U.S. Department of Justice
Federal Bureau of Investigation

FY 2019 Authorization and Budget Request to Congress

February 2018

Table of Contents

I. OVERVIEW FOR THE FEDERAL BUREAU OF INVESTIGATION

A. Introduction

Budget Request Summary: The Federal Bureau of Investigation's (FBI's) Fiscal Year (FY) 2019 budget request proposes a total of $8,923,975,000 in direct budget authority, of which $8,872,080,000 is for Salaries and Expenses (S&E) and $51,895,000 is for Construction.

The S&E request includes a total of 34,694 direct positions and 33,528 direct full time equivalents (FTE); the positions include:

- 12,927 Special Agents (SAs)
- 3,055 Intelligence Analysts (IAs)
- 18,712 Professional Staff (PS)

The FY 2019 Adjustments to Base (ATBs) include an overall reduction of 500 positions (175 SAs, 45 IAs) and an increase of $164.4 million for continual support of the FBI's base resource. This request does not include any program enhancements. The reduced position level reflects a Department-wide reduction of headquarters personnel as well as personnel adjustments based on resources provided.

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

Because no final 2018 appropriation bill has been enacted, a technical adjustment of $14,919,000 in S&E and a reduction of $365,430,000 in Construction is included to reflect the difference between the 2018 President's Budget and the annualized amounts provided in the Continuing Appropriations Act, 2018 (P.L. 115-56) (CR). Funding is included to sustain 1,625 positions funded in FY 2017 including Special Agents, Intelligence Analysts, Computer Scientists, Forensic Accountants, and surveillance professionals. These positions provide field support to ensure the FBI is able to appropriately address the current threat environment and protect the American people.

The request also includes balance offsets totaling $148,000,000 from Criminal Justice Information Services (CJIS) automation surcharge balances.

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 2019 budget request is a product of these assessments and provides the resources to aggressively continue the FBI's strategic vision into the future.

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

The FBI's Mission and Priorities:

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 358 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.

The FBI also operates 63 Legal Attaché (Legat) offices and 27 sub-offices in 75 countries around the world. These offices are typically staffed at fewer than 10 personnel to enable the FBI's presence in and liaise with a number of foreign countries and partners. 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 (NSB), which includes the Counterterrorism Division (CTD), Counterintelligence Division (CD), Terrorist Screening Center (TSC), and the Weapons of Mass Destruction Directorate (WMDD).
- The Intelligence Branch (IB), which includes the Directorate of Intelligence (DI) and the Office of Partner Engagement (OPE).
- The Criminal, Cyber, Response and Services Branch (CCRSB), which includes the Criminal Investigative Division (CID), the Cyber Division (CyD), the Critical Incident Response Group (CIRG), and the International Operations Division (IOD).
- The Science and Technology Branch (STB), which includes the Criminal Justice Information Services (CJIS) Division, the Laboratory Division (LD), and the Operational Technology Division (OTD).

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

- The Information and Technology Branch (ITB) oversees the IT Enterprise Services Division (ITESD), the IT Applications and Data Division (ITADD), and the IT Infrastructure Division (ITID).

- The Human Resources Branch (HRB) includes the Human Resources Division (HRD), the Training Division (TD), and the Security Division (SecD).
- Administrative and financial management support is provided by the Facilities and Logistics Services Division (FLSD), the Finance Division (FD), the Records Management Division (RMD), the Resource Planning Office (RPO), and the Inspection Division (InSD).
- Specialized support is provided directly to the Director and Deputy Director through a number of staff offices, including the Office of Public Affairs (OPA), the Office of Congressional Affairs (OCA), the Office of the General Counsel (OGC), the Office of Equal Employment Opportunity Affairs (OEEOA), the Office of Professional Responsibility (OPR), the Office of the Ombudsman, and the Office of Integrity and Compliance (OIC).

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 DI 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 LD, the International Operations Division, and the Operational Technology Division, are allocated to the decision units based on workload. For example, 21 percent of the LD's workload is in support of counterterrorism investigations and accordingly, 21 percent of the LD'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 the ITB, the FLSD, and the HRD 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. 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.

As of the end of FY 2017, 318 Americans traveled or attempted to travel to Syria to participate in the conflict.

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 Violence Reduction 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 FY 2017, the FBI's Office of Partner Engagement (OPE) produced two documentaries that identified possible extremist indicators and characteristics. These documentaries are being disseminated to local law enforcement communities and security professionals via FBI field divisions in furtherance of the engagement and prevention lines of effort.

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 businesspersons – as well as cyber-based tools to target, penetrate, and influence U.S. institutions.

Recent notable successes include the September 2017 sentencing of Gregory Allen Justice to five years in prison for selling sensitive information he stole from his employer to a person he believed to be an agent of the Russian intelligence service.

As a production engineer for a U.S. company's commercial and military satellites division since 2000, Justice's employment included work on satellites sold to the U.S. Air Force, U.S. Navy, and National

Aeronautics and Space Administration. Through his work, he had access to closely held trade secrets, including anti-jamming technology, encryption plans, and technical data.

In February 2016, Justice began meeting with an FBI undercover employee he believed to be a representative of a Russian intelligence service. During the meetings, Justice offered and subsequently provided to the undercover employee digital copies of more than 60 documents, which were both proprietary to his employer and controlled for export from the United States or to foreign persons subject to International Traffic in Arms Regulations. Justice sought and received $3,500 in exchange for the documents.

Following an investigation conducted jointly by the FBI and U.S. Air Force Office of Special Investigations, Justice was arrested in July 2016. He pleaded guilty in May 2017 to attempting to commit economic espionage and attempting to send restricted information out of the United States.

Another example includes the October 2017 sentencing of Lyudmila Bagdikian and Viktoria Klebanova to time served in prison, concluding the successful prosecution of eight members of an extensive and sophisticated procurement network that provided Russia with restricted, dual-use U.S. technology. The FBI's investigation into the network also resulted in the seizure of more than $1 million and the addition of 165 foreign individuals and companies to the U.S. Department of Commerce's Entity List.

The FBI's investigation revealed Alexander Fishenko, a dual U.S.-Russian citizen, led a conspiracy to ship at least $50 million worth of advanced microelectronics—many of which are frequently used in military systems for radar, surveillance, and missile guidance—to Russian military and intelligence agencies. A federal indictment charged Fishenko and seven other U.S.-based individuals, including Bagdikian and Klebanova, as well as two companies and three Russia-based individuals, with export violations, money laundering, obstruction of justice, and wire fraud. Fishenko was also charged with acting as an unregistered agent of the Russian Government. Following his guilty plea, Fishenko was sentenced in July 2016 to 10 years in prison—the longest sentence ever obtained by the U.S. Department of Justice for acting as an unregistered agent of a foreign government. Sentences for the other defendants ranged from time served to more than 11 years in prison.

The FBI's investigation ultimately halted Fishenko and his companies' criminal activities, disrupted the entire proliferation network, and degraded Russia's illicit technology transfer capabilities.

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

While these threats are not new, the means by which actors implement them are changing. Today, these actors engage via the Internet and other computer networks. These networks provide ample cover from attribution, making the identification of the intrusion difficult as the motive of the attacker – be it criminal, and terrorist or nation-state espionage – can remain unknown. Just as the Internet has enabled businesses to maximize profits by inexpensively connecting with millions of customers, it has also enabled threat actors to amplify their impacts by inexpensively attacking millions of victims. Despite formidable investments and concerted efforts by the private sector and government to build more secure and defensible computer networks, risks remain high and cybersecurity remains a rapidly growing concern with no easy solutions in sight.

The FBI's mission in cybersecurity is to counter the threat by investigating intrusions to determine criminal, terrorist, and nation-state actor identities, and engaging in activities to reduce or neutralize these threats. At the same time, the FBI collects and disseminates information significant to those responsible for defending networks, including information regarding threat actor targets and techniques. The FBI's jurisdiction is not defined by network boundaries; rather, it includes all territory governed by U.S. law, whether domestic or overseas, and spans individual citizens, private industry, critical infrastructure, U.S. government, and other interests alike. Collectively, the FBI and its federal partners take a whole-of-government approach to help deter future threats and bring closure to current threats that would otherwise continue to infiltrate and harm our network defenses.

In July 2017, DOJ announced the seizure of the largest criminal marketplace on the Internet, AlphaBay, which operated for over two years on the dark web and was used to sell deadly illegal drugs, stolen and fraudulent identification documents and access devices, counterfeit goods, malware and other computer hacking tools, firearms, and toxic chemicals throughout the world. This international operation to seize AlphaBay's infrastructure was led by the U.S. and involved cooperation and efforts by law enforcement authorities in Thailand, the Netherlands, Lithuania, Canada, the United Kingdom, and France, as well as the European law enforcement agency Europol.

According to publicly available information on **AlphaBay** (available prior to its takedown), one AlphaBay staff member claimed that it serviced **over 200,000 users and 40,000 vendors**. Around the time of takedown, there were **over 250,000** listings for illegal drugs and toxic chemicals on AlphaBay, and **over 100,000 listings** for stolen and fraudulent identification documents and access devices, counterfeit goods, malware and other computer hacking tools, firearms and fraudulent services. Comparatively, the **Silk Road** dark web marketplace, which was seized by law enforcement in November 2013, had reportedly **approximately 14,000 listings** for illicit goods and services at the time of seizure and was the largest dark web marketplace at the time.

On July 5, 2017, Alexandre Cazes aka Alpha02 and Admin, 25, a Canadian citizen residing in Thailand, was arrested by Thai authorities on behalf of the United States for his role as the creator and administrator of AlphaBay. On July 12, 2017, Cazes apparently took his own life while in custody in Thailand. Law enforcement authorities in the United States worked with numerous foreign partners to freeze and preserve millions of dollars' worth of cryptocurrencies that were the subject of forfeiture counts in the indictment, and that represent the proceeds of the AlphaBay organization's illegal activities.

***White Collar Crime*:** The White Collar Crime (WCC) program addresses the following principal threats:

Public Corruption	Public Corruption, which involves the corruption of local, state, and federally elected, appointed, or contracted officials, undermines our democratic institutions and threatens public safety and national security. Government fraud affects U.S. border security, neighborhood safety, judicial integrity, and public infrastructure quality such as schools and roads.
Border Corruption	The documented presence of corrupt border officials facilitates a wide range of illegal activities along the northern and southern borders. Resource-rich cartels and criminal enterprises employ a variety of methods to target and recruit U.S. Border Patrol Agents, Customs and Border Protection Officers, and local police officers who can facilitate criminal activity. Corrupt officials assist these entities

	by providing intelligence and contraband across these borders. To help address this threat, the FBI established the Border Corruption Initiative (BCI), which has developed a threat-tiered methodology, targeting border corruption in all land, air, and sea ports of entry to mitigate the threat posed to national security.
Corporate Fraud	As the lead agency investigating corporate fraud, the FBI focuses on cases involving complex accounting schemes, self-dealing corporate executives and obstruction of justice. The majority of these cases involve accounting schemes – deceiving investors, auditors and analysts about the true condition of a corporation. In addition to significant financial losses to investors, corporate fraud has the potential to cause immeasurable damage to the U.S. economy and investor confidence. Insider trading, which is a type of corporate fraud, continues to pose a serious threat to the U.S. financial markets. Through national-level coordination, the FBI strives to protect the fair and orderly operation of the U.S. financial markets and help maintain public trust in the financial markets and the financial system as a whole.
Securities/Commodities Fraud	The FBI focuses its efforts in the securities fraud arena on schemes involving high yield investment fraud market manipulation and commodities fraud. During and after the recent financial crisis, the FBI saw an unprecedented rise in the identification of Ponzi and other high yield investment fraud schemes, many of which involve thousands of victims and staggering losses. 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: (1) Loan Origination Schemes; (2) Illegal property-flipping; and (3) Bailout Schemes.
Health Care Fraud	The FBI identifies and pursues investigations against the most egregious offenders involved in health care fraud and abuse, including criminal enterprises and other crime groups, corporations, companies, and providers whose schemes affect public safety. Besides federal health benefit programs, such as Medicare and Medicaid, private insurance programs also lose billions of dollars each year to fraud schemes in every sector of the industry.
Other Complex Financial Crimes (Insurance, Bankruptcy, and Mass Marketing Fraud)	The FBI also investigates other complex financial crimes that may impact the health of the U.S. economy. For example, if insurance fraud continues to increase, this will contribute to increases in insurance premiums as well as threaten the financial viability of insurance companies. Furthermore, since 2006, the year after bankruptcy laws were changed to make it more difficult for an individual to discharge all debts, bankruptcy filings have significantly increased each year, according to the U.S. Bankruptcy Courts, leading to higher potential for fraud within this area.
Intellectual Property Rights	The FBI's overall strategy for Intellectual Property Rights (IPR) enforcement is to disrupt and dismantle international and domestic criminal organizations and

	individuals that manufacture or traffic in counterfeit and pirated goods and/or steal, distribute or otherwise, profit from the theft of intellectual property. Investigative priorities include theft of trade secrets; counterfeit goods that pose a threat to health and safety; and copyright and trademark infringement cases having a national security, organized crime, or significant economic impact.

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.

In 2017, the FBI led 169 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 (such as 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 that protect all citizens and persons within the U.S., including these four major areas:

Hate Crimes	Investigating hate crimes is the leading priority of the Civil Rights Program due to the devastating impact that the crimes have on individuals, families, and communities. A hate crime is a traditional criminal offense, such as murder, arson, or vandalism, motivated in whole or in part by an offender's bias against a victim's actual or perceived race, religion, national origin, disability, gender, gender identify, or sexual orientation.

Color of Law (COL)	COL violations are the deprivation of any rights, privileges, or immunities secured or protected by the U.S. Constitution by someone in his/her official, governmental capacity. The FBI has investigative responsibility for federal COL matters involving local and state law enforcement and concurrent responsibility with the Office of Inspectors General for other federal agencies.
Human Trafficking	Human trafficking is a form of modern-day slavery and is a significant and persistent problem in U.S. and internationally. Victims are often lured with false promises of good jobs and better lives and then forced to work under brutal and inhumane conditions. Many trafficking victims are forced to work in the sex industry; however, trafficking can also take place in labor settings involving domestic servitude, prison-like factories, and migrant agricultural work. Human trafficking cases require extensive outreach and cooperation with local, state, and federal agencies, as well as non-governmental organizations.
Freedom of Access	Under the Freedom of Access to Clinic Entrances (FACE) Act, the FBI has the sole investigative responsibility for conducting investigations of potential FACE Act violations. Incidents include murder, death threats, invasions, burglaries, and other acts of intimidation. The number of FACE Act violations remains relatively low, with occasional spikes during dates, which mark significant events in the pro-choice and pro-life movements.

The FBI is the only federal agency with sole jurisdiction to investigate child abductions. The FBI's 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 2017, there were 1,254 Crimes Against Children convictions.

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.

Child Abductions	Innocence Lost Initiative	Child Sex Tourism (CST) Initiative
The FBI's Violent Crimes Section, in coordination with the CIRG Behavior Analysis Unit III (BAU III), created regional CARD Teams in order to enhance the FBI's response to abductions and the mysterious disappearance of children. The teams are geographically distributed throughout the five regions of the U.S. The CARD Teams, collectively, consists of over approximately 60 experienced Crimes Against Children investigators	The initiative addresses 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.	This 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, pursuant to the FBI's 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 (STTFs) 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.

In FY 2017, there were 1,222 arrests, 1,057 indictments, and 901 convictions in Indian Country Crime cases.

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.

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 these back to priority targets outside of the U.S.

C. Intelligence Driven Operations

The FBI's 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 the FBI's 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 CD, CTD, CyD, DI, High-Value Detainee Interrogation Group (HIG), TSC, and WMDD. 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 matters.

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 DI 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, FBI 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 work of the FBI's 56 Field Offices.

D. FBI's 2019 Budget Strategy

The FBI's vision, mission, and strategic objectives support its overall strategy. The FBI's vision statement—Ahead of the threat through leadership, agility, and integration—demonstrates the FBI's pledge to be ahead of criminals and potential threats. The FBI achieves this in two different ways. First, the FBI has to continuously evolve to anticipate and mitigate existing threats. Second, the FBI needs to be able to recognize and address threats it has not yet seen.

The mission of the FBI is to protect the American people and uphold the Constitution. 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 2019 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 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 developed an organizational Environmental Management System (EMS) that provides corporate protection standards for Field Offices and major facilities (including CJIS, Quantico, Redstone, 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. The major facilities are covered by the higher-tier organizational EMS and have not developed facility-level EMSs.

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 Energy Conservation Measures (ECMs) and Water Conservation Measures (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.

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, $8,872,080,000, 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, $148,000,000 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).

Note.—A full-year 2018 appropriation for this account was not enacted at the time the budget was prepared; therefore, the budget assumes this account is operating under the Further Continuing Appropriations Act, 2018 (P.L. 115-56) (CR). The amounts included for 2018 reflect the annualized level provided by the continuing resolution.

Analysis of Appropriations Language

- No substantive changes.

IV. Decision Unit Justification

A. Intelligence Decision Unit

INTELLIGENCE DECISION UNIT TOTAL	Direct Pos.	FTE	Amount ($000)
2017 Enacted	6,771	6,286	$1,726,083
2018 Continuing Resolution	6,722	6,295	1,685,350
Adjustment to Base and Technical Adjustments	(115)	61	27,103
2019 Current Services	6,607	6,356	1,712,453
2019 Program Increases	…	…	…
2019 Program Decreases	…	…	…
2019 Request	6,607	6,356	1,712,453
Total Change 2018-2019	**(115)**	**61**	**$27,103**

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 the following functions:

- 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

Performance Materials will be provided at a later date.

B. Counterterrorism/Counterintelligence Decision Unit

COUNTERTERRORISM/COUNTERINTELLIGENCE DECISION UNIT TOTAL	Direct Pos.	Estimate FTE	Amount ($000)
2017 Enacted	13,527	12,738	$3,542,615
2018 Continuing Resolution	13,325	12,660	3,513,974
Adjustment to Base and Technical Adjustments	(192)	(17)	66,858
2019 Current Services	13,133	12,643	3,580,832
2019 Program Increases	…	…	…
2019 Program Decreases	…	…	…
2019 Request	13,133	12,643	3,580,832
Total Change 2018-2019	**(192)**	**(17)**	**$66,858**

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

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

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

[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 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, U.S. Intelligence Community (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. 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.

II. Decision Unit Performance and Resources

Performance Materials will be provided at a later date.

C. Criminal Enterprises Federal Crimes Decision Unit

CRIMINAL ENTERPRISES/FEDERAL CRIMES DECISION UNIT TOTAL	Direct Pos.	Estimated FTE	Amount ($000)
2017 Enacted	12,638	12,309	$2,969,590
2018 Continuing Resolution	12,921	12,443	3,007,312
Adjustment to Base and Technical Adjustments	(130)	13	68,119
2019 Current Services	12,791	12,456	3,075,431
2019 Program Increases	…	…	…
2019 Program Decreases	…	…	…
2019 Request	12,791	12,456	3,075,431
Total Change 2018-2019	**(130)**	**13**	**$68,119**

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.

Program Objectives

White Collar Crime:

Resources	Positions	Dollars ($000)
FY 2017 Enacted	3,685	552,275
FY 2018 Continuing Resolution	3,715	550,904
FY 2019 Request	3,673	599,400

- 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:

Resources	Positions	Dollars ($000)
FY 2017 Enacted	1,912	357,542
FY 2018 Continuing Resolution	1,912	353,903
FY 2019 Request	1,907	370,970

- 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:

Resources	Positions	Dollars ($000)
FY 2017 Enacted	369	57,492
FY 2018 Continuing Resolution	370	57,759
FY 2019 Request	389	64,283

- 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:

Resources	Positions	Dollars ($000)
FY 2017 Enacted	1,497	243,296
FY 2018 Continuing Resolution	1,496	242,609
FY 2019 Request	1,626	267,371

- 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*:**

Resources	Positions	Dollars ($000)
FY 2017 Enacted	1,340	227,577
FY 2018 Continuing Resolution	1,350	229,722
FY 2019 Request	1,436	237,552

- 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:

Resources	Positions	Dollars ($000)
FY 2017 Enacted	1,565	272,701
FY 2018 Continuing Resolution	1,579	274,462
FY 2019 Request	1,721	300,880

- 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

II. Decision Unit Performance and Resources

Performance Materials will be provided at a later date.

D. Criminal Justice Services Decision Unit

CRIMINAL JUSTICE SERVICES DECISION UNIT TOTAL	Pos.	FTE	Amount ($000)
2017 Enacted	2,258	2,167	$528,913
2018 Continuing Resolution	2,226	2,102	501,027
Adjustment to Base and Technical Adjustments	(63)	(29)	2,337
2019 Current Services	2,163	2,073	503,364
2019 Program Increases	…	…	…
2019 Program Decreases	…	…	…
2019 Request	2,163	2,073	503,364
Total Change 2018-2019	**(63)**	**(29)**	**$2,337**

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.

Fingerprint checks processed by NGI:

FY 2016	FY 2017	FY 2018 Estimate
Approximately 76 million	Approximately 76 million	70.5 million

At the close of FY 2017, the Unsolved Latent File (ULF) contained approximately 771,929 records against which incoming fingerprint checks were searched. The ULF is expected to increase an additional 10% in FY 2018. 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, a service which is designed to assist federal, state, and local agencies in the continuous vetting of individuals in a position of trust. 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.

In FY 2017, NCIC processed over 4.7 billion transactions with an average response time of less than .02 seconds.

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.

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.

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.

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 DHS, 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. Consistent with the National Strategy for Information Sharing and Safeguarding, LEEP also connects users to other federations serving the USIC, 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

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, 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 10-week multi-disciplinary course at the FBI National Academy. FBI also conducts and/or 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, and arson.

In FY 2017, 906 state and local law enforcement officers, and 93 international law enforcement officers participated in the National Academy program at the FBI Academy.

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.

II. Decision Unit Performance and Resources

Performance Materials will be provided at a later date.

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.

The FY 2019 request includes a total of $51.895 million for Construction. The requested funding will support the SWE Program ($49.895 million), as well as renovations at the FBI Academy in Quantico, Virginia ($2 million).

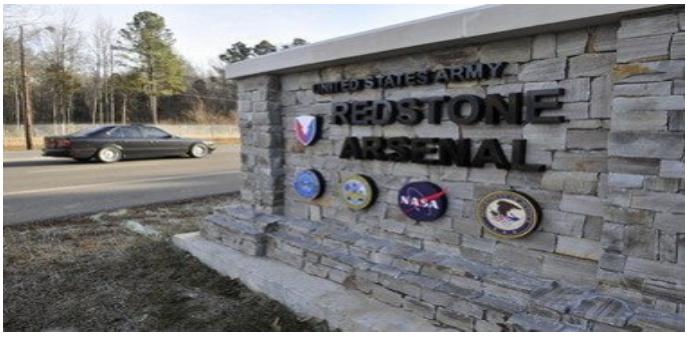
21st Century Facilities: As the lead domestic intelligence and law enforcement agency in the U.S., the FBI defends the U.S. against terrorism, foreign intelligence, and cyber threats, while enforcing the criminal laws of the U.S. and protecting civil rights and civil liberties. The FBI's facilities play a key role in this mission. The FBI manages over 700 locations (18 million square feet) of both federally owned and leased space, including over 160 FBI-owned locations/buildings (approximately 3.5 million square feet), 23 FBI-direct leases (approximately 900,000 square feet), and 516 GSA-leased facilities (over 14 million square feet).

These facilities are not merely office space -- they are operational spaces that enable the FBI to conduct joint operations with other Federal, state, local, and tribal law enforcement partners through Joint Terrorism, Cyber, Safe Streets, and other Task Forces; analyze and disseminate essential intelligence to all partners; forensically exploit digital media and other evidence obtained in national security and criminal cases; monitor audio, visual, and electronic surveillance; coordinate undercover operations; serve as a translation hub for foreign language needs throughout the intelligence community; host meetings with private sector partners to convey sensitive threat information; and coordinate extraterritorial investigations overseas.

The FBI's 21st Century Facilities Plan focuses on renovation and expansion possibilities at FBI-owned properties in Clarksburg, West Virginia; Huntsville, Alabama; Pocatello, Idaho; and Quantico, Virginia.

FBI CJIS Campus

Clarksburg, West Virginia has been home to the FBI's Criminal Justice Information Services (CJIS) Division for the past 22 years. Construction of the Biometrics Technology Center (BTC) concluded in the fall of 2015 and serves as a collaborative site for the FBI, DoD, other government agencies, and academia to provide biometric technologies and services to law enforcement and intelligence agencies and further advances in identification technologies.



Redstone Arsenal

Facilities at Redstone Arsenal in Huntsville, Alabama, which includes the TEDAC, are the newest to the FBI footprint allowing the FBI to collocate counter-IED, training and other FBI mission operations in one location.

Pocatello

The FBI has had a presence in Pocatello, Idaho since 1984. As part of the Department of Justice's Data Center Optimization Initiative, the FBI is constructing a new Data Center on this site. This facility, along with two other Core Enterprise Facilities in Clarksburg, WV and Sterling, VA, will allow DOJ to consolidate over 100 Data Centers nationwide.

Quantico

The FBI's Quantico complex has grown from a training site to a multi-tenant/multi-mission venue. In addition to serving as a national training asset, Quantico is home to operational entities, including the Critical Incident Response Group, the Laboratory, and Operational Technology Divisions. Today, the site encompasses nearly 2.3 million sq. ft. of facilities and supports approximately 3,400 personnel, 13,500 students, and 20,000 visitors annually.

Central Records Complex

In April 2017, the General Services Administration awarded a construction contract for the FBI's Central Records Complex (CRC) facility to be located in Winchester, Virginia. Construction began in the fall of 2017 and facility completion is estimated in FY 2020.

Appropriations Language and Analysis of Appropriations Language

Appropriations Language for Construction

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

Note.—A full-year 2018 appropriation for this account was not enacted at the time the budget was prepared; therefore, the budget assumes this account is operating under the Further Continuing Appropriations Act, 2018 (P.L. 115-56) (CR). The amounts included for 2018 reflect the annualized level provided by the continuing resolution.

VIII. Glossary

ACE	Asian Criminal Enterprises
AFIT	Advanced Fingerprint Identification Technology
ALAT	Assistant Legal Attaché
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