ($3,000,000)

- $1,700,000 will support IC ITE adoption activities by providing contract engineering resources to ensure the following:

  1) IC Audit is fully enabled and supported
  2) Engineer ingest for all IC ITE data sources and ensure data is maintained
  3) Engineer the integration of Sentry into the Desktop Environment.

- $1,300,000 will provide contract support to the IC ITE Program Management Office (PMO) implementation and integration activities, including: intelligence domain analyst, system engineering, and program management advisory support.

Training ($297,000) to support DTE migration. The investment will support training for 10 classes with approximately 200 FBI personnel using IC ITE's Commercial Cloud Services (C2S).

DTE Migration ($23,700,000). The investment will provide funding for DTE migration to occur in FY 2017 (4,560 DTE installations estimated at $5,200 per installation). This request builds on the FY 2016 enhancement.

Impact on Performance

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 increased security.

Collaboration with other IC members is critical. The coordination between agencies involved is 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 an IT infrastructure that provides controlled access and tools to facilitate better collaboration. This includes 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.

Without these investments, the FBI will not be able to fully 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.

Funding

Base Funding

FY 2015 Enacted				FY 2016 Enacted				FY 2017 Current Services			
Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)
3	…	3	$1,455	3	…	3	$10,340	3	…	3	$10,340

Non-Personnel Increase Cost Summary

Non-Personnel Item	Unit	Quantity	FY 2017 Request ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
Contract – IT Consulting	n/a	n/a	$26,700	$...	$...
Training	n/a	n/a	297	...	...
Total Non-Personnel	n/a	n/a	$26,997	$...	$...

Total Request for this Item

	Pos	Agt	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2018 Net Annualization (change from 2017) ($000)
Current Services	3	…	3	$640	$9,700	$10,340	$...
Increases	…	…	…	…	26,997	26,997	…
Grand Total	3	…	3	$640	$36,967	$37,337	$...

Item Name: **Physical Surveillance**

Strategic Goal(s) & Objective(s): 1.1, 1.2, 1.4, 2.3
Budget Decision Unit(s): Counterterrorism/Counterintelligence

Organizational Program(s): Critical Incident Response

Program Increase: Positions 36 Agt 18 FTE 18 Dollars $8,242,000

Description of Item

The FBI requests 36 positions (18 agents) and $8,242,000 to improve the FBI's ability to conduct surveillance on the highest priority targets. This request builds on the increase funded with the FY 2016 Appropriation.

Please refer to the Classified Addendum for additional details on this request.

Item Name: **Biometrics Technology Center (BTC) Operations and Maintenance (O&M)**

Strategic Goal(s) & Objective(s): 1.1, 2.1, 2.2
Budget Decision Unit(s): Criminal Justice Services

Organizational Program: Criminal Justice Information Services (CJIS)

Program Increase: Positions ... Agt … FTE … Dollars $7,375,000 (all non-personnel)

Description of Item

The FBI requests $7,375,000 for the operations and maintenance (O&M) of the new Biometrics Technology Center (BTC) in Clarksburg, West Virginia. The BTC is a collaborative effort between the FBI and the Department of Defense (DoD) and will serve as the center for biometric research and development. The BTC will house the Biometric Center of Excellence, which coordinates biometrics research and development efforts for the FBI. The BTC will also serve as an alternate Continuity of Operations Plan site for approximately 65 relocated FBIHQ personnel. Additionally, the BTC will house the DoD Biometrics Fusion Center, which will be managed and funded by the DoD. The BTC will provide 300,000 square feet for the FBI and 60,000 square feet for the DoD to house approximately 2,000 personnel.

The $7,375,000 requested for BTC O&M will fund facility O&M and IT O&M:

Facility O&M - $4,442,000
The BTC O&M cost includes all aspects of operating and maintaining the physical facility: facility supplies, equipment and services, custodial/grounds maintenance, central plant equipment maintenance, building modifications/repairs, preventative maintenance and inspections, utility costs, and contracted service providers. In addition, CJIS User Fees will support $2,620,000 of the total requirement and the DoD will pay an additional $1,588,000 for its portion of the BTC facility O&M.

IT O&M - $2,933,000
The BTC building requires communications and network infrastructure, including firewalls, intrusion detection systems, servers, and storage. In addition, there are new labs and training spaces that require communications and network infrastructure. This portion of the request includes the cost of maintaining communications and equipment, including hardware/software maintenance and five-year technical refreshment costs for FBI workstations and network equipment. These requirements are specific to FBI personnel, and cannot be passed on to the DoD. CJIS User Fees will support $1,729,942 of the total requirement.

Justification

The construction of the main facility and central plant expansion concluded in the Fall of 2015. The complete outfitting of the facility and move in of personnel will conclude in by the end of Calendar Year 2016. Further, this O&M funding will enable the BTC to prevent system or work stoppage and/or delays. BTC O&M funding is required to support the BTC facilities and IT) requirements. CJIS User Fees will support $4,349,942 of the BTC O&M requirement, and DoD will pay an additional $1,588,000 for its portion of the O&M. This request for $7,375,000 is to support the remaining requirement of BTC O&M.

Impact on Performance

If the requested O&M funding is not received for the BTC building the maintenance on both CJIS facilities will be severely impacted, leading to shorter useful building life, potential life safety issues, and degraded working conditions. In addition, if the BTC is not maintained properly, or repairs are not made in a timely fashion, the DoD may seek an alternative location, which would defeat the collaboration gained by collocating the FBI and the DoD biometric efforts.

Funding

Base Funding

FY 2015 Enacted				FY 2016 Enacted				FY 2017 Current Services			
Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)
…	…	…	$…	…	…	…	$…	…	…	…	$…

Non-Personnel Increase Cost Summary

Non-Personnel Item	Unit	Quantity	FY 2017 Request ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
O&M	n/a	n/a	$7,375	$…	$…
Total Non-Personnel			$7,375	$…	$…

Total Request for this Item

	Pos	Agt	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
Current Services	…	…	…	$…	$…	$…	$…	$…
Increases	…	…	…	…	7,375	7,375	…	…
Grand Total	…	…	…	$…	$7,375	$7,375	$…	$…

Item Name: **National Instant Criminal Background Check System (NICS)**

Strategic Goal(s) & Objective(s): 3
Budget Decision Unit(s): Criminal Justice Services

Organizational Program: Criminal Justice Information Services

Program Increase: Positions… Agt … FTE … Dollars $35,000,000 ($20,000,000 non-personnel)

Description of Item

The FBI requests $35 million to support the statutorily mandated firearm background checks conducted by the National Instant Criminal Background Check System (NICS) Section within the mandated three day timeframe. Of the $35 million, $15 million will sustain the 75 professional support positions funded in FY 2016. The remaining $20 million (non-personnel) will secure an estimated 160 contractors that would provide direct support processing firearm background checks and provide for the implementation of recommendations to improve NICS personnel recruitment and retention. These recommendations will include, among other, pay scale adjustments.

Justification

The NICS was established in 1993 by mandate of the Brady Handgun Violence Prevention Act (Brady Act) of 1993, and implemented in 1998. Since implementation, CJIS has conducted approximately 225 million NICS background checks. An average annual increase of 6.88 percent has taken place for the past five years. Firearm background checks have increased from approximately 6,569,000 in FY 2011, to nearly 8,536,000 in FY 2015. The following table reflects the projected increase in transaction volume over the previous fiscal years. However, the number of NICS checks may increase beyond this estimate due to the Bureau of Alcohol, Tobacco, Firearms, and Explosives' (ATF) guidance on Federal Firearms Licensees issued in support of the President's Executive actions.

FY	Projected Increase of Transaction Volume
2016	587,253
2017	627,656

To address the projected increases, while pursuing quality control, the NICS Section intends to:

- Continue to honor the regulation and achieve due diligence
- Aim to improve the rate of determination for Delayed/Open checks lowering the processing rate of 2.0 per hour, adjusting processing times on Transfer Process and E-Check to improve quality
- Reduce service levels from 90 percent to 80 percent to ensure quality is provided to all incoming calls.

The NICS Section has determined that inadequate staffing, paired with the current volume of background checks, deprives the employees the time needed to perform at a desirable level of accuracy. With additional staffing, the NICS Section can conduct thorough examinations and follow-up research to make final determinations and closeout transactions while ensuring it maintains quality.

The FBI currently employs 511 NICS staff members, of which it designates 314 as the NICS background check research and analysis staff. The NICS staff is working at capacity and must be augmented with additional personnel to maintain production. (See chart below.) For example, in the

month of December 2015, the FBI redirected over 200 personnel assigned to the NICS Section to concentrate exclusively on processing background checks. This redirection of the NICS Section staff resulted in placing a hold on the handling of appeals, addressing Congressional correspondence, and performing other crucial tasks. In addition, the FBI mandated 44 other employees, not currently assigned to the NICS Section to provide surge support. Even with the surge support, the requirement for overtime on some weeks exceeded 2,000 hours. Furthermore, with the redirected and surged employees and the use of overtime, many transactions were carried into the fourth day and the gun checks were not completed within the Brady Bill mandated timeframe. The Brady Bill requires that a final determination be made within three business days; if no determination is made, the Federal Firearms Licensee can legally transfer the firearm to the purchaser, who potentially may be an individual prohibited from purchasing firearms.

Year	NICS Transactions (handled by FBI staff)	Delay Queue Transactions	FBI NICS Staff at beginning of FY	Delay Queue Transactions per NICS Staff	Percentage of Delay Queue Denied	Delay Queue - Denied Transactions
2003	4,398,638	473,450	542	874	0.97%	4,592
2004	4,632,699	381,677	521	733	0.97%	3,702
2005	4,772,152	414,428	521	795	0.94%	3,896
2006	5,299,618	457,063	526	869	0.94%	4,296
2007	5,188,044	424,005	500	848	0.88%	3,731
2008	5,382,109	448,718	499	899	0.80%	3,590
2009	6,405,958	526,161	498	1,057	0.70%	3,683
2010	5,910,965	532,049	498	1,068	0.78%	4,150
2011	6,568,831	603,765	498	1,212	0.75%	4,528
2012	7,810,000	693,476	501	1,384	0.67%	4,646
2013	9,960,107	876,429	511	1,715	0.59%	5,171
2014	8,126,421	760,727	448	1,698	0.69%	5,249
2015	8,535,654	845,561	545	1,551	0.74%	6,257
2016	9,591,280**	887,495**	511*	1,737**	TBD	TBD

*Does not include the 75 new professional support positions funded in FY 2016.
**Projected Volume

While the New NICS IT system is currently under development, several efficiencies are anticipated with the initial operating capabilities such as 24/7/365 system availability, improved name matching resulting in fewer delays and decreased wait time, and a new scoring algorithm to allow for automatic denials. To address the immediate need for more personnel to support the increased work volume and quality concerns, the FBI requests $20 million to hire approximately 160 contractor staff to provide research and analysis assistance for the FBI's NICS staff.

Impact on Performance

At current levels, FBI staff will be unable to consistently provide timely and accurate determinations of individuals' eligibility to possess firearms and/or explosives in accordance with federal law. This increases the likelihood that gun and explosives dealers could sell firearms and/or explosives to prohibited persons. Sales to prohibited persons not only threaten public safety and national security, but also create increased workload for the Bureau of Alcohol, Tobacco, Firearms and Explosives, the

Federal Agency tasked with retrieving firearms from prohibited persons who are in possession of a firearm due to delays in a NICS final determination. Any firearm retrieval is a high risk action that could result in the death or injury of law enforcement officers. Moreover, the continued growth in the number of background checks requested is causing additional backlogs in responding to appeals, conducting explosives checks, conducting Nuclear Regulatory Checks, resolving Immigration and Customs Enforcement discrepancies and submitting NICS Index updates.

With the additional contractor support, the FBI will be able to conduct quality firearm background checks and explosives checks within mandated deadlines.

To ensure that an adequate cadre of well-trained NICS examiners are available, the FBI will begin implementation of recommendations to improve the recruitment and retention of personnel. The FBI intends to conduct targeted recruitment efforts towards family and friends of current CJIS employees as well as pursue students attending local colleges and universities. In an effort to retain the workforce, the FBI will explore the possibility for retention incentives like student loan repayment and tuition reimbursement.

Funding

Base Funding

FY 2015 Enacted				FY 2016 Enacted				FY 2017 Current Services			
Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)
593	…	580	$87,477	668	…	618	$94,077	668	…	655	$86,081

Personnel Increase Cost Summary

Type of Position	Modular Cost per Position ($000)	Number of Positions Requested	FY 2017 Request ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
Professional Support	$...	…	$15,000	$...	$...
Total Personnel	$...	…	$15,000	$...	$...

Non-Personnel Increase Cost Summary

Non-Personnel Item	Unit	Quantity	FY 2017 Request ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
Contractor Support	n/a	n/a	$20,000	$…	$…
Total Non-Personnel			$20,000	$…	$…

Total Request for this Item

	Pos	Agt	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
Current Services	668	…	655	$56,775	$29,306	$86,081	$…	$…
Increases	…	…	…	15,000	20,000	35,000	…	…
Grand Total	668	…	655	$71,775	$49,306	$121,081	$…	$…

VI. Program Offsets by Item
Item Name: **Personnel Offset**

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

Organizational Program: All

Program Decrease: Positions (380) Agt (200) FTE (380) Dollars ($57,000,000)

Description of Item

The FBI's FY 2017 budget reflects a reduction of $57 million from personnel funding. This reduction, which is the equivalent of 380 lower-priority positions, will be achieved by not hiring to funded, yet unfilled current vacancies and vacancies that occur due to attrition.

Justification

The FBI does not require the funding to support these unfilled positions and they should be eliminated.

Impact on Performance

This reduction will permanently eliminate 380 lower-priority positions.

Funding

Base Funding

FY 2016 Enacted				FY 2017 Current Services			
Pos	Agt	FTE	($000)	Pos	Agt	FTE	($000)
35,138	13,074	33,372	$5,137,539	35,138	13,074	33,372	$5,209,784

Funding Offset Summary

Item	Unit Cost	Quantity	FY 2017 Request ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
Personnel	n/a	n/a	($57,000)	$ …	$ …
Total Personnel			($57,000)	$ …	$ …

Total Offset for this Item

	Pos	Agt	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
Current Services	35,138	13,074	33,372	$5,209,784	$...	$5,209,784	$...	$ …
Decreases	(380)	(200)	(380)	(57,000)	…	(57,000)	…	…
Grand Total	34,758	12,874	32,992	$5,152,784	$...	$5,152,784	$...	$ …

Item Name: **Base Adjustment**

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

Organizational Program: All

Program Decrease: Positions (46) Agt (10) FTE (23) Dollars ($73,646,000)

Description of Item

The FBI's FY 2017 budget reflects a reduction of $73,646,000.

Justification

The FY 2016 Omnibus Appropriations Act provided $74 million for one-time expenditures, including investments at the Terrorist Explosive Device Analytical Center (TEDAC) and the Hazardous Devices School (HDS). This funding is non-recurred in FY 2017.

Impact on Performance

As one-time expenditures, there will be no impact on performance as a result of non-recurring this funding in FY 2017.

Funding

Base Funding

FY 2015 Enacted				FY 2016 Enacted				FY 2017 Current Services			
Pos	Agt	FTE	($000)	Pos	Agt	FTE	($000)	Pos	Agt	FTE	($000)
…	…	…	$...	46	10	23	$73,646	46	10	23	$73,646

Funding Offset Summary

Item	Personnel ($000)	Non-Personnel ($000)	FY 2017 Request ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
Program Non-Recurs	($17,110)	($56,536)	($73,646)	$ …	$ …
Total Offset	($17,110)	($56,536)	($73,646)	$ …	$ …

Total Offset for this Item

	Pos	Agt	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
Current Services	46	10	23	$17,110	$56,536	$73,646	$...	$ …
Decreases	(46)	(10)	(23)	(17,110)	(56,536)	(73,646)	…	…
Grand Total	…	…	…	$...	$...	$...	$...	$ …

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.

Recent construction projects funded through this account include the Terrorist Explosive Device Analytical Center (TEDAC) and the Hazardous Devices School (HDS), both of which are located in Huntsville, AL. The FY 2016 Omnibus Appropriations Act included initial funding for the consolidated FBI Headquarters (FBI HQ) project.

The FY 2017 request includes a total of $783.5 million for Construction, including a permanent program reduction of $16.5 million for the Secure Work Environment (SWE) Program. The requested funding will support the new FBI HQ ($646 million), the DOJ Data Center Transformation Initiative ($85 million), and the SWE Program ($50.5 million), as well as renovations at the FBI Academy in Quantico, VA ($2 million).

In addition to the FBI's FY 2017 request, the General Services Administration's (GSA) FY 2017 budget request includes $759 million in the Federal Building Fund for the new FBI HQ, for a total of $1.4 billion for the project. The department also proposes to make available to the FBI up to $315 million from the Working Capital Fund (WCF) for the HQ project.

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] *Federally*-owned buildings; [and] preliminary planning and design of projects; [$308,982,000] *and operation and maintenance of secure work environment facilities and secure networking capabilities; $783,482,000,* to remain available until expended, *of which $85,000,000 shall be derived by transfer from unobligated balances identified by Treasury Appropriation Fund Symbol 15X0200, and such funds shall be merged with this account: Provided further, That no amounts may be transferred 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: Provided further, That $646,000,000 shall be for the construction of the new Federal Bureau of Investigation consolidated headquarters facility in the National Capital Region.*

Analysis of Appropriations Language

The changes proposed for FY 2017 include:

- Re-inserting language pertaining to the Secure Work Environment (SWE) that was not included in the FY 2016 Omnibus Appropriations Act
- The direction to transfer $85 million from unobligated Salaries and Expenses (S&E) balances into this account
- Language regarding the new FBI consolidated headquarters

General Provision, Section 220
(Related to FBI)

Sec. 220 In addition to any other transfer authority available to the Department of Justice, for fiscal years 2017 through 2022, unobligated balances available in the Department of Justice Working Capital Fund pursuant to title I of Public Law 102–140 (105 Stat. 784; 28 U.S.C. 527 note) may be transferred to the "Federal Bureau of Investigation, Construction" account, to remain available until expended for the construction of the new Federal Bureau of Investigation headquarters in the National Capital Region: Provided, That the cumulative total amount of funds transferred from the Working Capital Fund from fiscal year 2017 through 2022 pursuant to this section shall not exceed $315,000,000: Provided further, That transfers pursuant to this section shall not count against any ceiling on the use of unobligated balances transferred to the capital account of the Working Capital Fund in this or any other Act in any such fiscal year.

Analysis of Appropriations Language

The new General Provision would make available up to $315 million for the construction of the new FBI HQ project if needed.

Program Increases
Item Name: **New FBI Headquarters (HQ)**

Strategic Goal(s) & Objective(s): All
Budget Decision Unit(s): N/A

Organizational Program: Facilities and Logistics Services

Program Increase: Positions … Agt … FTE … Dollars $646,000,000 (all non-personnel)

Description of Item

The FBI requests $646,000,000 to support the full consolidation of the FBI HQ operations in a new, modern, and secure facility that will bring together all of the existing disparate headquarters locations and functions. This funding will be combined with $759 million in the General Services Administration's (GSA) Federal Building Fund (FBF) for a total FY 2017 request of $1.4 billion for the project.

Justification

The current FBI HQ is obsolete, inefficient, costly to maintain, and would be prohibitively expensive to modernize. Multiple satellite offices are located at leased locations throughout the National Capital Region. The new facility will promote information sharing by exploiting synergies previously stovepiped in the FBI. Unifying the FBI HQ personnel into a modern facility will allow it to better address its complex national security and crime prevention work.

The FY 2016 Omnibus provided $180 million in one-time funding for the new construction, and allows the FBI to use up to $135 million of prior year balances for design and preconstruction activities. In addition to the FBI and GSA requests, language is included that would allow for the use of up to $315 million from the Department's Working Capital Fund for the FBI headquarters project.

Impact on Performance

Without this funding, there will not be adequate funding for the new FBI headquarters.

Funding

Base Funding

FY 2015 Enacted				FY 2016 Enacted				FY 2017 Current Services			
Pos	Agt	FTE	($000)	Pos	Agt	FTE	($000)	Pos	Agt	FTE	($000)
…	…	…	$...	…	…	…	$180,000*	…	…	…	$...

* While the $180 million is non-recurred in FY 2017, Construction funding is available until expended.

Non-Personnel Increase Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2017 Request ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
New FBI HQ	n/a	n/a	$646,000	$ …	$ …
Total Non-Personnel			$646,000	$ …	$ …

Total Request for this Item

	Pos	Agt	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
Current Services	…	…	…	$...	$...	$...	$...	$ …
Increase	…	…	…	…	646,000	646,000	…	…
Grand Total	…	…	…	$...	$646,000	$646,000	$...	$ …

Item Name: **DOJ Data Center Transformation Initiative**

Strategic Goal(s) & Objective(s): All
Budget Decision Unit(s): N/A

Organizational Program: Facilities and Logistics Services

Program Increase: Positions … Agt … FTE … Dollars $85,000,000 (all non-personnel)

Description of Item

The FBI requests $85million to support the DOJ Data Center Transformation Initiative (DCTI).

Justification

As part of the DCTI, DOJ plans to consolidate over 40 data centers into 3 Core Enterprise Facilities (CEFs) in Pocatello, Idaho (FBI), Clarksburg, WV (FBI), and Sterling, VA (DEA) by FY 2019. The goals of this effort include:

a. strengthening our cybersecurity posture and data protection through placement in fewer standardized, resilient environments
b. optimizing and standardizing infrastructure
c. improving operation efficiency and agility
d. leveraging staff and resources
e. reducing energy use and property footprint

DOJ closed 13 data centers in FY 2015. One of these facilities was the DOJ data center in Dallas that was consolidated into the FBI's Pocatello Information Technology Center (PITC), resulting in a reduction of 30,000 square feet of leased floor spaces and a 57 percent reduction in energy cost per kilowatt hour (kWh).

The requested resources will fund sitework and construction of the PITC Data Center.

Impact on Performance

Without this funding, DOJ will not be able to complete the Pocatello, Idaho CEF.

Funding

Base Funding

FY 2015 Enacted				FY 2016 Enacted				FY 2017 Current Services			
Pos	Agt	FTE	($000)	Pos	Agt	FTE	($000)	Pos	Agt	FTE	($000)
…	…	…	$...	…	…	…	$...	…	…	…	$...

Non-Personnel Increase Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2017 Request ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
Data Center	n/a	n/a	$85,000	$ …	$ …
Total Non-Personnel			$85,000	$ …	$ …

Total Request for this Item

	Pos	Agt	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
Current Services	…	…	…	$...	$...	$...	$...	$ …
Increase	…	…	…	…	85,000	85,000	…	…
Grand Total	…	…	…	$...	$85,000	$85,000	$...	$ …

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

Strategic Goal(s) & Objective(s): All
Budget Decision Unit(s): N/A

Organizational Program: Facilities and Logistics Services

Program Decrease: Positions … Agt … Atty … FTE … Dollars ($16,500,000) (all non-personnel)

Description

The FBI's FY 2017 request includes a permanent $16,500,000 reduction to the SWE Program. As a national security agency, sufficient funding for the SWE Program is critical to ensuring the FBI's Field Offices, Resident Agencies, and Legats have the proper facilities and robust network and analytical tools to gather, store and analyze classified information provided by, and share information with, our IC partners. This funding not only ensures the FBI's classified information technology remains current and in compliance with IC standards, it provides tools not available elsewhere in the FBI to conduct analysis in support of active national security intelligence and investigative matters. Providing secure facilities, workspace, and information technology is a core requirement and expectation for the FBI as an IC partner.

Justification

The $16.5 million reduction enables the Program to continue to maintain the existing SCIF facilities and Top Secret workstations.

Impact on Performance

The recommended reduction will ensure that the SWE Program will focus its resources on priority field and Legat locations and improve capabilities to discuss, process, and store TS/SCI information. The SWE Program will leverage prior-year balances when and where necessary to continue to ensure that the FBI's TS network is not at risk. Other investments in infrastructure elsewhere in this Budget will help to ensure that there will be no negative impacts from this reduction to missions or operations.

Funding

Base Funding

FY 2015 Enacted				FY 2016 Enacted				FY 2017 Current Services			
Pos	Agt	FTE	($000)	Pos	Agt	FTE	($000)	Pos	Agt	FTE	($000)
…	…	…	$66,982	…	…	…	$66,982	…	…	…	$66,982

Non-Personnel Offset Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2017 Request ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
Secure Work Environment	n/a	n/a	($16,500)	$ …	$ …
Total Non-Personnel			($16,500)	$ …	$ …

Total Offset for this Item

	Pos	Agt	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
Current Services	…	…	…	$...	$66,982	$66,982	$...	$ …
Decreases	…	…	…	…	(16,500)	(16,500)	…	…
Grand Total	…	…	…	$...	$50,482	$50,482	$...	$ …

IX. Glossary

ACE	Asian Criminal Enterprises
AFIT	Advanced Fingerprint Identification Technology
AML	Applications Mall
ASCLD-LAB	American Society of Crime Laboratory Directors - Laboratory Accreditation Board
ATB	Adjustment to Base
ATF	Firearms and Explosives
BAU III	Behavior Analysis Unit III
BCI	Border Corruption Initiative
BCTF	Border Corruption Task Force
BCWG	Border Corruption Working Group
BMR	Black Market Reloaded
BOP	Bureau of Prisons
BTC	Biometrics Technology Center
C2S	Commercial Cloud Service
CARD	Child Abduction Rapid Deployment
CD	Counterintelligence Division
CEFC	Criminal Enterprises Federal Crimes Decision Unit
CHS	Confidential Human Source
CI	Counterintelligence
CID	Criminal Investigative Division
CIP	Computer Intrusion Program
CIRG	Critical Incident Response Group
CJIS	Criminal Justice Services Division
CJS	Criminal Justice Services Decision Unit
CODIS	Combined DNA Index System
COL	Color of Law
CONOPS	Concept of Operations
CORE	Collection Operations Requirements Environment
COTS	Commercial Off-The-Shelf
CPC	Counterproliferation Center
CPOT	Consolidated Priority Organization Target
CST	Child Sex Tourism
CT	Counterterrorism
CT/CI	Counterterrorism/Counterintelligence Decision Unit
CVE	Countering Violent Extremism
DEA	Drug Enforcement Administration
DI	Directorate of Intelligence
DOD	Department of Defense
DTE	Desktop Environment
DU	Decision Unit
EAD-I	Executive Assistant Director for Intelligence
ECE	Eurasian Criminal Enterprises
EDAM	Enterprise Data Access Management

EFCON	Electronic Fingerprint Conversion
EFTS	Electronic Fingerprint Transaction Standard
EMS	Environmental Management System
EMT	Enterprise Management Service
EPCRA	Emergency Planning & Community Right-to-know Act
EPP	Environmental Protection Programs
ERF	Engineering Research Facility
FACE	Under the Freedom of Access to Clinic Entrances
FBI	Federal Bureau of Investigation
FCOP	Federal Convicted Offender Program
FIG	Field Intelligence Group
FIS	Foreign intelligence services
FISA	Foreign Intelligence Surveillance Act
FLP	Foreign Language Program
FO	Field Offices
FTE	Full time equivalents
FTTTF	The Foreign Terrorist Tracking Task Force
G/CE	Gang/Criminal Enterprise
GangTECC	National Gang Tracking Enforcement Coordination Center
GEOINT	Geospatial Intelligence
HDS	Hazardous Devices School
HHS	Health and Human Services
HUMINT	Human intelligence
IA	Intelligence Analysts
IAA/IdAM	Identity Authentication Authorization/Identity and Access Management
IAFIS	Integrated Automated Fingerprint Identification System
IC	Intelligence Community
IC ITE	Intelligence Community Information Technology Enterprise
IC3	Internet Crime Complaint Center
ICC	Indian Country Crimes
ICE-HSI	Customs Enforcement, Homeland Security Investigations
IDU	Intelligence Decision Unit
IED	Improvised explosive devices
IIR	Intelligence Information Report
ILNI	Innocence Lost National Initiative
IOD	International Operations Division
IPR	Intellectual Property Rights
ISSM	Information System Security Manager
IT	Information Technology
ITS	Information Transport Service
JCA	Joint Community Assessments
JPO C-IED	Joint Program Office for Countering Improvised Explosive Devices
JWICS	Joint Worldwide Intelligence Communication System
LCN	La Cosa Nostra
LEED	Leadership in Energy and Environmental Design

LEEP	Law Enforcement Enterprise Portal
LEGATS	Legat Attaché Offices Overseas - Legal Attaché
LEO	Law Enforcement Online
LEOKA	Law Enforcement Officers Killed and Assaulted
MST	Mobile Surveillance Teams
MST-A	Mobile Surveillance Teams - Armed
NBTF	National Border Corruption Task Force
NCIC	National Crime Information Center
NCIJTF	National Cyber Investigative Joint Task Force
NCTC	National Counterterrorism Center
N-DEx	National Data Exchange
NDIS	National DNA Index System
NEPA	National Environmental Policy Act
NGC	Next Generation Cyber
NGI	Next Generation Identification
NHCAA	National Health Care Anti-Fraud Association
NIBRS	National Incident-Based Reporting System
NIE	National Intelligence Estimates
NIP	National Intelligence Program
NRES	Network Requirements and Engineering Services
NVTC	National Virtual Translation Center
O&M	Operations and Maintenance
OCDETF	Organized Crime Drug Enforcement Task Force Program
OCP	Organized Crime Program
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
OPE	Office of Partner Engagement
OSG	Operational Section: Gangs
OTD	Operational Technology Division
OTT	Over-The-Top
PDB	Presidential Daily Briefing
PMO	Program Management Office
POE	Ports of Entry
POL	Petroleum, Oil, & Lubricants
PS	Professional Support
RA	Resident Agencies - satellite offices throughout the country
RISC	Repository for Individuals of Special Concern
S&E	Salaries & Expenses
SA	Special Agents
SAR	Suspicious Activity Reports
SCC	IC Security Coordination Center
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facilities
SCINet	Sensitive Compartmented Information Operations Network
SIG	Special Interest Group

SIT	System Integration and Test
SMC	System Management Center
SOCM	Sense of the Community Memoranda
SOD	Special Operations Division
SOS	Staff Operation Specialist
SSPP	Strategic Sustainability Performance Plan
TCO	Transnational Criminal Organization
TEDAC	Terrorist Explosive Device Analytical Center
TFC	Threat Fusion Cells
TOC	Transnational Organized Crime
TRP	Threat Review and Prioritization
TS	Top Secret
TSC	Terrorist Screening Center
UCR	Uniform Crime Reporting
USG	U.S. Government
USIC	U.S. Intelligence Community
USMS	U.S. Marshals Service
VC	Violent Crime
VCC	Virtual Command Center
VCTS	Violent Criminal Threat Section
VGSSTF	Violent Gang Safe Streets Task Forces
WCC	White Collar Crime
WMD	Weapons of Mass Destruction
WMDD	Weapons of Mass Destruction Directorate
XTS	Exploitation Threat Section