U.S. Department of Justice
Federal Bureau of Investigation

FY 2018 Authorization and Budget Request to Congress

May 2017

Table of Contents

Page No.

I. OVERVIEW FOR THE FEDERAL BUREAU OF INVESTIGATION

A. Introduction

Budget Request Summary: The Federal Bureau of Investigation's (FBI's) Fiscal Year (FY) 2018 budget request proposes a total of $8,774,477,000 in direct budget authority, of which $8,722,582,000 is for Salaries and Expenses (S&E) and $51,895,000 is for Construction. The S&E request includes a total of 33,533 direct positions and 31,999 direct full time equivalents (FTE); the positions include:

- 12,484 Special Agents (SAs)
- 2,950 Intelligence Analysts (IAs)
- 18,099 Professional Staff (PS)

The FY 2018 Adjustments to Base (ATB) include a Department-wide workforce rightsizing initiative mandated by the Attorney General, which translates into a position reduction at the FBI totaling 2,095 positions, including:

- 750 Special Agents (SAs)
- 150 Intelligence Analysts (IAs)
- 1,195 Professional Staff (PS)

The S&E program increases total $117,583,000, 470 positions (150 SAs, 50 IAs), and 470 FTE, for the following:

- $41,474,000 for cyber investigative capabilities
- $19,727,000 to support foreign intelligence and insider threat investigations and continuous evaluation
- $21,636,000 to counter the threat of Going Dark and for Investigative Technology
- $6,779,000 to combat transnational organized crime (TOC)
- $8,242,000 to support physical surveillance capabilities
- $7,375,000 for the Biometrics Technology Center (BTC) Operations and Maintenance (O&M)
- $3,450,000 for the Violent and Gun-Related Crime Reduction Task Force
- $8,900,000 to support the National Instant Criminal Background Check System (NICS).

The positions identified above support operations and are critical to meeting the FBI's mission.

The $51,895,000 requested in Construction accounts for the Secure Work Environment (SWE) Program ($49,895,000) and facility upgrades at the FBI Academy campus ($2,000,000).

The request also includes balance offsets totaling $195,000,000 from Criminal Justice Information Services (CJIS) automation excess surcharge fee balances and a $16,500,000 permanent program reduction from the Secure Work Environment program Construction funds.

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 2018 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:

The mission of the FBI is to protect the American people and uphold the Constitution of the United States. The FBI's mission priorities are to:

- Protect the US from terrorist attack
- Protect the US against foreign intelligence operations and espionage
- Protect the US against cyber-based attacks and high-technology crimes
- Combat public corruption at all levels
- Protect civil rights
- Combat domestic and transnational criminal organizations and enterprises
- Combat major white-collar crime
- Combat significant violent crime

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, typically staffed at fewer than 20 personnel 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 and Assistant Directors in Charge of FBI field offices report directly 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. In April 2017, the General Services Administration awarded a construction contract for the FBI's Central Records Center facility to be located in Winchester, Virginia. Construction is scheduled to begin in the fall of 2017 and facility completion estimated in FY 2020.

FBI Quantico

FBI CJIS Campus

The FBI also operates 63 Legal Attaché (Legat) offices and 27 sub-offices in 75 countries around the world. This number fluctuates based upon demand and the global threat environment.

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 Enterprise Services 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, 21 percent of the Laboratory Division’s workload is in support of counterterrorism investigations and accordingly, 21 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 appropriation.

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

In an effort to better address all aspects of the FBI's requirements, the FBI 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 ash-Sham, commonly known as ISIS, 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 March 2017, the FBI estimates over 300 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 ISIS, may have over those living in the U.S. 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.

ISIS 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, ISIS has persistently used the Internet to communicate. From a homeland security perspective, it is ISIS's widespread reach through the Internet and social media which is most concerning as ISIS has aggressively employed this technology for its nefarious strategy. ISIS 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 ISIS by facilitating an associate's travel to Syria to join ISIS. 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 2016 and early 2017, the FBI's Office of Partner Engagement (OPE) took the lead on producing two documentaries on extremist indicators and profiles, and these documentaries will be disseminated for viewing to local law enforcement communities and security professionals, mainly through local FBI field divisions. The FBI continues to be represented on the DHS-DOJ led interagency CVE Task Force.

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, penetrate, and influence U.S. institutions.

A recent notable success was the March 2017 guilty plea by ZTE, a Chinese telecommunications company, which agreed to pay the United States an $892 million penalty for violating U.S. sanctions on Iran. The FBI investigation determined that ZTE had been obtaining restricted dual-use goods in the United States, embedding them into ZTE's own products, then shipping them to Iran for sale, even though these items were designated on the Department of Commerce's (DOC) controlled items list and therefore, barred from export to Iran. ZTE knowingly conducted this illegal activity for nearly six years, and it took active steps to conceal its activity, such as by making false statements on customs declarations and using other companies to insulate ZTE's involvement.

ZTE agreed to enter a guilty plea and to pay a $430,488,798 penalty to the U.S. for conspiring to violate the International Emergency Economic Powers Act (IEEPA), obstructing justice, and making a material false statement. ZTE simultaneously reached settlement agreements with DOC's Bureau of Industry and Security (BIS) and the Department of the Treasury's Office of Foreign Assets Control (OFAC), thus bringing its total penalties to $892,360,064. The agreement also included an additional $300 million that ZTE must pay if it violates its settlement agreement in the future.

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.

During the course of an investigation into the 2014 breach of Yahoo! databases, the FBI discovered Russian FSB officers' conspiracy to protect, direct, facilitate, and pay criminal hackers to gain unauthorized access to Internet service providers' (ISPs) computers and their customers located in the U.S. and around the world, to maintain unauthorized access to those computers, and to steal information from those computers.

As a result, account information, including personally identifiable information, of at least 500 million user accounts was stolen from Yahoo!'s user database as part of a larger intrusion into the company's computer networks, which continued through at least September 2016. As part of this intrusion, malicious files and software tools were downloaded into Yahoo!'s networks. The conspirators used their unauthorized access to the network to identify and access accounts of interest to Russia and the FSB and for personal financial gain.

One of the criminal hackers involved, Aleksey Belan, further utilized unauthorized access to Yahoo!'s network for personal profit at the expense of his victims. He compromised Yahoo!'s search engine to direct users to an online pharmacy in exchange for marketing fees, searched within Yahoo! user email accounts for financial information (such as credit card and gift card numbers), and obtained access to the contents of the email accounts of more than 30 million Yahoo! users, whose contact lists were then stolen in a spam scheme.

The conspirators also targeted webmail accounts at other providers, including Google, based in part on information about those accounts stolen from Yahoo.

On March 14, 2017, the United States District Court for the Northern District of California unsealed an indictment of four individuals in connection with the breach. The indictment and arrest warrants were for FSB officers Dmitry Dokuchaev and Igor Sushchin and criminal hackers Alexsey Belan and Karim Baratov. Dokuchaev, Sushchin, and Belan are Russian citizens who reside in Russia. Baratov is a Canadian citizen who resides in Canada. The U.S. arrest warrant for Baratov was subsequently provided to the Canadian Department of Justice and the Royal Canadian Mounted Police. The RCMP executed the arrest of Baratov on March 14, 2017. The U.S. plans to pursue extradition of Baratov.

***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.

> **<u>Public Corruption</u>:** 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.

<u>Other Complex Financial Crimes (Insurance, Bankruptcy, and Mass Marketing Fraud)</u>: 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.

<u>Intellectual Property Rights</u>: 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 May 2016, the FBI leads 170 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:

- <u>Hate Crimes</u>: 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.

- <u>Color of Law (COL)</u>: 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.

- <u>Human Trafficking</u>: 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.

- <u>Freedom of Access</u>: 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. In FY 2016, FBI efforts led to 1,440 Crimes Against Children convictions.

- 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 consists of over 60 experienced Crimes Against Children investigators.

- 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 Unit (ICCU) has developed and implemented strategies to address the most egregious crime problems in Indian Country (IC) where the FBI has jurisdiction. These matters generally focus on death investigations, child sexual assault and physical abuse, assault resulting in serious bodily injury, gang/criminal enterprise investigations, and financial crimes. DOJ has reported that 25 percent of all violent crimes prosecuted by the U.S. Attorneys' Offices are related to Indian Country. ICCU supports joint investigative efforts with the Bureau of Indian Affairs and tribal law enforcement agencies. ICCU also manages 15 Safe Trails Task Forces (STTF) and conducts essential investigative training to support these STTFs, as well as approximately 130 FBI agents and other law enforcement partners, who focus on IC crimes. Although IC cases are generally reactive, many are cross-programmatic in nature, including Indian gaming, public corruption, and complex financial fraud.

Due to jurisdictional issues and the remote nature of many reservations, 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 generally only prosecute misdemeanor violations involving Indian subjects, 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. In FY 2016, FBI efforts led to 855 Indian Country arrests and 674 Indian Country convictions.

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.

[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.

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 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.

- 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 2018 Budget Strategy

The foundation of the FBI's budget strategy is supported by the FBI's mission, vision, and strategic objectives. At the heart of the FBI's strategy is the vision statement: Ahead of the threat through leadership, agility, and integration. The FBI aims to be ahead of the threat in two different ways. First, the FBI's goal is to continuously evolve to anticipate and mitigate existing threats. Second, the FBI needs to be able to recognize and address threats that it has not yet seen.

The mission of the FBI is to protect the American People and uphold the Constitution of the United States. The FBI has identified eight priorities to focus efforts and accomplish the mission. In addition, the FBI uses a threat prioritization process to maximize its effect in these areas and ensure that all threat issues are considered.

The FBI must also structure the organization to be as effective as possible by identifying and closing strategic gaps. To close strategic gaps, the FBI has 11 enterprise objectives, organized thematically into four pillars: capability, technology, talent, and stewardship. Each represents a broad area of focus for the entire FBI and an overarching strategy to accomplish FBI's mission. The 11 strategic objective focus areas are as follows:

- Focus on Leadership in Every Aspect of the FBI;
- Incorporate Intelligence in All We Do;
- Enhance Cyber Capabilities;
- Improve Organizational Agility;
- Strengthen Partnerships;
- Improve Information Technology;
- Deploy Innovative Solutions;
- Promote a Culture of Accountability and Transparency;

- Transform Recruitment and Hiring;
- Improve Workforce Development; and,
- Improve Stewardship of Resources.

The FBI's success depends on monitoring and improving its ability to meet these objectives. The FBI conducts headquarters level Quarterly Strategy Reviews to discuss FBI's progress on its objectives, and Project Management Reviews to track particular projects that support the strategy. These reviews are conducted both at an enterprise level. In the field, the strategy is cascaded through the Integrated Program Management Process, which tracks the FBI's execution of its mission. Headquarters operational programs evaluate the threat landscape and develop mitigation strategies. Field offices then evaluate the threat in their areas and create a strategy to address it throughout the year. These strategies undergo mid-year and end-of-year assessments; both Headquarters and the field are held to measures to track their performance. FBI executives and Program Managers hold regular meetings to review and evaluate the effectiveness and success of the strategic measures throughout the fiscal year.

By understanding the threat-based landscape and identifying critical enterprise-wide capabilities needed to perform its mission, the FBI's budget strategy and future resource requirements and requests are designed to enable the FBI to address the current range of national security threats and crime problems and also focus on the future needs of the FBI.

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. Additionally, 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. The FY 2018 budget request is designed to promote capabilities and strategies that are sufficiently agile to meet ongoing, emerging and as yet unknown national security, cyber, and criminal threats.

The FBI's 2018 budget request also incorporates the "Workforce Rightsizing" initiative into forward leaning strategic planning. The FBI continues to seek opportunities to leverage its numerous intelligence community and law enforcement partners' reach, expertise and resources, as well as independently operate efficiently and effectively within an ever-changing threat environment. As always, central to the FBI's success are the talented individuals that support the agency and its mission.

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 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'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 enhance the FBI’s cyber efforts, the FBI will improve technical tools, support the FBI’s cyber program, and expand high-speed networks. This will support the FBI’s mission to defeat cyber intrusion threats through a unique combination of law enforcement and national security authorities.	36	36	$41,474	5-1
Foreign Intelligence and Insider Threat and Continuous Evaluation	To address threats posed by foreign intelligence and insiders.	93	93	19,727	5-2
Going Dark/Investigative Technology	To counter the threat of Going Dark, which includes the inability to access data because of constraints related to encryption, mobility, and other communications device challenges.	80	80	21,636	5-3
Transnational Organized Crime (TOC)	To support ongoing Transnational Organized Crime investigations of the highest-level TOC actors, both domestically and internationally.	65	65	6,779	5-4
Physical Surveillance	To support FBI surveillance operations.	78	78	8,242	5-8
Biometrics Technology Center (BTC) Operations and Maintenance (O&M)	To support the Operations and Maintenance (O&M) requirements of the FBI's BTC.	...	…	7,375	5-9
Violent and Gun-Related Crime Reduction Task Force	To support the President’s February 9, 2017 Executive Order “Task Force on Crime Reduction and Public Safety” by assisting with the implementation of recommendations from the Task Force, which was created by the Attorney General on February 28, 2017.	33	33	3,450	5-12
National Instant Criminal Background Check System (NICS)	To maintain efforts addressing high volumes of firearms background checks	85	85	8,900	5-16
Total, Salaries and Expenses Enhancements		**470**	**470**	**$117,583**	

Program	Description	Pos.	FTE	Dollars ($000)	Page
Construction Program Reduction					
Secure Work Environment (SWE) Permanent Program Reduction	This permanent program reduction offset will reduce funding from the SWE Program, which includes Sensitive Compartmented Information Facilities (SCIF) and the Sensitive Compartmented Information Network (SCINet) and will better align resources with actual program requirements.	…	…	($16,500)	7-3
Total, Construction Permanent Program Reduction		…	…	**($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] *$8,722,582,000*, 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, $195,000,000 are hereby permanently cancelled 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 Balanced Budget and Emergency Deficit Control Act of 1985, as amended. (Department of Justice Appropriations Act, 2016.)

Analysis of Appropriations Language

- No substantive changes.

IV. Decision Unit Justification

A. Intelligence Decision Unit

INTELLIGENCE DECISION UNIT TOTAL	**Pos.**	**FTE**	**Amount ($000)**
2016 Enacted	7,191	6,544	$1,677,185
2017 Continuing Resolution	6,792	6,401	1,617,030
Adjustment to Base and Technical Adjustments*	(413)	(360)	31,415
2018 Current Services**	6,379	6,041	1,648,445
2018 Program Increases	63	63	10,199
2018 Program Decreases	...	...	...
2018 Request	6,442	6,104	$1,658,644
Total Change 2017-2018	**(350)**	**(297)**	**$41,615**

* reflects elimination of funded/unfilled positions and FTE with corresponding amounts and inflationary adjustments for funded/filled positions and FTE
** represents projected onboard positions/FTE as of pay period #1, FY 2018

1. Program Description

The FBI’s Intelligence Decision Unit (IDU) is comprised of the entirety of the Intelligence Branch (IB), including the Directorate of Intelligence (DI) and the Office of Partner Engagement (OPE); the intelligence functions within the Counterterrorism, Counterintelligence, Cyber, and Criminal Investigative Divisions and the Weapons of Mass Destruction Directorate; Field Intelligence Groups (FIGs); 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 operational 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 leader of the FBI’s Intelligence Program, the IB 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, resources, policy, and functions for actively engaging with the FBI’s partners across the intelligence, law enforcement, and private sector partners. The FBI’s Intelligence Program Strategy and its six areas of focus—workforce success, culture and mindset, technology capabilities, information sharing, collection, and exploitation and analysis—guide the branch’s direction and oversight of all aspects of the organization’s intelligence work.

The IB includes the Bureau Intelligence Council, which provides FBI leaders with a consolidated, integrated perspective on threats while helping to integrate and balance the organization’s priorities with those of the broader Intelligence Community and U.S. government. Led by a Deputy Assistant Director, the council is made up of Senior National Intelligence Officers with subject-matter expertise on geographic and functional programs who help integrate the FBI’s understanding of priority threat issues. The council also houses the Bureau Control Office, which manages the FBI’s sensitive compartmented information program.

Directorate of Intelligence

The 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 seven 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; excellence in language services; and enhanced technology capabilities to foster efficient data exploitation and analysis. 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 collection and 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 IA 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 ensure FBI investigative and operational strategies 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 responsible for the management, execution, and coordination of intelligence functions, to include the collection, analysis, production, and dissemination of strategic and tactical intelligence to all FBI investigative programs and other federal, state, local, tribal, and territorial partners. FIGs integrate the intelligence cycle (requirements; planning and direction; collection; processing and exploitation; analysis and production; dissemination) to meet current and future national security and criminal threats.

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 use and deployment of its linguist workforce, language tools, and technology. The FBI workforce has certified capabilities in over 90 languages and dialects, spanning approximately 100 FBI domestic and overseas locations. The FLP promulgates policies and compliance requirements to ensure fidelity of finished English-language intelligence products. 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 performing intelligence workforce.

Language Analysis

Nearly every major FBI investigation 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 component of 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 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) provides and facilitates timely and accurate translation services to the U.S. Intelligence Community (IC). NVTC was established under Section 907 of the USA Patriot Act (2001) and designated an IC service of common concern in 2014. Since its inception, NVTC has complemented IC elements' foreign language translation capabilities by supporting tasks ranging from high-volume surges to immediate translation requirements. 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.

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 has instituted an integrated approach to training that brings employees together at the beginning of their careers to understand the importance and impact of an integrated intelligence and operational methodology – a model that continues throughout the organization's intermediate and advanced courses of instruction.

Office of Partner Engagement

The OPE implements initiatives and strategies which support engagement, communication, coordination, and cooperation efforts with law enforcement, intelligence, public and private agencies and partners in a continuous effort to enhance the FBI's capabilities in the Domestic Information-Sharing Architecture. The OPE accomplishes this mission by establishing and maintaining methods and practices to enhance engagement, coordination, and information sharing with the IC; federal, state, local, tribal, and territorial law enforcement; and public and private organizations and working groups. The office leads the FBI's approach to intelligence supporting the Domestic Information-Sharing Architecture, provides program management for the FBI's engagement with state and local fusion centers, and proactively reviews and disseminates relevant and appropriate threat information to FBI federal, state, local, tribal, and territorial partners.

Exploitation Threat Section

The Counterterrorism Division's Exploitation Threat Section (XTS) leads law enforcement and intelligence efforts in the United States to defeat terrorism by targeting terrorist communications, and by 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. The TSC identifies, prevents, deters, and disrupts potential terrorist activity and other national security threats by maintaining a thorough, accurate, and current database of known and suspected terrorists, and by sharing this information with law enforcement, intelligence, screening, and regulatory agencies at the federal, state, local, territorial, tribal, and international levels. This effort provides 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 a participant in ICITE, an ODNI-led multi-year IT initiative to create an IC-wide information sharing infrastructure.

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

Decision Unit: Intelligence											
RESOURCES		**Target**		**Actual**		**Projected**		**Changes**		**Requested (Total)**	
		FY 2016		**FY 2016**		**FY 2017**		**Current Services Adjustments & FY 2018 Program Changes**		**FY 2018 Request**	
Total Costs and FTE		**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		6,544	1,677,185	6,544	1,677,185	6,401	1,617,029	(360)	31,415	6,104	1,658,644
TYPE	**PERFORMANCE**	**FY 2016**		**FY 2016**		**FY 2017**		**Current Services Adjustments & FY 2018 Program Changes**		**FY 2018 Request**	
Performance Measure (non-NIP)	% of Counterterrorism FISA collection reviewed by the Language Program: • Audio • Text • Electronic File	100% 100% 100%		95% 100% 100%		100% 100% 100%		- - -		100% 100% 100%	
Performance Measure: *Responsiveness* (NIP)	% of IIRs citing US Intelligence Community (USIC) Priority 1 or 2 requirements	80%		77.4%		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.											

PERFORMANCE MEASURE TABLE							
Decision Unit: Intelligence							
Performance Report and Performance Plan Targets	**FY 2012**	**FY 2013**	**FY 2014**	**FY 2015**	**FY 2016**	**FY 2017**	**FY 2018**

		Actual	Actual	Actual	Actual	Target	Actual	Target	Target
Performance Measure	% of Counterterrorism FISA collection reviewed by the Language Program:								
	• Audio	79%	100%	100%	93%	100%	95%	100%	100%
	• Text	56%	100%	100%	100%	100%	100%	100%	100%
	• Electronic File (non-NIP)	82%	79%	100%	100%	100%	100%	100%	100%
Performance Measure: ***Responsiveness***	% of IIRs citing US Intelligence Community (USIC) Priority 1 or 2 requirements (NIP)	N/A	76	76%	75.6%	80%	77.4%	80%	80%

2. Performance, Resources, and Strategies

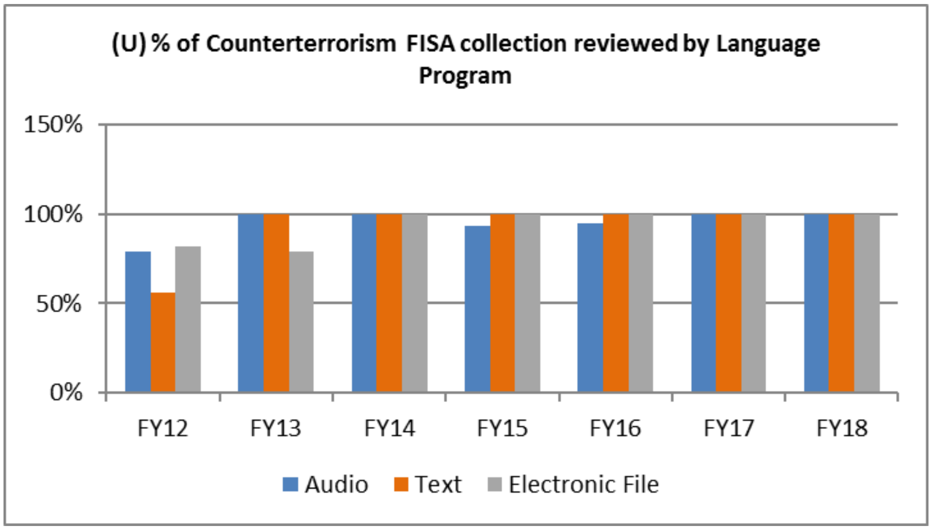
a. Performance Plan and Report for Outcomes

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

2016 Actuals:
Audio: *95%*
Text: *100%*
Electronic: *100%*

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

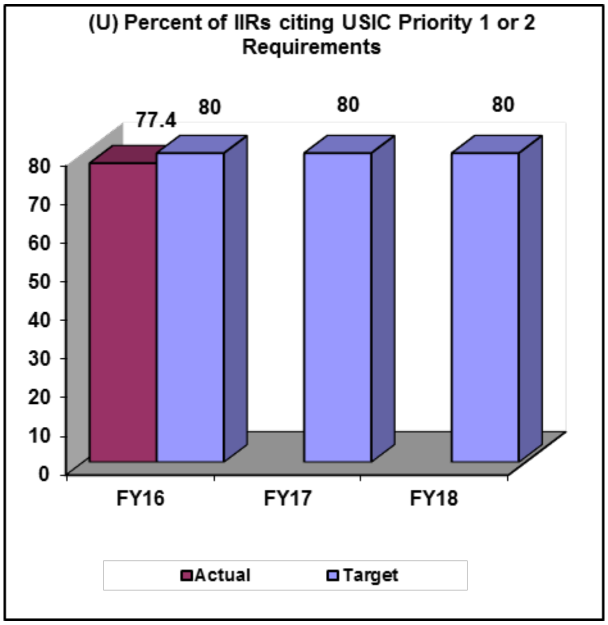
2018 Targets:
Audio: *100%*
Text: *100%*
Electronic: *100%*



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." 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 2012 through FY 2016 data represents actual results, while FY 2017 and FY 2018 data reflect targets.

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

2016 Actual: 77.4%
2017 Target: 80%
2018 Target: 80%



Discussion: This measure was designed to determine whether the FBI is collecting and meeting the needs of the IC 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 2017 and FY 2018 targets are based on current trends and projected future performance. The target will remain at 80 percent in FY 2018.

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)
2016 Enacted	13,210	12,142	3,452,493
2017 Continuing Resolution	13,620	12,889	3,435,899
Adjustment to Base and Technical Adjustments*	(875)	(775)	47,217
2018 Current Services**	12,745	12,114	3,483,116
2018 Program Increases	208	208	60,855
2018 Program Decreases	...	...	...
2018 Request	12,953	12,322	3,543,971
Total Change 2017-2018	**(667)**	**(567)**	**108,072**

* reflects elimination of funded/unfilled positions and FTE with corresponding amounts and inflationary adjustments for funded/filled positions and FTE

** represents projected onboard positions/FTE as of pay period #1, FY 2018

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 operational 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 Special Agents (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 Terrorist Screening Center (TSC) and Foreign Terrorist Tracking Task Force (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.

[2] Please note that while the TSC and 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 revised its approach to strategic planning, and refocused recruiting and hiring efforts to attract individuals with skills critical to its counterterrorism and intelligence missions. The FBI has also developed a comprehensive training program and instituted new leadership initiatives to keep its workforce flexible.

The FBI has divided its CT operations into branches, each of which focuses on a different aspect of the current terrorism threat facing the Nation. These components are staffed with SAs, Intelligence Analysts (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 collocation of personnel at Liberty Crossing, it is clear that the FBI and its partners in the IC are integrated at 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's (WMDD) mission is to lead USG law enforcement and domestic intelligence efforts to prevent and neutralize weapons of mass destruction (WMD) threats against the homeland and support interests abroad. Establishing the WMDD in FY 2006 unified this distinctive combination of law enforcement authorities, intelligence analysis capabilities, and technical subject matter expertise into an effective national approach to preventing and responding to WMD threats.

Preparing, assessing, and responding to WMD threats and incidents is challenging, because WMD materials and events are unique in character, response requirements, and potential consequences. The WMDD integrates and links all of the necessary counterterrorism, intelligence, counterintelligence, and scientific and technological components to accomplish the FBI's overall WMD mission while adhering to FBI core values. In addition to its lead role in WMD matters, the WMDD supports its partners in the Counterterrorism Division, Counterintelligence Division, Directorate of Intelligence, Criminal Investigative Division, and Cyber Division when their cases and intelligence involve a WMD nexus.

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, relevant, and actionable intelligence to and collaborate with key stakeholders – other FBI divisions, USIC, and law enforcement, foreign, and private sector partners - to identify, understand, and mitigate priority current and emerging WMD threats and vulnerabilities.

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 Directorate of Intelligence 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, in conjunction with the National Counterproliferation Center (NCPC), 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 in 2011, there have been over 140 arrests stemming from CPC cases.

Counterintelligence Program

Executive Order 12333 assigns to the Director of the FBI, under the Attorney General, oversight and supervision responsibility for conducting and coordinating counterintelligence (CI) activities within the United States. The FBI's CI mission is to protect the U.S. by identifying, understanding, and combating foreign government activities that pose a threat to national security. As the lead for domestic CI matters, the FBI leverages partners and methods to combat the threat posed by foreign government activities threatening our national security. The FBI's primary counterintelligence responsibility is to identify, understand, and combat these threats.

The domestic counterintelligence environment is more complex than ever, posing a continuous threat to U.S. national security and the economy, targeting sensitive U.S. strategic technologies, industries, sectors, and critical infrastructures. Historically, asymmetric counterintelligence threats involved foreign intelligence service (FIS) officers seeking US Government and USIC information. Within the past few years, the FBI has observed adversaries employing a wide range of non-traditional collection techniques. These techniques include FIS use of human collectors affiliated with non-intelligence services, foreign investment in critical U.S. sectors, and infiltration into U.S. supply chains. The FBI continues to adjust its CI priorities and posture to address the evolving and multi-faceted threat.

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 Special Operations Group (SOG) and the Special Surveillance Group (SSG) – and its Aviation Surveillance program. SOGs are comprised of armed agents who perform surveillances of targets that might have the propensity for violence; SSGs are comprised of unarmed investigative specialists who perform surveillances of targets who are unlikely to be violent. SOGs, SSGs, and Aviation Surveillance provide critical support to CT and CI investigations.

Legal Attaché (Legat) Program

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

Decision Unit: Counterterrorism/Counterintelligence											
WORKLOAD/ RESOURCES		**Target**		**Actual**		**Projected**		**Changes**		**Requested (Total)****	
		FY 2016		**FY 2016**		**FY 2017**		**Current Services Adjustments & FY 2018 Program Changes**		**FY 2018 Request****	
Number of Cases: Counterterrorism, Counterintelligence, & Computer Intrusions		†		61,029		†		†		†	
Total Costs and FTE		**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		12,142	3,452,493	12,142	3,452,493	12,889	3,435,899	(567)	108,072	12,322	3,543,971
TYPE	**PERFORMANCE**	**FY 2016**		**FY 2016**		**FY 2017**		**Current Services Adjustments & FY2018 Program Changes**		**FY 2018 Request****	
Program Activity	**1. Counterterrorism (CT)**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		7,042	2,002,446	7,042	2,002,446	6,738	1,796,138	(323)	49,160	6,415	1,845,298
Workload -- # of cases investigated (pending and received)		†		28,469		†		†		†	
Program Activity	**2. Counterintelligence**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		4,128	1,173,848	4,128	1,173,848	4,198	1,119,023	(162)	41,794	4,036	1,160,817
Program Activity	**3. Cyber Program (Intrusions)**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		972	276,199	972	276,199	1,953	520,738	(82)	17,118	1,871	537,856
Workload -- # of cases investigated (pending and received)		†		9,969		†		†		†	
Efficiency Measure	Efficiency cost savings from online cyber training ($000)	$2,000		$2,792		-		-		-	

Data Definition, Validation, Verification, and Limitations:

- Counterterrorism measures are provided through records kept by the FBI's Counterterrorism Program, including the Terrorist Screening Center. The count of JTTF participants erroneously did not include part-time participants until FY 2008, but will henceforth include them. No other known data limitations exist.
- Counterintelligence measures are based on records kept by the FBI's Counterintelligence Program. Percentages are updated based upon the most recent review.
- The data source for cases and conviction/pre-trial diversion data is the FBI's Integrated Statistical Reporting and Analysis Application (ISRAA) database. The database tracks statistical accomplishments from inception to closure. Before data are entered into the system, they are reviewed and approved by an FBI field manager. They are subsequently verified through FBI's inspection process. FBI field personnel are required to enter accomplishment data within 30 days of the accomplishment or a change in the status of an accomplishment, such as those resulting from appeals. Data for this report are compiled less than 30 days after the end of the fiscal year, and thus may not fully represent the accomplishments during the reporting period.
- Estimates of cost savings per student taking an online course, compared with an in-service training

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

Performance Report and Performance Plan Targets		FY 2011	FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	FY 2018
		Actual	Actual	Actual	Actual	Actual	Actual	Target	Target
Efficiency Measure	Cost avoidance from online Cyber training ($000)	$4,987	$2,395	$3,585	$2,416	$1,207	$2,792	-	-

2. Performance, Resources, and Strategies

Counterterrorism (CT)

a. Performance Plan and Report for Outcomes

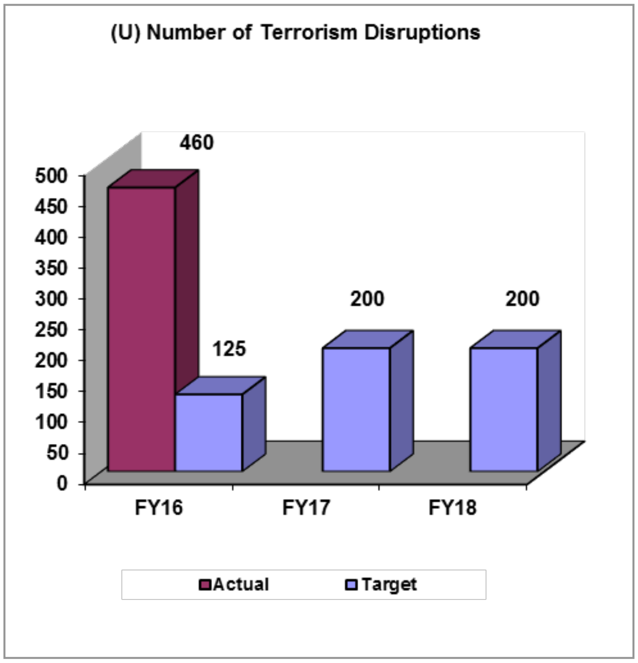
The FBI must understand all dimensions of the threats facing the Nation and address them with new and innovative investigative and operational strategies. Additionally, the FBI must be able to effectively respond to the challenges posed by unconventional terrorist methods, such as the use of chemical, 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.

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

FY 2016 Actual:	**460**
FY 2017 Target:	**200**
FY 2018 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. 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. 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 number of terrorism disruptions effected through CT investigations was 460 in FY 2016, which exceeded the annual target by a wide margin. Overall, domestic terrorism disruption numbers were unusually high in the first two quarters of FY 2016, resulting from the Malheur National Wildlife Rescue standoff. For international terrorism disruptions, numbers in the first two quarters were higher due to the holiday threat posture, which resulted in more arrests, plot disruptions and travel disruptions.

For the first quarter of FY 2017, the number of terrorism disruptions was 76, surpassing the average quarterly target of 31 by 145%, due to an evolving threat directed at the homeland and U.S. interests abroad. Also of note, a Black Separatist extremist network was disrupted in November 2016, leading to five disruptions. The FBI remains proactively positioned to combat a constantly evolving threat landscape, which can lead to disparities between reported disruption totals and previously established targets.

Counterintelligence (CI)

a. Performance Plan and Report for Outcomes

Please refer to the Classified Addendum

b. Strategies to Accomplish Outcomes

The FBI's CI Program continues to execute a comprehensive National Strategy for CI 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 U.S. while effectively leveraging its available resources.

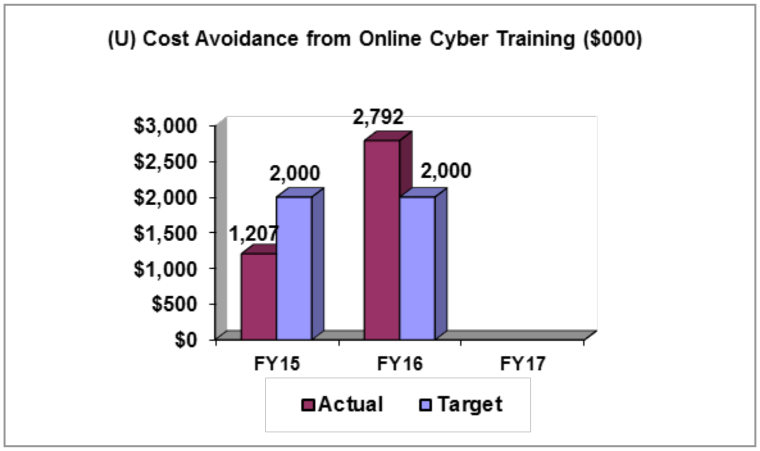
Computer Intrusions

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 2016 Actual: $2,792,000
FY 2017: Discontinued



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.

Due to the reinstatement of funding to cover travel expenses for training and the expansion of in-person course offerings, the Cyber Training & Logistics Unit projects that the online savings for FY 2017 will overall be less than $1 million.

C. Criminal Enterprises Federal Crimes Decision Unit

CRIMINAL ENTERPRISES/FEDERAL CRIMES DECISION UNIT TOTAL	Pos.	FTE	Amount ($000)
2016 Enacted	12,531	11,934	2,879,484
2017 Continuing Resolution	12,509	11,960	2,928,148
Adjustment to Base and Technical Adjustments*	(614)	(533)	50,911
2018 Current Services**	11,895	11,427	2,979,059
2018 Program Increases	114	114	29,055
2018 Program Decreases	…	…	…
2018 Request	12,009	11,541	$3,008,114
Total Change 2017-2018	**(500)**	**(419)**	**$79,966**

* reflects elimination of funded/unfilled positions and FTE with corresponding amounts and inflationary adjustments for funded/filled positions and FTE

** represents projected onboard positions/FTE as of pay period #1, FY 2018

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 operational 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 is a truly international effort, and the people who make up the FBI’s International Operations Division (IOD) and Legat Program work together to lead and direct the FBI’s growing number of operations around the globe.

The FBI’s Legats and their staffs work hard to combat crime 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 also includes a major training component, which includes efforts such as supporting the International Law Enforcement Academies in Budapest or Botswana and teaching 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.

<u>Program Objectives</u>

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.

***Transnational 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.

- *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.

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

2. PERFORMANCE/RESOURCES TABLE

Decision Unit: Criminal Enterprises and Federal Crimes

WORKLOAD/ RESOURCES		**Target**		**Actual**		**Projected**		**Changes**		**Requested (Total)**	
		FY 2016		**FY 2016**		**FY 2017**		**Current Services Adjustments & FY 2018 Program Changes**		**FY 2018 Request**	
Workload -- # of cases investigated (pending and received)		†				†		†		†	
Total Costs and FTE		**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		11,934	2,879,484	11,934	2,879,484	11,960	2,928,148	(419)	79,966	11,541	3,008,114
	PERFORMANCE	**FY 2016**		**FY 2016**		**FY 2017**		**Current Services Adjustments & FY 2018 Program Changes**		**FY 2018 Request**	
	1. White-Collar Crime/Cybercrime	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		5,490	1,324,563	5,490	1,324,563	5,502	1,346,948	(193)	36,785	5,309	1,383,733
Workload -- # of cases investigated (pending and received)		†				†		†		†	
Performance Measure	Restitutions & Recoveries / Fines ($000) • Intellectual Property Rights Violations • Public Corruption • White Collar Crimes (all other)	 †† †† ††		 N/A 391,570 6,814,479		 †† †† ††		 †† †† ††		 †† †† ††	
Performance Measure	Convictions/Pre-Trial Diversions (total) • Intellectual Property Rights Violations **[Discontinued Measure]** • Public Corruption • White Collar Crimes (all other)	 †† †† ††		 N/A 918 2,274		 †† †† ††		 †† †† ††		 †† †† ††	
Performance Measure	Number of Criminal Organizations Engaging in White-Collar Crimes Dismantled	400		302		400		…		400	
Efficiency Measure	% of Major Mortgage Fraud Investigations to all pending Mortgage Fraud Investigations	74%		74%		74%		…		74%	
Performance Measure	Number of convictions for Internet fraud	††		9		††		††		††	

	PERFORMANCE	**FY 2016**		**FY 2016**		**FY 2017**		**Current Services Adjustments & FY 2018 Program Changes**		**FY 2018 Request**	
	2. Criminal Enterprises/Civil Rights/Violent Crimes	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
		6,444	1,554,921	6,444	1,554,921	6,458	1,581,200	(226)	43,181	6,232	1,624,381
Workload -- # of cases investigated (pending and received)		†				†		†		†	
Performance Measure	Convictions/Pre-trial Diversions • Organized Criminal Enterprises • Gang/Criminal Enterprises • Crimes Against Children • Civil Rights	1,400 †† 1,600 ††		2,799 2,580 1,450 185		1,400 †† 1,600 ††		… †† … ††		1,400 †† 1,600 ††	
Efficiency Measure	% of FBI OCDETF Investigations with links to CPOT-linked DTOs **[Discontinued Measure]**	N/A		N/A		N/A		N/A		N/A	
Performance Measure	CPOT-Linked DTOs • Disruptions • Dismantlements	50 20		80 23		50 20		… …		50 20	
Performance Measure	Number of Organized Criminal Enterprise Dismantlements	160		148		160		…		160	
Performance Measure	Number of Gang/Criminal Enterprises Dismantlements	150		123		124		…		124	
Performance Measure	Number of Agents serving on Violent Crime Task Forces	†		1,824		†		†		†	

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.

– Internet Fraud data come from a record system maintained by the IC3. The list of targets is updated each year. Targets are determined by subject matter expert teams at the IC3 and approved by the Unit Chief. IC3 staff maintains the list and determine when a target has been the subject of a take-down. There is some possibility of underreporting of accomplishments resulting from referrals to state, local, and other federal law enforcement organizations. This underreporting is possible where investigations resulting from IC3 referrals do not involve the FBI.

† FBI does not project targets for case workload data.

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

		FY 2011	FY 2012	FY 2013	FY 2014	FY 2015	FY 2016		FY 2017	FY 2018
		Actual	**Actual**	**Actual**	**Actual**	**Actual**	**Target**	**Actual**	**Target**	**Target**
Performance Measure	Restitutions/Recoveries/Fines ($000) • Intellectual Property Rights Violations • Public Corruption • White Collar Crimes (all other)	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	705,289 12,051,979	N/A N/A N/A	N/A 391,570 6,814,479	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)	81 969 3,384	N/A 924 3,529	N/A 1,038 2,958	N/A 1,087 2,695	N/A 583 2,564	N/A N/A N/A	N/A 918 2,274	N/A N/A N/A	N/A N/A N/A
Performance Measure	Number of Criminal Organizations Engaging in White Collar Crimes Dismantled	368	409	458	464	416	400	302	400	400
Efficiency Measure	% of Major Mortgage Fraud Investigations to all pending Mortgage Fraud investigations	71%	71%	72%	73%	74%	74%	74%	74%	74%
Performance Measure	Number of convictions for Internet fraud	27	21	22	12	19	N/A	9	N/A	N/A
Performance Measure	Number of high-impact Internet fraud targets neutralized	11	23	17	25	23	17	N/A	17	17
Performance Measure	Convictions/Pre-Trial Diversions: • Organized Criminal Enterprises • Gang/Criminal Enterprises • Crimes Against Children • Civil Rights	812 N/A 338 268	845 6,467 373 227	833 N/A 1,312 238	723 7,338 1,570 205	1,455 2,445 1,401 56	1,400 N/A 1,600 N/A	2,799 2,580 1,450 185	1400 N/A 1,600 N/A	1,400 N/A 1,600 N/A
Efficiency Measure	% of FBI OCDETF Investigations with links to CPOT-linked DTOs **[Discontinued Measure]**	16.35%	19%	20%	20%	22%	N/A	N/A	N/A	N/A
Performance Measure	CPOT-Linked DTOs • Disruptions • Dismantlements	54 22	64 30	139 40	150 31	136 34	50 20	80 23	50 20	50 20
Performance Measure	Number of Organized Criminal Enterprise Dismantlements	39	47	70	82	120	160	148	160	160
Performance Measure	Number of Gang/Criminal Enterprise Dismantlements	165	163	251	167	153	150	123	124	124
Performance Measure	Number of Agents serving on Violent Crime Task Forces	1,050	1,071	1,131	1,121	1,146	N/A	1,824	N/A	N/A

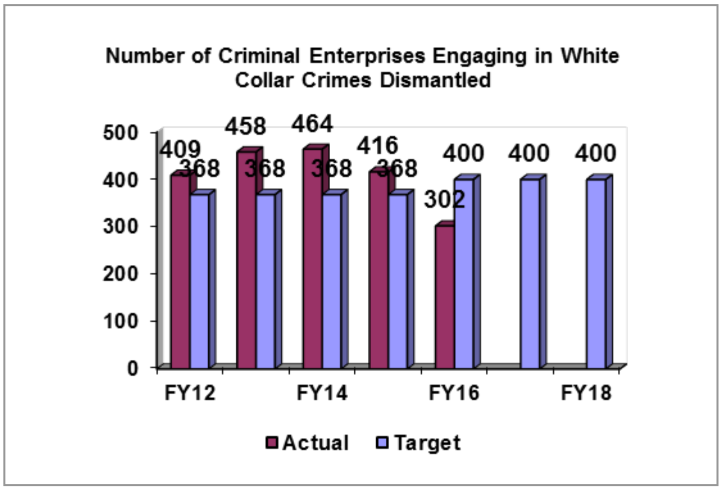
3. Performance, Resources, and Strategies

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.

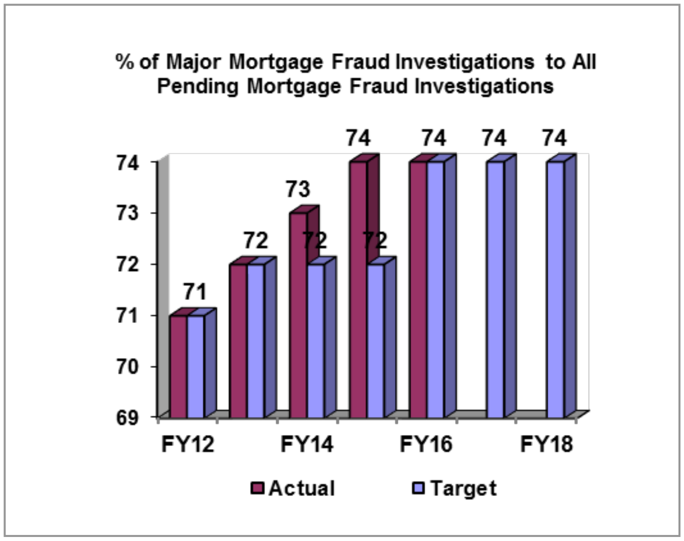
Performance Measure: Number of criminal organizations engaging in white collar crimes dismantled



FY 2016 Actual: 302
FY 2017 Target: 400
FY 2018 Target: 400

Discussion: 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 2016 Actual: 74%
FY 2017 Target: 74%
FY 2018 Target: 74%

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. 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 2018, 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, all of which 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.

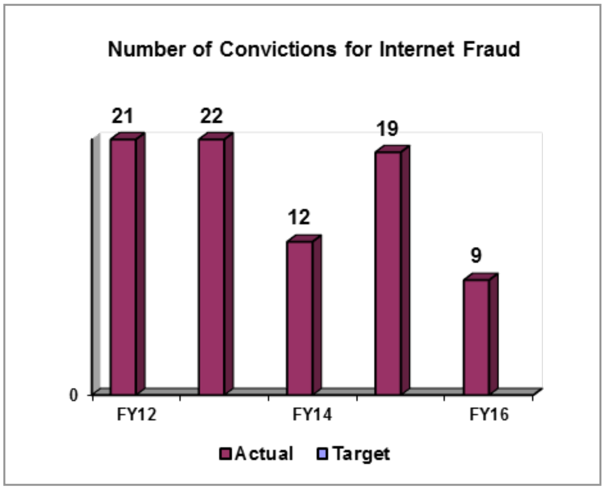
Internet Fraud

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 2018 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. As of April 2017, the FBI has already nearly doubled its FY 2016 number of internet fraud convictions.

Gangs, Organized Criminal Enterprises, and Consolidated Priority Organization Targets

The following sections discuss some of the issues, strategies, and performance measures associated with the president's recent Enforcing Federal Law with Respect to Transnational Organized Criminal Organizations and Preventing International Trafficking *and* Enhancing Public Safety in the Interior of the United States *executive orders, which fall under this DU.*

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 violent activity of MS-13 has prompted an FBI initiative that will assure extensive coordination among 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). SOD/OSG 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 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

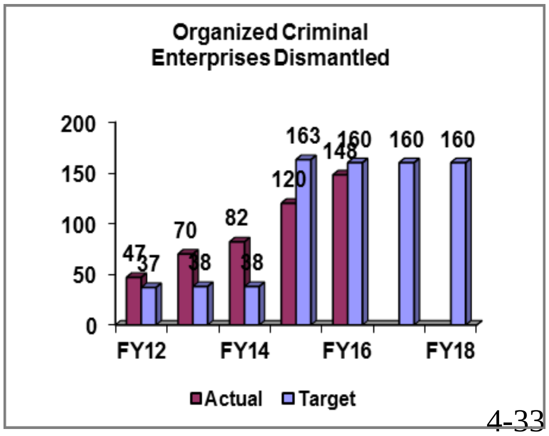
Organized Criminal Enterprises

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 2016 Actual: 148
FY 2017 Target: 160
FY 2018 Target: 160

Discussion: Based on National Intelligence Estimates (NIEs) and other factors that gauge threats



[3] https://www.justice.gov/criminal-ocgs/about-violent-gangs/

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

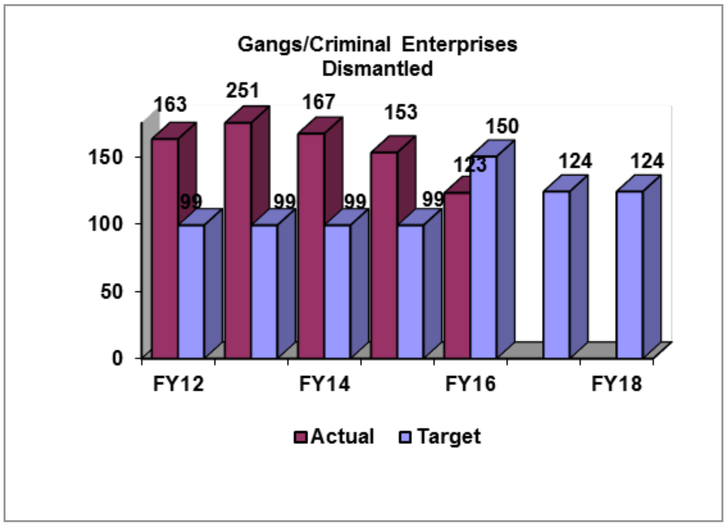
The mission of the FBI's Gang/Criminal Enterprise Program is to disrupt and dismantle the domestic cells (local, regional, national, and transnational) of criminal enterprises, which pose the greatest threat to the economic and national security of the U.S. Many of these criminal enterprises have ties 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 SOD/OSG focuses on enhancing gang investigations of all federal agencies by acting as a deconfliction and case coordination center. SOD/OSG 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 2016 Actual: 123
FY 2017 Target: 150
FY 2018 Target: 124



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)
2016 Enacted	2,226	2,025	480,624
2017 Continuing Resolution	2,237	2,122	492,723
Adjustment to Base and Technical Adjustments*	(193)	(175)	1,656
2018 Current Services**	2,044	1,947	494,379
2018 Program Increases	85	85	17,474
2018 Request	2,129	2,032	$511,852
Total Change 2017-2018	**(108)**	**(90)**	**19,129**

* reflects elimination of funded/unfilled positions and FTE with corresponding amounts and inflationary adjustments for funded/filled positions and FTE
** represents projected onboard positions/FTE as of pay period #1, FY 2018

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
- A prorated share of resources from the FBI's operational 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, 7 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. In FY 2016, approximately 80 million fingerprint checks were processed. Additionally, at the close of FY 2016, the Unsolved Latent File (ULF) contained approximately 704,000 records against which incoming fingerprint checks were searched. The ULF contains latent (finger and palm) prints that have searched against the legacy Integrated Automated Fingerprint Identification System (IAFIS) and/or NGI System but remain unidentified. There are approximately 710,000 records on file relating to active criminal and terrorism investigations – many of which were obtained from Improvised Explosive Devices and other materials by the Department of Defense and the FBI’s Terrorist Explosive Device Analytical Center. In the legacy IAFIS, only newly established criminal events performed a cascaded or reverse search against the ULF to identify new suspects within unsolved investigations. The NGI System cascades nearly all incoming biometric events (criminal, select civil, and investigative) against the ULF, which has significantly increased the identification of suspects within major investigations.

In FY 2013, NGI added the National Palm Print System containing over 20 million images, and the Interstate Photo System (IPS), as well as new services, such as rapid mobile searches, facial recognition, and Rap Back. The IPS, through Facial Recognition, now provides ways to search over 26 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.

In September 2014, the NGI Rap Back Services were deployed with the implementation of the NGI Increment 4. There are two domains within the NGI Rap Back Services: Noncriminal Justice (NCJ) and Criminal Justice (CJ). The NGI NCJ Rap Back Service is designed to assist local, state, and federal agencies in the continuous vetting of individuals in a position of trust. Once the initial fingerprint is retained in the NGI System and a Rap Back Subscription is set on the NGI Identity, if there is any activity on the identity history for that individual subscribed, the Submitter will immediately be notified. In essence, it alleviates the re-fingerprinting of an individual for the same position over a period of time. The NGI CJ Rap Back Service is designed to provide immediate notifications to law enforcement on an NGI Identity of subscribed individuals currently under an active criminal investigation, active probation, or parole (custody and supervision).

Currently, two of the largest submitting agencies include the State of Utah and the Transportation Security Administration. Utah has enrolled 123,640 Rap Back Subscriptions to include teachers, nurses, and EMS workers. The TSA has enrolled over 74,000 Rap Back subscriptions from numerous airports and airlines throughout the United States.

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.

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 99.74% 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 million active records and processes an average of 14.6 million transactions a day. On November 30, 2016, NCIC processed a record 17.6 million transactions with an average response time of less than .0249 seconds. In FY 2016, NCIC processed over 5.1 billion transactions.

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 goal of N3G 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.

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.

The Initial Operational Capability of the New NICS was deployed on August 9, 2016. The New NICS delivered updated capabilities, additional flexibility to make systematic and business changes, 24/7 system capability and greater operational efficiencies such as immediate denials of transactions with algorithm scoring 100 against NICS Indices records. The IT Architecture has been upgraded to include a total redesign and refresh of the NICS hardware and software. Since the deployment of the Initial Operating Capability, the NICS Section along with IT support have been focused on system stability and system enhancements. The schedule for the Full Operational Capability (FOC) development will begin in June 2018 and will utilize the agile development framework. The FOC development contract will end December 2018. The FOC is highlighted by technical functionality such as computer telephony integration capabilities and increased automation of operational processes.

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. The FBI UCR Program has two types of collections — Summary Reporting System (SRS) and the National Incident-Based Reporting System (NIBRS). Information derived from the data collected within the UCR Program is the basis for the annual publications Crime in the United States (which includes cargo theft and federal reporting), Law Enforcement Officers Killed and Assaulted (LEOKA), Hate Crime Statistics, and National Incident-Based Reporting System. 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. These publications also fulfill the FBI's obligations under Title 28, United States Code, Section 534.

The CJIS Division has chartered the FBI's New UCR Project to manage the acquisition, development, and integration of a new and improved crime data collection system. The stated goal for this project is to improve the accuracy and timeliness of the crime data collection and delivery process. The New UCR System was moved from a development status to Initial Operating Capability in January 2017.

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" and it is on track to be published in 2017. This study, which began in March 2013, focused on felonious killings and assaults of law enforcement officers during ambush and unprovoked attack situations. The findings from 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, and to expand the depth and breadth of data collected. As a Director's Priority Initiative, this effort will be achieved through the completion of a five prong approach. Prong One is to transition local, state, and tribal law enforcement agencies (LEAs) from the SRS to the NIBRS. The FBI seeks to sunset the SRS and replaces it with the NIBRS as the national standard for crime reporting by January 1, 2021. Prong Two is to develop a National Use-of-Force Data Collection to encompass all non-fatal/fatal police officer-involved incidents at the local, state, tribal, and federal levels. 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. Prong Five is to develop technical efforts to ensure crime data is accessible and timely.

In 2016, 6,270 agencies (approximately 29.5% of population covered of all UCR agencies) reported crime to the FBI UCR Program using the NIBRS Technical Specification. The UCR Program is actively working to increase NIBRS participation by partnering with the Bureau of Justice Statistics on the National Crime Statistics Exchange, working with advocacy groups to emphasize the importance of NIBRS data for the public and the law enforcement community, and transitioning the UCR Program to a NIBRS only data collection within five years.

National Data Exchange (N-DEx): The FBI's N-DEx System is an unclassified national information sharing system that enables criminal justice agencies to search, link, analyze, and share local, state, tribal, and federal records across jurisdictional boundaries. The N-DEx System contains incident, arrest, and booking reports; pretrial investigations; supervised released reports; calls for service; photos; and field contact/identification records.

By using the N-DEx System 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 System connects many regional and local information-sharing systems and leverages their collective power to provide access to millions of records. The N-DEx System 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 System contains over 332 million records from nearly 6,000 criminal justice agencies. Additionally, the N-DEx System provides access to an additional 292 million records from the Department of Homeland Security, the Interstate Identification Index, the NCIC and INTERPOL. N-DEx System records contain information on more than 2.5 billion entities (persons, places, things, and events).

Law Enforcement Enterprise Portal (LEEP): The FBI's LEEP is a gateway for thousands of users in the criminal justice, intelligence, and military communities to gain access to critical data protected at Controlled Unclassified Information level in one centralized location. With one click, users can securely access national security, public safety, and terrorism information contained within dozens of federal information systems, including: cyber-crime investigative resources; situational awareness tools; nationwide criminal justice records; national gang information; training tools; secure file sharing;

national security and suspicious activity reporting data; geo-spatial tools; as well as tools to report crime statistics and police data. Consistent with the National Strategy for Information Sharing and Safeguarding, LEEP also connects users to other federations serving the United States Intelligence Community, the criminal intelligence community, and homeland security community. LEEP gives users the ability to transfer and use information efficiently and effectively in a consistent manner across multiple organizations and systems to accomplish operational goals.

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).

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, TEDAC was formally designated 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.

Training Division

In addition to training FBI agents, the FBI provides instruction for state and locals, 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 2016, there were 804 state and local law enforcement officers, and 92 international law enforcement officers that participated in the National Academy program at the FBI Academy in Quantico, Virginia. In FY 2017, is the FBI estimates that 940 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.

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.

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

WORKLOAD/ RESOURCES	Target	Actual	Projected	Changes	Requested (Total)
	FY 2016	FY 2016	FY 2017	Current Services Adjustments & FY 2018 Program Changes	FY 2018 Request
Fingerprint background checks	83,743,292	80,102,358	83,092,857	4,491,666	87,584,523
NCIC transactions	4,946,550,400	5,173,388,482	5,292,808,928	370,496,625	5,663,305,553
Total number of federal, state, and local investigations aided by the Combined DNA Index System (CODIS)	†	40,307	†	†	†
Total number of forensic and offender matches identified at CODIS	†	42,474	†	†	†

Total Costs and FTE	FTE	$000	FTE	$000	FTE	$000	FTE	$000	FTE	$000
	2,025	480,624	2,025	480,624	2,122	492,723	(90)	19,129	2,032	$511,852

TYPE	PERFORMANCE	FY 2016	FY 2016	FY 2017	Current Services Adjustments & FY 2018 Program Changes	FY 2018 Request
Efficiency Measures	**NGI:** % of fingerprint checks: Criminal: • Completed w/in 2 hours Civil: • Completed w/in 24 hours	95.00% 95.00%	99.43% 99.21%	97.00% 97.00%	… …	97.00% 97.00%
Performance Measure	**RISC Searches Response Time:** Average NGI response time of RISC rapid searches	<10 seconds	3.98 seconds	<10 seconds	…	<10 seconds
Performance Measure	**NCIC:** • System availability • Downtime in minutes	99.50% 2,268	99.82% 1,006	99.50% 2,268	… …	99.50% 2,268
Performance Measure	**NICS:** % of NICS system availability	98.00%	99.62%	98.00%	…	98.00%
Performance Measure	**NICS:** % of NICS checks with an Immediate Determination	90.00%	89.70%	90.00%	…	90.00%

2. PERFORMANCE/RESOURCES TABLE

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	12 days	30 days	…	30 days
Performance Measure	Student-weeks of Instruction at the Hazardous Devices School (HDS)	2,350	2,284	2,500	572	3,072
Performance Measure	**N-DEx:** Percentage of population covered by N-DEx via state and local law enforcement participation MEASURE DISCONTINUED	N/A	NA	N/A	N/A	N/A
Performance Measure	**N-DEx:** Increase in the number of N-DEx system searches – cumulative total of 5 million for FY	5,000,000	7,243,140	7,500,000	…	7,500,000
Performance Measure	**N-DEx: [New Measure for FY 2015]** Annual percentage increase of agencies submitting data to N-DEx MEASURE DISCONTINUED	N/A	N/A	NA	N/A	NA
Performance Measure	**LEO:** Number of VCC new events boards open	848	941	848	…	848
Performance Measure	**LEO:** Number of identity or service providers on-boarded to the Law Enforcement Enterprise Portal (LEEP)	10	14	5	…	5

Data Definition, Validation, Verification, and Limitations:

- 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.
- **In** September 2014, the FBI replaced the Integrated Automated Fingerprint Identification System (IAFIS) fingerprint and criminal history system with the Next Generation Identification (NGI) system, and trends in efficiency and performance measures should be analyzed accordingly.

Performance Report and Performance Plan Targets		FY 2011	FY 2012	FY 2013	FY 2014	FY 2015	FY 2016		FY 2017	FY 2018
		Actual	Actual	Actual	Actual	Actual	Target	Actual	Target	Target
Efficiency Measures	**NGI:** % of 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% 99.34%	98.00% 97.00%	95.00% 95.00%	99.43% 99.21%	97.00% 97.00%	97.00% 97.00%
Performance Measure	**RISC Searches Response Time:** Average NGI response time of RISC rapid searches	N/A	N/A	N/A	4.2 seconds	3.94 seconds	<10 seconds	3.98 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 42s55m24 s	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	NA NA NA NA	N/A N/A N/A N/A	N/A N/A N/A N/A	N/A N/A N/A N/A	N/A N/A N/A N/A
Performance Measure	**NICS:** % of NICS checks with an Immediate Determination	91. 40%	91.72%	91.64%	91.00%	90.40%	90.00%	89.70%	90.00%	90.00%
Performance Measure	**NICS:** % of NICS system availability	N/A	99.93%	99.81%	99.00%	99.70%	98.00%	99.62%	98.00%	98.00%
Performance Measure	**NCIC:** • System availability • Downtime in minutes	99.76% 1,273	99.75% 1,351	99.81% 1,000	99.50% 1,440	99.80% 1,287	99. 50% 2,268	99. 82% 1,006	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	13 days	30 days	12 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	5,000,000	7,243,140	5,000,000	5,000,000
Performance Measure	**N-DEx:** Percentage of population covered by N-DEx via state and local law enforcement participation MEASURE DISCONTINUED	35.30%	50.00%	54.00%	68.00%	N/A	N/A	N/A	N/A	N/A
Performance Measure	**N-DEx:** Annual percentage increase of agencies submitting data to N-DEx MEASURE DISCONTINUED	N/A	N/A	N/A	N/A	6%	N/A	N/A	N/A	N/A
Performance	**LEO:**	N/A	N/A	2,167	1,500	1,222	848	941	848	848

Measure	Number of VCC new events boards open									
Performance Measure	**LEO:** Number of identity or service providers on-boarded to the Law Enforcement Enterprise Portal (LEEP)	N/A	N/A	NA	15	10	10	14	5	5
Performance Measure	Student-weeks of Instruction at the Hazardous Devices School (HDS)	2,295	2,052	2,024	1,848	2,286	2,350	2,284	2,500	3,072

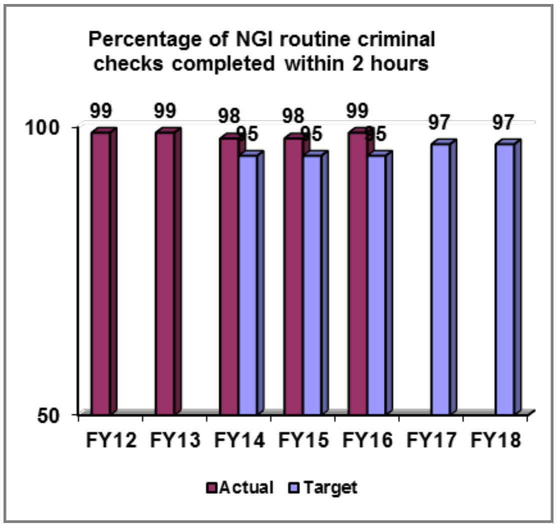
3. Performance, Resources, and Strategies

a. Performance Plan and Report for Outcomes

Next Generation Identification

Performance Measure: Percentage of criminal fingerprint checks completed within 2 hours

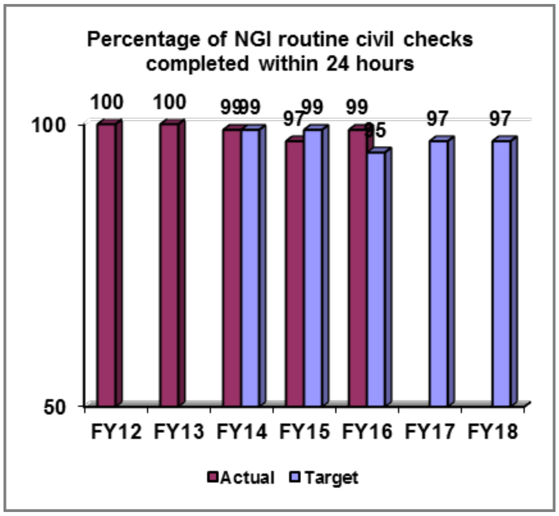
FY 2016 Actual: 99.43%
FY 2017 Target: 97.00%
FY 2018 Target: 97.00%



Discussion: On July 28, 1999, the FBI launched the Integrated Automated Fingerprint Identification System (IAFIS), a national fingerprint and criminal history system that provided automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses, 24 hours a day, 365 days a year. The FBI replaced all IAFIS segments in September 2014 with the NGI system, which expanded and significantly enhanced the FBI's biometric identification capabilities and provides the criminal justice community with the world's largest and most efficient electronic repository of biometric and criminal history information. NGI provides timely and accurate identification services in a paperless environment 24 hours a day, 7 days a week.

Performance Measure: Percentage of civil fingerprint checks completed within 24 hours

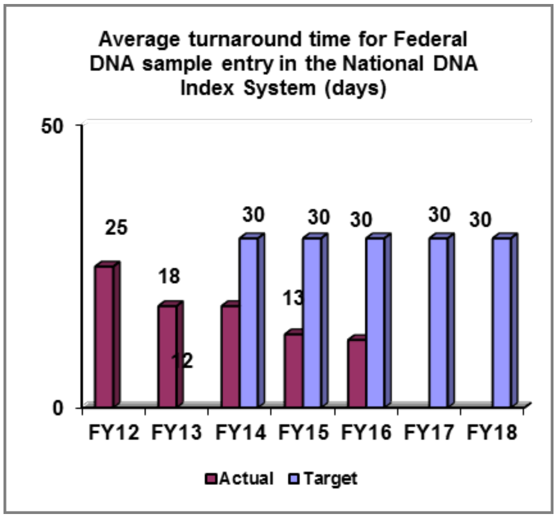
FY 2016 Actual: 99.21%
FY 2017 Target: 97.00%
FY 2018 Target: 97.00%



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 2016 Actual: 12 days
FY 2017 Target: 30 days
FY 2018 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 samples requiring analysis, the Federal DNA Database (FDD) Program consistently (1) implements process improvements in how samples are analyzed/reworked to increase efficiency, and (2) specifically monitors the turnaround time of samples that require analysis/re-analysis. In FY 2016, the FDD program significantly exceeded its target of an average 30-day turnaround time for sample processing/upload by achieving a 12-day average turnaround time on first run samples.

Law Enforcement National Data Exchange (N-DEx)

The FBI's N-DEx System is an unclassified national information sharing system that enables criminal justice agencies to search, link, analyze, and share local, state, tribal, and federal records across jurisdictional boundaries. The N-DEx System contains incident, arrest, and booking reports; pretrial investigations; supervised released reports; calls for service; photos; and field contact/identification records.

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

Discussion: The FBI proposes to discontinue this measure in favor of the measure "Increase in the number of N-DEx System searches."

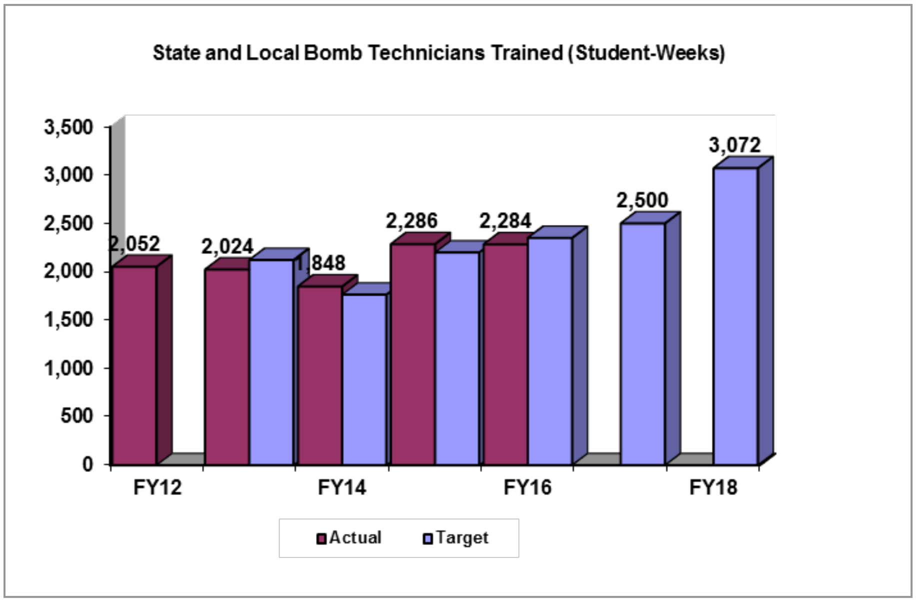
Performance Measure: Increase in the number of N-DEx System searches

FY 2016 Actual: 7,243,140
FY 2017 Target: 7,500,000
FY 2018 Target: 7,500,000

Discussion: This measure is projected based on the number of searches performed over the past two fiscal years and takes into account the new partnership with RISS and ongoing collaboration with LInX.

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 2016 Actual: 2,284
FY 2017 Target: 2,500
FY 2018 Target: 3,072

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.

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.

V. Program Increases

Item Name: **Cyber**

Budget Decision Unit(s): All

Organizational Program: Cyber, Operational Technology

Program Increase: Positions 36 Agt 20 FTE 36 Dollars $41,474,000 ($37,694,000 non-personnel)

Description of Item

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

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

Budget Decision Unit(s): Counterterrorism/Counterintelligence/ Intelligence

Organizational Program: Counterintelligence

Program Increase: Positions 93 Agt 50 FTE 93 Dollars $19,727,000 ($9,962,000 non-personnel)

Description of Item

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

Item Name: **Going Dark**

Budget Decision Unit(s): Intelligence, Counterterrorism/Counterintelligence, Criminal Enterprises Federal Crimes

Organizational Program: Operational Technology

Program Increase: Positions 80 Agt 20 FTE 80 Dollars $21,636,000 ($13,236,000 non-personnel)

Description of Item

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

Item Name: **Transnational Organized Crime**

Budget Decision Unit(s): Criminal Enterprises Federal Crimes, Intelligence

Organizational Program: Criminal Investigative

Program Increase: Positions 65 Agt 40 FTE 65 Dollars $6,779,000 (all personnel)

Description of Item

The FBI requests 65 positions (40 Special Agents) and $6,779,000 (all personnel) to address transnational organized criminal threats to the United States.

The FBI's transnational organized crime (TOC) program aims to thwart transnational criminal organizations (TCOs) affecting the United States by targeting their infrastructures, depriving them of their enabling means, and preventing their facilitation. This program is managed by the FBI's Criminal Investigative Division, but TOC cases are investigated using all intelligence tools at the FBI's disposal, including those of the United States Intelligence Community (USIC) and both foreign and domestic law enforcement partners.

Threat Summary

Today, the threat posed by TOC is broader and more complex than ever, as crime syndicates in both the eastern and western hemispheres operate multi-national, multi-billion dollar schemes from start to finish. With the expansion of the Internet, the federal government—and specifically the FBI—requires increased resources to mitigate the TOC threat.

Although many of these TCOs may be based overseas, they also operate throughout the United States, and the threats—both criminal and national security—they pose to our country are real. These organizations threaten the safety of American citizens and the security of our nation through a variety of means, including drug trafficking, violence, terrorism, corruption, alien smuggling, human trafficking, extortion, kidnapping, weapons trafficking, complex financial crimes, and public corruption.

As the lead federal agency for many of these violations, often the FBI is best equipped to investigate the violations posed by—and ultimately disrupt and dismantle—TCOs.

Justification

TOC-Western Hemisphere (TOC-W)
The FBI regards transnational organized crime in the western hemisphere (WH) as one of its top priorities, with a heavy emphasis toward Mexico-based threat actors. As a law enforcement agency with both a national security and an intelligence mission, the FBI's TOC-W program focuses on WH TCOs that use the U.S. as a destination or platform for their criminal activities.

Although the FBI does not open drug cases, the organization's broader strategy to counter TOC does have a drug nexus. Due to the continued threat emanating from the WH TCOs along the southwest border, investigations initiated to focus on the heroin and fentanyl problem set continues to rise. With the escalating overdose statistics released by the Center for Disease Control for 2015, the long-term strategy to disrupt the supply chains directing heroin to the U.S. poses a significant challenge. The FBI's 28 current TOC task forces consist of 118 task force officers with an overall operating budget of approximately $2 million; High Intensity Drug Trafficking Areas (HIDTA) funding and Organized Crime Drug Enforcement Task Forces (OCDETF) funding contribute to this program.

In an effort to maximize the personnel resources dedicated to address the TOC threat, the FBI partners with the Drug Enforcement Administration (DEA) and the Department of Homeland Security (DHS)/Homeland Security Investigations (HSI), the Department of Defense, USIC members, and foreign law enforcement partners via the Joint Interagency Task Force-South (JIATF-S), which detects and monitors illicit trafficking in the air and maritime domains to facilitate international and interagency interdiction and apprehension for U.S. prosecution.

For example, in the first quarter of FY 2017, JIATF-S was responsible for 10,673 kilograms of illicit contraband disrupted/seized, 69 maritime interdictions of illicit trafficking vessels, 53 arrests of foreign TCO actors brought back to the US for prosecution, and 18 arrests of foreign TCO actors by partner nations.

Currently, the FBI staffs eight assistant legal attaché (ALAT) positions in Mexico, four of which are assigned in close proximity to the southwest border, dedicated solely to address international threats to U.S. security. Additionally, border liaison officers (BLO) are assigned along the U.S. side of the southwest border to address a range of criminal matters engaged in by Mexican citizens whose crimes have links with U.S.-based investigations. ALATs and BLOs often coordinate with their liaison contacts to coordinate the rescue and return of U.S. citizens who have been kidnapped, as well as U.S. fugitives captured in Mexico.

TOC-W also staffs ALAT positions in Central America (Panama and Honduras), Colombia, and the Dominican Republic. The ALATS in these countries work with their foreign partners and actively work U.S.-based narcotics and money laundering investigations that target TOC organizations in the Americas with a nexus to the United States. The Colombian and Dominican Republic ALATs coordinate drug enforcement operations on a weekly basis.

To successfully mitigate the threat posed by transnational criminal organizations, the FBI requests staffing in order to identify, disrupt, and dismantle TCOs impacting the U.S.

TOC-Eastern Hemisphere (TOC-E)

The Internet has fundamentally changed the way TOC groups traffic drugs such as fentanyl, cocaine, and heroin, as well as how they victimize U.S. citizens through online fraud. Further, due to the anonymity and encryption enabled by the DarkNet and The Onion Router (TOR) Hidden Services, it is more difficult for criminal law enforcement officers to target the transnational criminal enterprises operating on this technical infrastructure. TOR is an open-source Internet network consisting of volunteer relays from around the world designed to obfuscate the location of infrastructure and people's online activity. Resources in this area will assist the FBI in proactively marrying online investigative techniques to traditional organized crime investigative techniques to effectively identify and target international drug trafficking organizations that are using the DarkNet to advertise, sell, and subsequently ship drugs into the U.S.

With the rise of substance abuse and the increase in drug advertisements on the DarkNet, a more proactive approach to targeting TCOs trafficking fentanyl, cocaine, and heroin on the DarkNet is warranted. This approach will include developing and leading a long-term strategy to infiltrate and strategically dismantle the transnational criminal networks operating on the DarkNet.

TOC-E staffs ALAT positions in Budapest, Prague, The Hague, Bucharest, Dubai, and Tokyo. Of these offices, the ALATs in Budapest and Prague work on task forces directly with host government authorities investigating cases of mutual interest. These task forces have been critical to developing sources, participating in sophisticated investigative techniques and predicating cases.

Without the requested positions, the FBI's ability to expand, or even maintain, its transnational organized criminal investigations into the DarkNet and other criminality facilitated by the Internet will be severely impacted. In addition, the ability to expand source bases and investigative reach with international partners will suffer.

The Top Gear investigation was based on information that an organized crime group operating in Washington, D.C., was involved in the use of counterfeit identification documents. The investigation targeted a Eurasian, Balkan, and Middle Eastern criminal enterprise involved in Internet-based auto auction fraud, business email compromise, drug trafficking, bank fraud, wire fraud, and money laundering. The TCO operates in Hungary, Israel, Romania, Poland, Slovakia, Czech Republic, The Netherlands, Germany, Turkey, and the United States. To date, the case has resulted in 35 arrests based on US warrants and an additional 22 arrests based on warrants in Israel. Over $60 million in transactions were interdicted. The case required cooperation from multiple international law enforcement agencies. Critical to the investigation was the ability to track online frauds and money flows. Yet this case only scratches the surface of the deeper level criminality occurring on the DarkNet.

Operation Hyperion was initiated to increase collaboration among domestic and international partners to collectively target illicit activity occurring on the DarkNet. During Operation Hyperion, federal agents from the FBI made contact with over 160 individuals around the country suspected of purchasing illicit items from various DarkNet marketplaces. Some of these individuals confessed to ordering a range of dangerous illegal narcotics, including heroin, opium, MDMA, methamphetamines, LSD, ecstasy, and cocaine. The FBI is employing a myriad of investigative techniques to target those facilitating supposedly anonymous illegal deals on DarkNet marketplaces.

Impact on Performance

This request of 65 positions will allow the FBI to continue its work toward disrupting—with the end goal of dismantling—the most culpable and high ranking TOC syndicates, especially those at the southwest border. Without these positions and this funding, the FBI's ability to maintain a robust pursuit to combat the highest-level TOC actors impacting the U.S. via the southwest border will be severely degraded.

These positions are required in order for the FBI to have the ability to adhere to the recent *Enforcing Federal Law with Respect to Transnational Organized Criminal Organizations and Preventing International Trafficking* and *Enhancing Public Safety in the Interior of the United States* executive orders.

Funding

Base Funding

FY 2016 Enacted				FY 2017 Continuing Resolution				FY 2018 Current Services			
Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)
1,109	642	1,094	$187,636	1,195	697	1,154	$194,036	1,110	640	1,069	$192,918

Personnel Increase Cost Summary

Type of Position	Modular Cost per Position ($000)	Number of Positions Requested	FY 2018 Request ($000)	FY 2019 Net Annualization (change from 2018) ($000)	FY 2020 Net Annualization (change from 2019) ($000)
Special Agent	$105	40	$4,200	$…	$…
Professional Staff	$105	25	2,625	…	…
Total Personnel		65	$6,779**	$…	$…

**Numbers do not sum correctly due to rounding in average position cost calculation.

Total Request for this Item

	Pos	Agt	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2019 Net Annualization (change from 2018) ($000)	FY 2020 Net Annualization (change from 2019) ($000)
Current Services	1,110	640	1,069	$182,082	$10,836	$192,918	$…	$…
Increase	65	40	65	6,779	…	6,779	$…	$…
Grand Total	1,175	680	1,134	$188,861	$10,836	$199,697	$…	$…

Item Name: **Physical Surveillance**

Budget Decision Unit(s): Counterterrorism/Counterintelligence

Organizational Program(s): Critical Incident Response

Program Increase: Positions 79 Agt … FTE 79 Dollars $8,242,000 (all personnel)

Description of Item

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

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

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 serves as a center for biometric research and development. The BTC houses the Biometric Center of Excellence, which coordinates biometrics research and development efforts for the FBI. The BTC also serves as an alternate Continuity of Operations Plan site for approximately 65 HQ personnel. Additionally, the BTC houses the DoD Biometrics Fusion Center, which is managed and funded by the DoD. The BTC provides 300,000 square feet for the FBI and 60,000 square feet for the DoD, housing approximately 2,000 personnel and facility administrative costs are shared between FBI and DOD accordingly.

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

Facility O&M - $4,442,000
The BTC O&M cost includes all aspects of operating and maintaining the physical facility, to include the following: 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 terms of the overall cost footprint of O&M associated with the BTC facility, 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. In terms of the overall cost footprint of O&M associated with IT at the BTC facility, CJIS User Fees will support $1,729,942 of the total requirement.

Justification

The construction of the main BTC facility and central plant expansion concluded in the Fall of 2015. The complete outfitting of the facility finished in Calendar Year 2016. Move in of both FBI and DOD personnel is ongoing and will conclude by the end of Calendar Year 2017.

BTC O&M funding is required to support the BTC facilities and IT requirements. Furthermore, the O&M funding will enable the BTC to prevent system or work stoppage and/or delays.

Impact on Performance

If the requested BTC building O&M funding is not received, the maintenance of the facility will be severely impacted, leading to shorter useful building life, potential life safety issues, and degraded working conditions.

Funding

Base Funding

FY 2016 Enacted				FY 2017 Enacted				FY 2018 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 2018 Request ($000)	FY 2019 Net Annualization (change from 2018) ($000)	FY 2020 Net Annualization (change from 2019) ($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 2019 Net Annualization (change from 2018) ($000)	FY 2020 Net Annualization (change from 2019) ($000)
Current Services	…	…	…	$…	$…	$…	$…	$…
Increases	…	…	…	…	7,375	7,375	…	…
Grand Total	…	…	…	$…	$7,375	$7,375	$…	$…

Item Name: **Violent and Gun-Related Crime Reduction Task Force**

Budget Decision Unit(s): Criminal Enterprises Federal Crimes, Intelligence

Organizational Program: Criminal Investigative

Program Increase: Positions 33 Agt 20 FTE 33 Dollars $3,450,000 (all personnel)

Description of Item

The FBI requests funding to support the president's February 9, 2017, *Task Force on Crime Reduction and Public Safety* executive order. The task force was created by the attorney general on February 28, 2017. The task force includes the Director of the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), the Administrator of the Drug Enforcement Administration (DEA), the Director of the Federal Bureau of Investigation (FBI), and the Director of the U.S. Marshals Service (USMS). The task force is central to the attorney general's commitment to combatting illegal immigration and violent crime, such as drug trafficking, gang violence, and gun crimes, and to restoring public safety to all of the nation's communities. Requested resources will support implementation of recommendations from the task force.

The FBI requests 33 positions (20 Special Agents) and $3,450,000 (all personnel) to fight the increasing violent crime threat across the United States.

Significant violent crimes can have a major impact on a community's sense of safety and quality of life. And although the FBI faces a myriad of national security threats, violent crime agents—and their intelligence analyst and professional staff colleagues—continue to protect Americans and investigate crimes in both big cities and small communities, giving those communities the sense of safety and high quality of life to which they have a right. The violent crime and gang program leads the FBI's effort in reducing violent crime and gang-related violence by identifying, prioritizing, targeting, investigating, and deterring the most violent and dangerous criminal offenders.

Threat Summary

The 2015 Uniform Crime Report (UCR) reports an upward tick in violent incident crimes affecting diverse communities across the United States. As a result, the FBI's criminal investigative program has experienced increased demand. In turn, the FBI's ability to support state and local law enforcement partners has also experienced high demand, which may compound the upward tick in violent crime. The FBI proposes to address the problem both by putting more agents on the streets of high-threat communities to deal with crimes that have already been committed and by supplementing its current professional staff cadre with additional personnel that can help the agents on the street identify threats before violent crimes are committed.

Justification

The Attorney General's Violent and Gun-Related Crime Reduction Task Force has a multi-agency focus on reducing violent and gun-related crime in particularly hard-hit urban areas by using innovative means to locate individuals, organizations, and gangs within specific high crime jurisdictions. Federal law enforcement, including the FBI, DEA, ATF, and USMS, will work with community leaders, educators, and local business owners to share information on identities, gang affiliation markers, and crime networking patterns with state and local law enforcement and members of the public. Resources will also provide for communications, surveillance and monitoring equipment, and dedicated tip-lines and rewards in select high crime areas–and provide community and individual incentives for reporting crime to ensure violent and gun-related crime reduction is sustained long-term.

The recent uptick in active shooter killings, killings in public places, gang violence, assaults/threats of federal officers/judges, fugitives, and law enforcement officer line-of-duty deaths has dramatically affected U.S. communities. From FY 2012 to FY 2016, the FBI's Violent Crime and Gang Program experienced a 27% increase in violent incident crime cases opened (4,495 in FY 2012 to 5,713 in FY 2016) and a 122% increase in violent incident arrests (3,930 in FY 2012 to 8,709 in FY 2016).

Despite a recent increase in federal and local violent crime, resources available to local police departments across the nation have not kept pace. This resource issue, combined with the Investigative Assistance for Violent Crimes Act of 2012 (IAVCA), culminates in an influx of requests from local law enforcement for FBI assistance in addressing violent crime. It is essential that the FBI appropriately address violent crime, protect the public, and ensure safe operations by law enforcement officers.

In the summer of 2016, the FBI Director met with chiefs of police and sheriffs from 18 major metropolitan cities/counties to discuss the rise in violent crime and strategize a joint local, state, and federal response. These cities represented diverse geographical areas and varying population sizes, yet have experienced similar upticks in violent crime. This supports FBI internal, FBI UCR, and DOJ Violence Reduction Network (VRN) empirical data demonstrating an uptick in violent crime.

Uniform Crime Report (UCR) Data
Increase Over 2014

Type of Violent Crime	2015 National Increase (%)
All	+3.9%
Murder/Non-Negligent Manslaughter	+10.8%
Rape	+6.3%
Aggravated Assault	+4.6%
Robbery	+1.4%

On many occasions while investigating violent crime matters, resources are leveraged from both the responding field office and from surrounding field offices and headquarters entities. On May 7, 2016, Dracy Clint Pendleton was stopped on a routine traffic stop by a Mahomet, Illinois police officer. Pendleton became combative, and the officer utilized a Taser in an attempt to gain compliance. Pendleton responded by brandishing a firearm and shooting the officer, who sustained non-life threatening injuries. Pendleton subsequently fled 230 miles south to a 280,000-acre, heavily-wooded national forest. FBI SWAT teams, investigative agents, and specialty personnel from five surrounding field offices, as well as the FBI's Hostage Rescue Team, joined the search to locate Pendleton. After days of searching, Pendleton was located on May 15, 2016, by an FBI SWAT team, where a shoot-out ensued, and Pendleton was killed. The FBI's Evidence Response Team then spent two days processing the crime scene. This violent crime investigation required a massive amount of specialized technical, tactical and investigatory expertise – which is illustrative of the unique nature of what the FBI brings to these types of investigations.

The FBI has a responsibility and statutory requirement to address violent crime—and especially the recent rise in violent crime—with its state and local partners. The violent crime program is also essential in developing working relationships in times of national crisis and critical incidents. Moreover, homeland and national security investigations also benefit from the resources allocated to the FBI's violent crime program. Terrorist acts, crime, and foreign intelligence activities are no longer distinct activities, but rather profound fluid enterprises that through their very existence have a reverberating impact on our national security. Terrorism and violent crime are inextricably linked. Terrorist organizations and their supporters engage in a myriad of crimes to fund and facilitate terrorist activities. These crimes include extortion, kidnapping, robbery, arms trafficking, money laundering and drug trafficking. For example, in January 2016, Edward Archer ambushed a Philadelphia police officer who was sitting in his patrol car. Archer claimed allegiance to ISIS, but was not a long-standing member. However, like most of those responsible for the attacks on police, Archer did have a violent criminal history.

It should be mentioned that the previous two examples involved criminals targeting law enforcement officers. A phenomenon that was virtually non-existent in 2012, 66 law enforcement officers were feloniously killed in 2016, representing a 61% increase over the 2015 total. The FBI must investigate incidents such as line-of-duty deaths and to adhere to the Administration's recent *Preventing Violence Against Federal, State, Tribal, and Local Law Enforcement Officers* executive order.

Empirical results routinely prove that a surge of resources to address a threat has a positive impact. Oakland is a good example of the accomplishments resulting from increased resources. Oakland had 126 homicides in 2012, which was greater than seven times the national average per 100,000 inhabitants. In 2013, the Oakland Police Department requested the assistance of the FBI's San Francisco office to address this chronic epidemic. FBI San Francisco surged five agents to address homicides with a federal nexus. In 2015, due in large part to task force efforts, homicides dropped by 34%, and the corresponding solution rate increased by 20%. However, surging has consequences, as it takes these agents away from working other violations investigated by the FBI.

Impact on Performance

As violent crime continues to plague American society, the FBI has an obligation to assume a leadership role in the nation's efforts to deter, investigate, and apprehend the most violent and dangerous criminal offenders who pose a threat to all segments of society. The resources requested here are a key part of that role.

Funding

Base Funding

FY 2016 Enacted				FY 2017 Continuing Resolution				FY 2018 Current Services			
Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)
2,922	1,763	2,898	$450,777	2,936	1,789	2,909	$486,824	2,903	1,769	2,876	$495,877

Personnel Increase Cost Summary

Type of Position	Modular Cost per Position ($000)	Number of Positions Requested	FY 2018 Request ($000)	FY 2019 Net Annualization (change from 2018) ($000)	FY 2020 Net Annualization (change from 2019) ($000)
Special Agent	105	20	$2,100	$…	$…
Professional Staff	105	13	1,300	…	…
Total Personnel		33	$3,450**	$…	$…

**Numbers do not sum correctly due to rounding in average position cost calculation.

Total Request for this Item

	Pos	Agt	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2019 Net Annualization (change from 2018) ($000)	FY 2020 Net Annualization (change from 2019) ($000)
Current Services	2903	1769	2876	$476,403	$19,474	$495,877	$…	$…
Increase	33	20	33	3,450	0	3,450	$…	$…
Grand Total	2934	1789	2909	$479,853	$19,474	$499,327	$…	$…

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

Budget Decision Unit(s): Criminal Justice Services

Organizational Program: Criminal Justice Information Services

Program Increase: Positions 85 Agt … FTE 85 Dollars $8,900,000 (all personnel)

Description of Item

The FBI requests 85 positions and $8,900,000 (all personnel) 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.

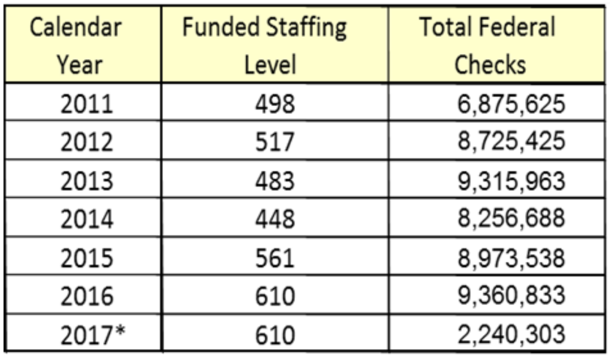
Justification

The NICS was established in 1993 by mandate of the Brady Handgun Violence Prevention Act (Brady Act) of 1993 and implemented in 1998. The Brady Act 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 may potentially be an individual prohibited from purchasing firearms. Since implementation, the NICS Section has conducted approximately 245 million NICS background checks. An average annual increase of 36.14 percent has taken place for federal check volume. Firearm background checks have increased from 8,725,425 in FY 2012, to 9,360,833 in FY 2016.

As of March 31, 2017, the NICS Section employs 610 staff members. A total of 434 members are dedicated to the NICS Operations Unit with the NICS Legal Instruments Examiner (NICS Examiner) job title. Of the 434 NICS Examiners, 61 are assigned to the Appeals Services Team and 16 are assigned to the NICS Command Center—and 357 NICS Examiners assigned to the Research and Analysis staff. The NICS staff is working at capacity and must be augmented with additional personnel to maintain production. The NICS Section has kept up with workload by offering significant amounts of overtime in FY 2016 and to date in FY 2017. Additional tools to combat the volume included surging all NICS Section non-NICS Examiners, recalling 43 CJIS Division employees to assist, cancellation of leave, and offering overtime during crucial workload volume peaks.

The NICS Section has determined by interviewing its employees that inadequate staffing, paired with the current volume of background checks, deprives the employees of the time needed to perform at a desirable level of accuracy. The NICS staff is working at capacity and must be augmented with additional personnel to maintain production. The NICS Section has kept up with workload by offering significant amounts of overtime in FY 2016 and to date in FY 2017. This cannot be sustained for long term without affecting the quality of work and employees' health. With additional staffing, the NICS Section believes it can conduct thorough examinations and follow-up research to make final determinations and closeout transactions while ensuring it maintains quality.

Transaction Volume from 2011-2017



Calendar Year	Funded Staffing Level	Total Federal Checks
2011	498	6,875,625
2012	517	8,725,425
2013	483	9,315,963
2014	448	8,256,688
2015	561	8,973,538
2016	610	9,360,833
2017*	610	2,240,303

*As of March 31, 2017

Impact on Performance

It is essential that the FBI maintain the requested 85 positions.

The requested personnel resources will allow the FBI to maintain 85 Legal Instrument Examiner positions. Without these personnel, the FBI's ability to effectively conduct the statutorily mandated firearm background checks conducted by the National Instant Criminal Background Check System (NICS) Section within the mandated three day timeframe could be compromised.

FBI staff enable CJIS to consistently provide timely and accurate determinations of individuals' eligibility to possess firearms and/or explosives in accordance with federal law. This decreases 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 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.

Funding

Base Funding

FY 2016 Enacted				FY 2017 CR				FY 2018 Current Services			
Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)
668	…	618	$81,059	666	…	653	$78,751	591	…	577	$70,344

Personnel Increase Cost Summary

Type of Position	Modular Cost per Position ($000)	Number of Positions Requested	FY 2018 Request ($000)	FY 2019 Net Annualization (change from 2018) ($000)	FY 2020 Net Annualization (change from 2019) ($000)
Professional Support	$...	85	$8,900	$...	$...
Total Personnel	$...	85	$8,900	$...	$...

Total Request for this Item

	Pos	Agt	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2019 Net Annualization (change from 2018) ($000)	FY 2020 Net Annualization (change from 2019) ($000)
Current Services	591	…	577	$52,715	$17,629	$70,344	$…	$…
Increases	85	…	85	$8,900	…	$8,900	…	…
Grand Total	676	…	662	$61,615	$17,629	$79,244	$…	$…

VII. 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 2018 request includes a total of $51.895 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 SWE Program ($49.895 million), as well as renovations at the FBI Academy in Quantico, VA ($2 million).

Appropriations Language and Analysis of Appropriations Language

Appropriations Language for Construction

For necessary expenses, to include the cost of equipment, furniture, and information technology requirements, related to construction or acquisition of buildings, facilities and sites by purchase, or as otherwise authorized by law; conversion, modification and extension of federally owned buildings; [and] preliminary planning and design of projects; *and operation and maintenance and development of secure work environment facilities and secure networking capabilities; $51,895,000,* [$308,982,000] to remain available until expended.

Analysis of Appropriations Language

- No substantive changes.

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

Budget Decision Unit(s): N/A

Organizational Program: Facilities and Logistics Services

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

The FBI's FY 2018 request includes a proposed $16,500,000 reduction to its SWE Program. As a national security and law enforcement agency, the FBI requires funding for its SWE Program to ensure its Field Offices, Resident Agencies, and Legats have the proper facilities and robust network and analytical tools to gather, store and analyze classified information and to share this information with its Intelligence Community partners. This funding ensures the FBI's classified information technology remains current and in compliance with IC standard and 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 SWE will allow the FBI to maintain its 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. The FBI will leverage prior-year balances when and where necessary to continue to ensure that its TS network is not put at risk.

Funding

Base Funding

FY 2016 Enacted				FY 2017 Continuing Resolution				FY 2018 Current Services			
Pos	Agt	FTE	($000)	Pos	Agt	FTE	($000)	Pos	Agt	FTE	($000)
…	…	…	$66,982	…	…	…	$66,982	…	…	…	$66,395

Non-Personnel Offset Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2018 Request ($000)	FY 2019 Net Annualization (change from 2018) ($000)	FY 2020 Net Annualization (change from 2019) ($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	…	…	…	$...	$66,395	$66,395	$...	$ …
Decreases	…	…	…	…	(16,500)	(16,500)	…	…
Grand Total	…	…	…	$...	$49,895	$49,895	$...	$ …

VIII. Glossary

ACE	Asian Criminal Enterprises
AFIT	Advanced Fingerprint Identification Technology
ALAT	Assistant Legal Attache
AML	Applications Mall
ASCLD-LAB	American Society of Crime Laboratory Directors - Laboratory Accreditation Board
ATB	Adjustment to Base
ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives
BAU III	Behavior Analysis Unit III
BCI	Border Corruption Initiative
BCTF	Border Corruption Task Force
BCWG	Border Corruption Working Group
BLO	Border Liaison Officer
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
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
DHS	Department of Homeland Security
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
HIDTA	High Intensity Drug Trafficking Area
HSI	Homeland Security Investigations
HUMINT	Human intelligence
IA	Intelligence Analysts
IAA/IdAM	Identity Authentication Authorization/Identity and Access Management
IAFIS	Integrated Automated Fingerprint Identification System
IAVCA	Investigative Assistance for Violent Crimes Act of 2012
IC	Intelligence Community
IC ITE	Intelligence Community Information Technology Enterprise
IC3	Internet Crime Complaint Center
ICC	Indian Country Crimes
ICE	Immigration and Customs Enforcement
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
JIATF-S	Joint Interagency Task Force- South
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
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
ONDCP	White House Office of National Drug Control Policy
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
SOG	Special Operations Group
SOS	Staff Operation Specialist
SSG	Special Surveillance Group
SSPP	Strategic Sustainability Performance Plan
SWAT	Special Weapons and Tactics
TCO	Transnational Criminal Organization
TEDAC	Terrorist Explosive Device Analytical Center
TFC	Threat Fusion Cells
TOC	Transnational Organized Crime
TOC-E	Transnational Organized Crime – Eastern Hemisphere
TOC-W	Transnational Organized Crime – Western Hemisphere
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
VCGS	Violent Crime and Gang Section
VCTS	Violent Criminal Threat Section
VGSSTF	Violent Gang Safe Streets Task Forces
VRN	DOJ Violence Reduction Network
WCC	White Collar Crime
WH	Western Hemisphere
WMD	Weapons of Mass Destruction
WMDD	Weapons of Mass Destruction Directorate
XTS	Exploitation Threat Section