U.S. Department of Justice
Federal Bureau of Investigation

FY 2020 Authorization and Budget Request to Congress

March 2019

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) 2020 budget request proposes a total of $9,309,322,000 in direct budget authority, of which $9,257,427,000 is for Salaries and Expenses (S&E) and $51,895,000 is for Construction.

The S&E request includes a total of 35,558 direct positions and 34,085 direct full time equivalents (FTE); the positions include:

- 13,201 Special Agents (SAs)
- 3,115 Intelligence Analysts (IAs)
- 19,242 Professional Staff (PS)

The S&E program increases total $144,923,000; 168 positions (47 SAs, 8 IAs, and 113 PS), and 85 FTE, for the following:

- $70,477,000 for cyber investigative capabilities
- $18,200,000 to combat transnational organized crime (TOC)
- $4,228,000 to support the National Instant Criminal Background Check System (NICS)
- $16,595,000 to effectively address the emerging requirements associated with the establishment of the National Vetting Center (NVC)
- $17,157,000 to enhance the Render Safe program
- $18,266,000 to support counterintelligence investigative capabilities

The FY 2020 Adjustments to Base (ATBs) include an increase of $82,302,000 for continual support of the FBI's base resource.

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).

The request also includes balance offsets totaling $60,000,000 from, but not limited to, Criminal Justice Information Services (CJIS) automation surcharge balances and $159,000,000 from balances in the Construction account.

The FBI continues to strategically assess current and prospective operations to ensure it meets mission requirements at the lowest possible cost to the United States (U.S.) taxpayer. The FY 2020 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 Justification and Capital Asset Plan and Business Case exhibits can be viewed or downloaded from the Internet using the Internet address: http://www.justice.gov/doj/budget-and-performance

The FBI's Mission: The mission of the FBI is to protect the American people and uphold the Constitution of the U.S. The FBI's mission priorities are to:

- Protect the U.S. from terrorist attack
- Protect the U.S. against foreign intelligence operations and espionage
- Protect the U.S. 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

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

- Strategic Goal 1: Enhance National Security and Counter the Threat of Terrorism
- Strategic Goal 3: Reduce Violent Crime and Promote Public Safety
- Strategic Goal 4: Promote Rule of Law, Integrity, and Good Government

FBI's 2020 Budget Strategy: The FBI's vision, mission, and strategic objectives support its overall strategy. The mission of the FBI is to protect the American people and uphold the Constitution. The FBI's vision statement—Ahead of the threat through leadership, agility, and integration—outlines the FBI's desired strategic position. The FBI will achieve this by continuously evolving to mitigate existing threats and recognizing and anticipating threats it has not yet seen.

The FBI has identified eight operational priorities to focus efforts and accomplish the mission. In addition, the FBI uses an annual threat prioritization process to concentrate on the most concerning threat issues within each of the operational program areas.

The FBI must also structure its 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 vision. The 11 strategic objectives align within the four pillars as follows:

- Capability
    - ✓ Focus on Leadership in Every Aspect of the FBI
    - ✓ Incorporate Intelligence in All We Do
    - ✓ Enhance Cyber Capabilities
    - ✓ Improve Organizational Agility
    - ✓ Strengthen Partnerships
- Technology
    - ✓ Improve Information Technology
    - ✓ Deploy Innovative Solutions
- Talent
    - ✓ Promote a Culture of Accountability and Transparency
    - ✓ Transform Recruitment and Hiring
    - ✓ Improve Workforce Development
- Stewardship
    - ✓ Improve Stewardship of Resources

The FBI's success depends on monitoring and improving its ability to meet these objectives. The FBI conducts Quarterly Strategy Reviews (QSRs) to discuss the FBI's progress on its objectives, and Project Management Reviews (PMRs) to track particular initiatives that support the strategy. These reviews are conducted both at an enterprise level and within each FBI headquarters division.

In the field, the FBI tracks the execution of its mission and operational strategy through the Integrated Program Management (IPM) Process. A key part of the IPM process is the Threat Review and Prioritization (TRP) process. 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. Every two years, headquarters operational divisions will prioritize national threat issues, determine FBI National Threat Priorities (NTPs), and develop national-level mitigation strategies. The 56 field offices then use this information to run a Field TRP process to prioritize the NTPs and other local threat issues.

Furthermore, headquarters operational programs evaluate the threat landscape and develop national threat mitigation strategies. Field offices then prioritize the threats in their areas and work from the national threat strategy to create a local strategy for the upcoming year. These strategies undergo mid-year and end-of-year review and the field offices 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 while also focusing on the future needs of the FBI.

The FBI Strategy is based on the FBI's knowledge of current and future national security, cyber, and criminal investigative threats. From this, 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 2020 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.

Organization of the FBI: The FBI operates field offices in 56 major U.S. cities and 350 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 28 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), 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 Customer Relationship and Management Division, 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/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 IOD, and the OTD, 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. This document lists each threat and activity the FBI is engaging in as well as achievements, where applicable, in these areas.

Terrorism: 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, as well as homegrown violent extremists (HVE) who may aspire to attack the U.S. from within. These threats remain among the highest priorities for the FBI and the Intelligence Community (IC) as a whole.

HVEs aspire to carry out attacks in the U.S. or travel overseas to participate in terrorist activity. Countering the HVE threat is especially challenging for law enforcement because it's difficult to distinguish violent rhetoric from terrorist intent. The FBI's ongoing HVE cases span all 50 states and all 56 FBI field offices.

Conflicts in Syria and Iraq continue to serve as the most attractive overseas theaters for Western-based extremists who want to engage in violence. More than 35,000 people from approximately 120 countries have traveled to join the fighting in Syria and Iraq, the large majority of which traveled to join ISIS. ISIS and other terrorist organizations in the region use these travelers to facilitate terrorist activity beyond Iraq and Syria, particularly in their home countries. Returning foreign fighters could radicalize members of the communities that they came from originally.

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. ISIS' widespread reach through the Internet and social media is most concerning from a homeland security perspective as the group 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 thought possible 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.

Foreign Intelligence: 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 June 2018 conviction of Kevin P. Mallory, a former Central Intelligence Agency (CIA) case officer and Defense Intelligence Agency (DIA) intelligence officer, for delivering, attempting to deliver, and conspiracy to deliver defense information to aid a foreign government, as well as making material false statements. According to court documents, in response to direction from the Chinese intelligence services, Mallory used a cell phone provided by a Chinese intelligence officer to transmit a series of classified documents—one of which included unique identifiers for confidential human sources who had helped the U.S. government.

Another example is the May 2018 sentencing of Turkish citizen Mehmet Hakan Atilla, an official with the Turkish state bank Halkbank, to 32 months in prison for his role in a scheme to use the U.S. financial system to conduct billions of dollars' worth of illegal transactions on behalf of the government of Iran, in violation of U.S. sanctions. The FBI's investigation revealed Atilla and others used false and fraudulent documents to disguise prohibited transactions for Iran as food payments, used Halkbank to conceal currency and gold, and induced U.S. banks to unknowingly process international financial transactions in violation of U.S. law. Atilla was convicted in January 2018 on conspiracy to defraud the United States, violate the International Emergency Economic Powers Act, commit bank fraud, and commit money laundering.

Cyber: The U.S. continues to face a range of criminal, terrorist, and nation state 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 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 cyber mission 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.

On March 23, 2018, the Department of Justice announced charges against nine Iranian nationals who were leaders, contractors, associates, hackers-for-hire, or affiliates of the Mabna Institute, an Iran-based company. These nine individuals allegedly stole more than 31 terabytes of documents and data from more than 140 American universities, 30 American companies, 5 American government agencies, and also more than 176 universities in 21 foreign countries since at least 2013. They conducted many of these intrusions on behalf of the Islamic Republic of Iran's Islamic Revolutionary Guard Corps (IRGC), one of several entities within the government of Iran responsible for gathering intelligence, as well as other Iranian government and university clients. In addition to these criminal charges, the Department of the Treasury designated the Mabna Institute and the nine defendants for sanctions for the malicious cyber-enabled activity outlined in the indictment.

***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. In 2018, the FBI led 168 VGSSTFs. 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.

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, white-collar crime (such as bank fraud) and cybercrime.

Transnational Criminal Organizations (TCO) 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 identity, 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 the 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.

Crimes Against Children: The Violent Crimes Against Children Program has developed a nationwide capacity to:

- Provide a rapid and effective investigative response to reported federal crimes involving the victimization of children;
- Reduce the vulnerability of children to acts of sexual exploitation and abuse;
- Reduce the negative impacts of international parental rights disputes; and,
- Strengthen the capabilities of federal, state, and local law enforcement agencies through training programs and investigative assistance.

The FBI is the only federal agency with sole jurisdiction to investigate child abductions. The FBI's Crimes Against Children Unit supports the Child Abduction Rapid Deployment (CARD) Team, Innocence Lost National Initiative, Innocent Images National Initiative, and the Child Sex Tourism (CST) Initiative.

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, consist of over 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 offenders 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 16 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 2018, there were 1,493 arrests, 1,406 indictments and complaints, and 776 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.

Southwest Border: The volatility among TCO 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.

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.

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.

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.

D. Environmental Accountability

The FBI is implementing an organizational Environmental Management System (EMS) that provides corporate policy and guidance for all FBI facilities, including Field Offices and major owned/operated facilities. The FBI established an overarching environmental policy to serve as the guiding framework for developing, implementing, and continually improving the EMS, and we are currently updating that policy to address all major environmental program areas. The FBI implements the organizational EMS through Environmental Protection Programs (EPPs) that are carried out at the facility and division level through full-time and part-time environmental, safety and health (ESH) staff. The FBI is in the process of updating its ESH Framework policy to clarify the roles and responsibilities of FBI leadership and implementers within the ESH program.

In early 2018, the FBI conducted an ESH risk and opportunities analysis to identify and prioritize major ESH program areas for development and improvement. The FBI identified 24 key areas and developed goals, project plans, and key performance indicators for each prioritized area. Among these areas are sustainable design and construction, the FBI Energy and Water Conservation and Investment Program,

implementation of the National Environmental Policy Act, ESPC/UESC implementation, and electric vehicle charging station installation. The FBI is using an integrated team approach to identify solutions that result in measurable ESH improvements across the FBI.

The FBI actively participates in DOJ's overall efforts to implement the new Executive Order 13834, "Efficient Federal Operations." 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 FBI tracks energy and water usage and audit findings to prioritize facility maintenance projects and forecast future consumption and costs based on identified Energy Conservation Measures (ECMs) and Water Conservation Measures (WCMs). The FBI will continue to evaluate the efficiencies gained on an ongoing basis to quantify both financial and natural resource savings.

Additionally, FBI 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. 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 obtained LEED Gold certification for the new Biometrics Technology Center (BTC) at FBI Clarksburg, and the 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. For an example, these facilities use re-refined motor oil for a majority of the vehicles serviced and recycle all used oil. 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 the pollution prevention and recycling program

II. SUMMARY OF PROGRAM CHANGES

Program	Description	Pos.	FTE	Dollars ($000)	Page
Salaries and Expenses Enhancements					
Cyber	To support the development of advanced technical capabilities and the implementation of a comprehensive, multi-pronged strategy to target malicious cyber actors that threaten global U.S. interests.	33	17	$70,477	5-1
Transnational Organized Crime (TOC)	To enhance the FBI's ability to disrupt and dismantle TOC networks by developing analytical and technical tools for the FBI's TOC program, which also supports the Joint Criminal Opioid Darknet Enforcement (J-CODE) initiative.	…	…	$18,200	5-2
National Instant Criminal Background Check System (NICS)	To support the statutorily required firearm background checks conducted by the NICS program.	40	20	$4,228	5-7
National Vetting Center	To effectively address the emerging requirements associated with the establishment of the National Vetting Center.	48	24	$16,595	5-10
Render Safe	To enhance the capabilities of the FBI's Render Safe, Stabilization and Special Agent Bomb Technician (SABT) programs.	41	21	$17,157	5-14
Counterintelligence	To address threats posed by foreign intelligence and the increased requirements relating to the Foreign Investment Risk Review Modernization Act (FIRRMA)	6	3	$18,266	5-15
Total, Salaries and Expenses Enhancements		**168**	**85**	**$144,923**	

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, $9,257,427,000, 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, $60,000,000 are hereby permanently cancelled, including from, but not limited to, 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.

Note.—A full-year 2019 appropriation for this account was not enacted at the time the budget was prepared; therefore, the budget assumes this account is operating under the Continuing Appropriations Act, 2019 (Division C of P.L. 115–245, as amended). The amounts included for 2019 reflect the annualized level provided by the continuing resolution.

Analysis of Appropriations Language

- No substantive changes.

IV. PROGRAM ACTIVITY JUSTIFICATION
A. Intelligence Decision Unit

INTELLIGENCE DECISION UNIT TOTAL	Direct Pos.	FTE	Amount ($000)
2018 Enacted	6,743	6,406	$1,729,469
2019 Continuing Resolution	6,716	6,420	1,703,695
Adjustment to Base and Technical Adjustments	…	…	10,333
2020 Current Services	6,716	6,420	1,714,028
2020 Program Increases	50	27	13,957
2020 Request	6,766	6,447	$1,727,985
Total Change 2019-2020	50	27	$24,290

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 guides 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 130 languages and dialects, spanning approximately 100 FBI domestic and overseas locations. The FLP promulgates policies and compliance requirements to ensure integrity of 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 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 timely and accurate translation services to support national intelligence priorities and protect our nation and its interests. NVTC was established under Section 907 of the USA Patriot Act (2001) and designated an Intelligence Community (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 in more than 120 languages and dialects. NVTC operates within a virtual model that connects NVTC program staff, translators, field offices, and customers globally 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 amongst its partners in the intelligence and academic communities, and 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, and intelligence 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 and federal, state, local, tribal, and territorial law enforcement. 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.

Office of Private Sector
The primary mission of the FBI's Office of Private Sector (OPS) is to protect the nation's economy and national security by strengthening the FBI's relationships with the U.S. private sector. OPS seeks to have knowledge of the FBI's interactions with the private sector, across the enterprise, and provides a 360 degree understanding of that relationship. OPS also enhances understanding of the private sector, to include academia and associations, to increase collaboration and information-sharing to mitigate risk

and remain "ahead of the threat." OPS works toward the following objectives: facilitating one "FBI voice" by providing a consistent contact for the private sector; focusing on meaningful dialogue with private sector partners to build trust between the FBI and the private sector to counter threats; and, assisting companies whose innovative technologies may be targeted. In addition to its main office at FBI Headquarters, OPS is represented in each FBI Field Office by at least one Private Sector Coordinator (PSC) to develop and maintain private sector partnerships in each Field Office's Area of Responsibility (AOR). OPS also manages two private sector information-sharing legacy programs: the Domestic Security Alliance Council (DSAC) and InfraGard, promoting effective information exchanges through public-private partnerships.

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 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 the Intelligence Community Information Technology Enterprise, an ODNI-led multi-year IT initiative to create an IC-wide information sharing infrastructure.

The unclassified side of the comprehensive system includes the FBI's ability to share unclassified information with other federal, state, and local governments and other partners through the Criminal Justice Information Services' Law Enforcement Enterprise Portal (LEEP) system and UNet, the FBI's unclassified connection to the Internet.

Secure Work Environment (SWE)

Secure Work Environment (SWE) includes two main components - a SCIF and SCINet. A SCIF is an accredited room, group of rooms, floors, or buildings where national security professionals collect, process, exploit, analyze, disseminate, and/or store Sensitive Compartmented Information. SCIFs are outfitted with information technology, telecommunications, general office machines, and requisite infrastructure to process unclassified through Top Secret information. SCIFs are equipped with intrusion detection and access control systems to prevent the entry of unauthorized personnel. SCINet is a compartmented network for Top Secret information, which is administered by employing increased security measures, enforcing user accountability, and enhancing information assurance methodology.

II. Decision Unit Performance and Resources

A. Intelligence Decision Unit

1. Performance and Resource Tables

Decision Unit: Intelligence										
RESOURCES	**Enacted**		**Actual**		**Projected**		**Changes**		**Requested (Total)**	
	FY 2018		**FY 2018**		**FY 2019**		**Current Services Adjustments & FY 2020 Program Changes**		**FY 2020 Request**	
Total Costs and FTE	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
	6,406	$1,729,469	6,332	$1,706,759	6,420	$1,703,695	27	$24,290	6,447	$1,727,985

DOJ Strategic Objective	PERFORMANCE MEASURE TABLE									
	Intelligence									
	Performance Report and Performance Plan Targets		FY14	FY15	FY16	FY17	FY18		FY19	FY20
			Actual	Actual	Actual	Actual	Target	Actual	Target	Target
1.1	Performance Measure	Percentage of Analytic Intelligence Products Scored Under the ODNI's Analytical Integrity Standards (AIS) as "Excellent" or "Good"	N/A	N/A	N/A	77%	70%	89%	70%	70%
1.1	Performance Measure	Median Velocity of Confidential Human Source (CHS)-derived Intelligence Information Reports (IIRs)	N/A	N/A	N/A	22.4 Days	25 Days or Less	22.2 Days	25 Days or Less	25 Days or Less
1.1	Performance Measure	Percentage of FBI Intelligence Information Reports (IIRs) used in the development of United States Intelligence Community (USIC) Intelligence Products	N/A	N/A	N/A	9%	12%	17.4%	12%	15%
1.1	Performance Measure	Percentage of FBI Intelligence Information Reports (IIRs) Citing National Intelligence Priorities Framework (NIPF) Priority 1 & 2 Requirements	N/A	N/A	N/A	82%	80%	84%	82%	80%

2. Resources and Strategies

Analytic Intelligence Products

Performance Measure:
Percentage of Analytic Intelligence Products Scored under the ODNI's Analytical Integrity Standards (AIS) as "Excellent" or "Good"

FY18 Actual: 89%
FY19 Target: 70%
FY20 Target: 70%

Discussion:
The intent of this measure is to assess the level of FBI Intelligence Products that have intelligence value (scoring an "Excellent" or "Good") under ODNI's Analytical Integrity Standards (AIS). The FBI continues to maintain or improve its scores on the Analytic Integrity and Standards (AIS) due to continued outreach and training provided to Intelligence Analysts (IAs) and managers in the field and at HQ divisions. The FBI continues to score Intelligence Bulletins, Assessments, Studies, and a limited amount of Strategic Perspective: Executive Analytical Report (SPEAR) products. The FBI began scoring External Intelligence Bulletins in 2017.

Strategies to Accomplish Outcomes:
The FBI continues to improve scores on the Analytic Integrity and Standards through increased internal training, policy changes, and interaction with ODNI. In order to continue to continue to accomplish this objective, the FBI has increased the level of guidance to product authors in order to ensure products use clear, logical argumentation and demonstrate customer relevance. Additionally, the FBI regularly provides field office training to product authors and supervisors.

CHS-Derived Intelligence Information Reports

Performance Measure:
Median Velocity of Confidential Human Source (CHS)-derived Intelligence Information Reports (IIRs)

FY18 Actual: 22.2 Days
FY19 Target: 25 Days or less
FY20 Target: 25 Days or less

Discussion:
The intent of this measure is to assess the speed with which FBI IIRs are disseminated to Law Enforcement and USIC partners, from the day of acquisition of information. This measure supports the FBI's efforts towards supporting the DOJ's Strategic Goal 1: Enhance National Security and Counter the Threat of Terrorism by continuing to further the FBI's collaboration with other USIC partners.

Strategies to Accomplish Outcomes:
The FBI regularly evaluates its dissemination of intelligence reports to its partners in the USIC with internal management, ensuring the process is transparent and efficient.

IIRs Used in the Development of USIC Products

Performance Measure:
Percentage of FBI Intelligence Information Reports (IIRs) used in the development of United States Intelligence Community (USIC) Intelligence Products

2018 Actual: 17.4%
2019 Target: 12%
2020 Target: 15%

Discussion:
This measure supports the FBI's efforts towards supporting the DOJ Strategic Plan through the continued success dependent, in part, on the strong collaboration between law enforcement and IC partners. Specifically, this measure highlights the quality of the FBI's intelligence products and their usefulness for the entire USIC.

Strategies to Accomplish Outcomes:
The FBI maintains a robust evaluation of its intelligence products and provides multiple training opportunities for authors of intelligence products, in order to meet sustained success and relevance to the broader IC community and DOJ goals.

IIRs Citing NIPF Requirements

Performance Measure:
Percentage of FBI Intelligence Information Reports (IIRs) Citing National Intelligence Priorities Framework (NIPF) Priority 1 & 2 Requirements

2018 Actual: 84%
2019 Target: 82%
2020 Target: 80%

Discussion:
The intent of this measure is to demonstrate the correlation between FBI's Priority Threats and USIC Intelligence Requirements. The measure definition is the number of IIRs matching NIPF Priority 1 & 2 Requirements, divided by the total number of IIRs disseminated.

Strategies to Accomplish Outcomes:
The FBI will track the total production and dissemination of IIRs and determine which products meet FBI priority threats and USIC intelligence requirements with an internal enterprise strategy tool and report the FBI's progress to executive management for accountability.

B. Counterterrorism/Counterintelligence Decision Unit

COUNTERTERRORISM/COUNTERINTELLIGENCE DECISION UNIT TOTAL	Direct Pos.	Estimate FTE	Amount ($000)
2018 Enacted	13,611	13,104	$3,676,272
2019 Continuing Resolution	13,498	12,927	3,686,305
Adjustment to Base and Technical Adjustments	…	…	28,335
2020 Current Services	13,498	12,927	3,714,640
2020 Program Increases	53	25	75,591
2020 Request	13,551	12,952	$3,790,231
Total Change 2019-2020	53	25	$103,926

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 policymakers 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, since the attacks of 9/11, 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 divided its CT operations into branches, each of which focuses on a different aspect of the current terrorism threat facing the Nation. These components are staffed with SAs, IAs, and subject matter experts who work closely with investigators in the field and integrate intelligence across component lines. This integration allows for real-time responses to threat information and quick communication with decision-makers and the field.

The FBI has also established strong working relationships with other members of the IC. Through the Director's daily meetings with other IC executives, the regular exchange of personnel among agencies, joint efforts in specific investigations and in the National

[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.

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 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.

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 209 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 CI responsibility is to identify, understand, and combat these threats.

The domestic CI 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 CI threats involved Foreign Intelligence Service (FIS) officers seeking U.S. 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.

Recent notable successes include an April 2018 federal sentencing of Weiqiang Zhang to more than 10 years in prison for his role in a conspiracy to steal genetically modified rice seeds from his employer, Kansas biotechnology firm Ventria Bioscience. Zhang was convicted in February 2017 for conspiring with Wengui Yan, a U.S. Department of Agriculture research scientist, to enable members of a Chinese delegation to steal proprietary rice seeds during their visits to U.S. government facilities in 2013. Federal investigators seized a large quantity of Ventria's seeds from the delegation members' luggage as they prepared to depart the United States for China.

The seeds have a wide variety of health research applications, and the company had invested millions of dollars in their development.

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 Critical Incident Response Program (CIRG) facilitates the FBI's rapid response to, and management of, crisis incidents and special events integrating tactical response and resolution, negotiations, behavioral analysis and assessments, surveillance, bomb technician and Render Safe programs, operations centers and crisis management resources. The CIRG personnel are on call around the clock to respond to crisis incidents requiring an immediate law enforcement response and to support FBI planning and coordination of special events. The CIRG also furnishes distinctive training to FBI field personnel as well as state, local, federal, tribal and international law enforcement partners in support of this mission. This includes Hazardous Device School (HDS) certification, recertification and advanced training to all U.S. public safety bomb technicians and accreditation of all U.S. public safety bomb squads.

The CIRG encompasses the Hostage Rescue Team (HRT), a full-time national tactical counterterrorism team, and manages the SWAT program in all FBI Field Offices. The 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 including the Unmanned Aerial Surveillance (UAS) 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 all programs. The CIRG operates the Strategic Information and Operations Center (SIOC) to maintain 24/7/365 enterprise-wide situational awareness. In addition, the CIRG oversees the National Center for the Analysis of Violent Crime Program and provides behavioral analysis and assessments for complex and time-sensitive investigations across multiple programs.

The CIRG's readiness posture provides the USG with deployment capabilities to counter a myriad of CT/CI and criminal threats—from incidents involving WMDs to a mass hostage

taking. The FBI's crisis response protocols are built upon lessons learned from past incidents, resulting in a tiered response, streamlined command and control, standardized training, equipment and operating procedures, and collaboration 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 the CIRG encompasses all of these elements.

Legal Attaché (Legat) Program

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

B. *Counterterrorism/Counterintelligence Decision Unit*

1. Performance and Resource Tables

Decision Unit: Counterterrorism/Counterintelligence										
WORKLOAD/ RESOURCES	**Target**		**Actual**		**Projected**		**Changes**		**Requested (Total)**	
	FY 2018		**FY 2018**		**FY 2019**		**Current Services Adjustments & FY 2020 Program Changes**		**FY 2020 Request**	
Total Costs and FTE	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
	13,104	$3,676,272	12,824	$3,622,417	12,927	$3,686,305	25	$103,926	12,952	$3,790,231

DOJ Strategic Objective	PERFORMANCE MEASURE TABLE									
	Counterterrorism / Counterintelligence									
	Performance Report and Performance Plan Targets		FY14 Actual	FY15 Actual	FY16 Actual	FY17 Actual	FY18 Target	FY18 Actual	FY19 Target	FY20 Target
1.1	Performance Measure	Number of Terrorism Disruptions (affected through investigations)	214	440	460	723	200	540	250	400
1.2	Performance Measure	Number of computer intrusion program deters, detects, disruptions, and dismantlements conducted	N/A	6,421	4,217	9,139	4,200	11,540	8,000	8,000
1.3	Performance Measure	Number of National Insider Threat Task Force Insider Threat HUB Operations Courses conducted	N/A	N/A	N/A	6	6	10	6	6
1.3	Performance Measure	Number of counterintelligence program disruptions and dismantlements conducted	360	232	2,132	450	400	698	400	400

2. Performance, Resources, and Strategies

Counterterrorism (CT)

***Performance Measure and Agency Priority Goal*:**
Number of Terrorism Disruptions (affected through investigations)
FY 2018 Actual: 540
FY 2019 Target: 250
FY 2020 Target: 400

Discussion:
A disruption is defined as interrupting or inhibiting a threat actor from engaging in criminal or national security-related activity. A disruption is the result of direct actions and may include, but is not limited to, the arrest; seizure of assets; or impairing the operational capabilities of key threat actors. In executing the FBI's number one priority to protect the U.S. from terrorist attacks, disruptions remain a key statistic that directly speaks to its CT responsibilities. To fulfill the mission of defeating terrorism, the FBI focused resources on targeting and disrupting terrorist threats and groups by leveraging its workforce and ensuring the use of the latest technology to thwart emerging trends.

The FBI remains proactively positioned to combat a constantly evolving threat landscape, which can lead to disparities between reported disruption totals and previously established targets.

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

Strategies to Accomplish Outcomes:
The FBI must be able to effectively respond to the challenges posed by unconventional terrorist methods, such as the use of chemical, biological, radiological, explosive, and nuclear materials. When terrorist acts do occur, the FBI must rapidly identify, locate, apprehend, and prosecute those responsible. As part of its counterterrorism mission, the FBI will continue to combat terrorism by investigating those persons and countries that finance terrorist acts. The FBI will aggressively use the money laundering and asset forfeiture statutes to locate and disrupt the financial sources of terrorist organizations. The FBI will also work to effectively and efficiently utilize the tools authorized by Congress. While the ultimate goal is to prevent a terrorist act before it occurs, the FBI must be able to respond should an act occur. The FBI's work in this area includes improved intelligence gathering and sharing, improved analytical capabilities, and enhanced training and liaison.

Cyber - Computer Intrusions

***Performance Measure*:**
Number of computer intrusion program deters, detections, disruptions, and dismantlements conducted

FY 2018 Actual: 11,540
FY 2019 Target: 8,000
FY 2020 Target: 8,000

Performance Plan and Report for Outcomes:
The Computer Intrusion Program (CIP) is a top priority of the FBI. The mission of the CIP is to identify, assess, and neutralize computer intrusion threats emanating from terrorist organizations, state sponsored threat actors, and criminal groups targeting the national information infrastructure.

The FBI's Cyber Division anticipates the number of detects, deters, disruptions, and dismantlements will continually climb due to significant emphasis placed on FBI field offices to achieve judicial, operational, and preventative outcomes through the annual Field Office Strategic Plan (FOSP) creation and evaluations processes.

Strategies to Accomplish Outcomes:
The FBI Cyber Division (CyD) addresses the growing criminal and national security threat of unauthorized computer intrusions by targeting investigative and mitigation resources on top-priority cyber threat actors. The FBI CyD seeks to eliminate threat actor intrusion capabilities through detection, deterrence, disruption, and dismantlement operations. Each fiscal year, the FBI CyD communicates cyber threat-level guidance to all FBI field offices, in order to direct FBI progress towards achieving these mitigation outcomes against the most important cyber threats.

Insider Threat

***Performance Measure*:**
Number of National Insider Threat Task Force Insider Threat HUB Operations Courses conducted

FY 2018 Actual: 10
FY 2019 Target: 6
FY 2020 Target: 6

Discussion:
The measure "Number of National Insider Threat Task Force Insider Threat HUB Operations Courses conducted" directly supports DOJ's Strategic Goal 1: Enhance National Security and Counter the Threat of Terrorism. This measure is intended to maintain the number of National Insider Threat Task Force Insider Threat HUB Operations Courses conducted to educate the federal workforce against internal and external threats in an effort to combat unauthorized disclosures, insider threats, and hostile intelligence activities.

Strategies to Accomplish Outcomes:
The FBI recognizes foreign nations take a broad-spectrum approach, in which traditional and non-traditional intelligence collectors seek to acquire vital U.S. assets. The FBI leverages the IPM's Consolidated Strategy Guide (CSG) and Field Office Strategic Plan (FOSP) to provide operational guidance for counterintelligence investigations. The FBI's strategy to counter foreign intelligence entities emphasizes the importance of 1) understanding what assets adversaries are targeting, 2) engaging the entities who possess those assets, and 3) helping protect them from foreign actors. The FBI also aligns its threat priorities with the DOJ's strategies to achieve Goal Objective 1.3: "Combat unauthorized disclosures, insider threats, and hostile intelligence activities," which nests under Goal 1: "Enhance National Security and Counter the Threat of Terrorism."

Counterintelligence (CI)

***Performance Measure*:**
Number of counterintelligence program disruptions and dismantlements conducted

FY 2018 Actual: 698
FY 2019 Target: 400
FY 2020 Target: 400

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

Performance Plan and Report for Outcomes:
The FBI utilizes its Threat Review and Prioritization (TRP) and the Integrated Program Management (IPM) process to develop national strategies that include measures of performance and measures of effectiveness in identifying, understanding, and combating CI National Threats. The FBI relies on these processes to allocate resources toward priority threats, clarify and enhance understanding of Foreign Intelligence Threats, identify new intelligence requirements, compare different perspectives, and inform decision making.

Strategies to Accomplish Outcomes:
In an effort to accomplish its established goal of educating the federal workforce against internal and external threat relating to unauthorized disclosures, insider threats, and hostile intelligence activities the National Insider Threat Task Force (NITTF) is piloting an effort to host its HUB Operations Courses on a regional basis. By hosting the course in different locations throughout the United States, the NITTF will be able to reach a more diverse audience of federal employees. The HUB Operations Courses will also continue to be hosted on a reoccurring basis in the Washington DC region.

C. Criminal Enterprises and Federal Crimes Decision Unit

CRIMINAL ENTERPRISES AND FEDERAL CRIMES DECISION UNIT TOTAL	Direct Pos.	Estimated FTE	Amount ($000)
2018 Enacted	12,692	12,258	$3,071,970
2019 Continuing Resolution	12,844	12,434	3,084,857
Adjustment to Base and Technical Adjustments	…	…	35,109
2020 Current Services	12,844	12,434	3,119,966
2020 Program Increases	25	13	52,227
2020 Request	12,869	12,447	$3,172,193
Total Change 2019-2020	**25**	**13**	**$87,336**

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, and 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 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.

II. Decision Unit Performance and Resources

C. *Criminal Enterprises and Federal Crimes Decision Unit*

1. Performance and Resource Tables

2. PERFORMANCE/RESOURCES TABLE										
Decision Unit: Criminal Enterprises and Federal Crimes										
WORKLOAD/ RESOURCES	**Target**		**Actual**		**Projected**		**Changes**		**Requested (Total)**	
	FY 2018		**FY 2018**		**FY 2019**		**Current Services Adjustments & FY 2020 Program Changes**		**FY 2020 Request**	
Total Costs and FTE	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
	12,258	$3,071,970	12,542	$3,046,635	12,434	$3,084,857	13	$87,336	12,447	$3,172,193

DOJ Strategic Objective	PERFORMANCE MEASURE TABLE									
	Criminal Enterprises and Federal Crimes Decision Unit									
	Performance Report and Performance Plan Targets		FY14	FY15	FY16	FY17	FY18		FY19	FY20
			Actual	Actual	Actual	Actual	Target	Actual	Target	Target
3.2	Performance Measure	CPOT-linked DTOs: Disruptions	139	150	136	80	50	78	50	50
3.2	Performance Measure	CPOT-linked DTOs: Dismantlements	40	31	34	23	20	22	20	20
4.1	Performance Measure	Number of Criminal Organizations Engaging in white-Collar Crimes Dismantled	458	464	416	302	400	510	400	400
3.1	Performance Measure	Percent of increase of non-CPOT Gang/Criminal Enterprise Dismantlements	N/A	N/A	N/A	N/A	15%	29%	15%	15%

3. Performance, Resources, and Strategies

White Collar Crime

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

FY 2018 Actual: 510
FY 2019 Target: 400
FY 2020 Target: 400

Discussion:
Corporate, Securities and Commodities Fraud, and many other financial crimes investigations are frequently long-term and resource-intensive. The impacts of resources received in one year are often not realized until several years later. Further, accomplishments in WCC can reach peaks at times when long-term cases initiated in prior years come to conclusion.

Performance Plan and Report for Outcomes:
The White Collar Crime (WCC) program uses a suite of performance measures that concentrate on priority programs such as Corporate, Securities and Commodities Fraud, Money Laundering Facilitation, Health Care Fraud, Financial Institution Related Fraud, and Frauds and Swindles, as well as traditional accomplishment data such as convictions and pre-trial diversions and the level of recoveries, restitutions, and fines generated by the WCC program. Corporate, Securities and Commodities Fraud, and many other financial crimes investigations are frequently long-term and resource-intensive. The impacts of resources received in one year are often not realized until several years later. Further, accomplishments in WCC can reach peaks at times when long-term cases initiated in prior years come to conclusion.

Strategies to Accomplish Outcomes:
In FY 2020, the FBI will continue to pursue corporate fraud, securities and commodities fraud, financial institution related fraud such as bank and mortgage fraud, health care fraud, money laundering facilitation, insurance fraud, intellectual property rights crimes, and other swindles directed at consumers and businesses such as mass marketing fraud and cyber enhanced fraud, all of which threaten to undermine our nation's financial infrastructure and often target our nation’s most vulnerable citizens. The FBI will aggressively leverage the money laundering and asset forfeiture statutes to ensure that fraudulently obtained funds are located and proper restitution is made to the victims of fraud. The enforcement strategy is a coordinated approach whereby the FBI will continue to work with other federal agencies to identify and target fraud schemes by successfully investigating, prosecuting, and obtaining judgments and settlements.

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

Performance Measure:
Number of CPOT-linked DTO disruptions and dismantlements

Disruptions
FY 2018 Actual: 78
FY 2019 Target: 50
FY 2020 Target: 50

Dismantlements
FY 2018 Actual: 22
FY 2019 Target: 20
FY 2020 Target: 20

Discussion: DTOs are dismantled through complex and coordinated intelligence-driven investigations that include analysis of drug investigative data and related financial data. These efforts effectively disrupt the operations of major trafficking organizations and ultimately destroy them. The FBI focuses resources on coordinated, nationwide investigations targeting the entire infrastructure of major DTOs and its members who traffic in narcotics and launder illicit proceeds. Strategic initiatives are developed to effectively exploit the DTO's most vulnerable points, thus attacking its infrastructure.

Performance Plan and Report for Outcomes:
DOJ maintains a national list of the most prolific major international drug trafficking and money laundering organizations threatening the United States. This list of targets, known as the CPOT list, reflects the most significant international narcotic manufacturers, poly-drug traffickers, suppliers, transporters, and money laundering organizations who further engage in violence, corruption, human smuggling, weapons trafficking, as well as complex financial and organized criminal activities.

Strategies to Accomplish Outcomes:
The FBI's strategy utilizes the enterprise theory of investigation which focuses on the overall organization. Further employing a comprehensive strategy that begins with the intelligence-based targeting of significant criminal organizations and the execution of multiple coordinated investigations against the highest value targets.

The FBI has developed a comprehensive counter-drug strategy designed to investigate and prosecute illegal drug traffickers and distributors, reduce drug related crime and violence, provide assistance to other law enforcement agencies, and strengthen international cooperation. The strategy focuses the FBI's counter-drug resources on identified CPOT organizations with the most adverse impact on U.S. national interests.

FBI's Criminal Investigative Division, OCDETF Unit works in tandem with the OCDETF Executive Office to track the number of organizations linked to targets on DOJ's CPOT list.

Organized Criminal Enterprises & Gangs/Criminal Enterprises

Performance Measure and Agency Priority Goal:
Percent increase of non-CPOT gang/criminal enterprise dismantlements

FY 2018 Actual: 29%
FY 2019 Target: 15%
FY 2020 Target: 15%

Discussion:
Successful mitigation of criminal enterprise and gang activity should lead to a decline in the overall threat criminal enterprises pose at a national level. By providing training and resources, coordinating investigative and intelligence-gathering activity, and by supplementing liaison efforts, the FBI seeks to promote an integrated approach to mitigation across the nation.

Performance Plan and Report for Outcomes:

Organized Criminal Enterprises & Gangs/Criminal Enterprises

The mission of the FBI's Gang/Criminal Enterprise and Transnational Organized Crime Programs are to disrupt and dismantle criminal enterprises and their respective cells (local, regional, national, and transnational), which pose the greatest threat to the economic and national security of the U.S. These criminal enterprises are engaged in a myriad of criminal activities, including drug trafficking, money laundering, human trafficking, alien smuggling, public corruption, weapons trafficking, extortion, kidnapping, exploitation and trafficking of natural resources, theft of cultural property, and insurance and health care frauds, and have ties across North, Central, and South America, as well as Asia, Africa, the Middle East, and Europe. The FBI will accomplish this mission through criminal investigations, directing efforts towards the top-priority, most detrimental criminal enterprises and utilizing the Racketeering Influenced Corrupt Organization (RICO) statute to target the entire enterprise when appropriate.

FBI efforts also include participation in and leadership of Department of Justice and other federal programs or initiatives such as the Organized Crime Drug Enforcement Task Forces (OCDETF) Program, High Intensity Drug Trafficking Areas (HIDTA) Program, and the Joint Criminal Opioid Darknet Enforcement (J-CODE) Team. The FBI also works closely with local, state, federal, and international law enforcement agencies to accomplish this mission through additional task forces and ad hoc working groups. The FBI also participates in multiple interagency organizations, such as the Special Operations Division (SOD), the OCDETF Fusion Center (OFC), and the International Organized Crime Intelligence and Operations Center (IOC-2) to enhance FBI investigation through deconfliction and case coordination efforts with other federal agencies.

D. Criminal Justice Services Decision Unit

CRIMINAL JUSTICE SERVICES DECISION UNIT TOTAL	Pos.	FTE	Amount ($000)
2018 Enacted	2,344	2,232	$552,491
2019 Continuing Resolution	2,332	2,219	555,345
Adjustment to Base and Technical Adjustments	…	…	8,525
2020 Current Services	2,332	2,219	563,870
2020 Program Increases	40	20	3,148
2020 Request	2,372	2,239	$567,018
Total Change 2019-2020	**40**	**20**	**$11,673**

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 needed 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 2017	FY 2018	FY 2019 Estimate
76,769,505	70,074,260	Approximately 63.4 million[3]

[3] The estimate for FY 2019 is lower because the NGI system adapted the best seven of ten fingerprint solutions to allow the system to raise the image quality score by removing up to three of the lowest quality fingerprints. This was implemented to reduce rejects and retain more fingerprint submissions. Since CJIS is rejecting less back to contributors, a subsequent secondary submission is not needed.

At the close of FY 2018, the Unsolved Latent File (ULF) contained approximately 811,923 records against which incoming fingerprint checks were searched. Of those, 290,550 are related to active terrorism investigations. The ULF is expected to increase approximately 10% in FY 2019. 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. 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 32 million booking photos of criminals – 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, three of the largest submitting agencies include the State of Utah, Texas and the Transportation Security Administration. Utah has enrolled 269,939 and Texas has enrolled 823,997 Rap Back Subscriptions to include teachers, nurses, and EMS workers. The TSA has enrolled over 625,195 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 99.89% 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

In FY 2018, NCIC processed over 3.7 billion transactions with an average response time of less than .02 seconds.

and the public.

NCIC is a valuable tool that aids law enforcement officers, investigators, judges, prosecutors, correction officers, court administrators, and other law enforcement and criminal justice agency officials in the execution of their day-to-day operations. The NCIC contains over 15.5 million active records and processes an average of 10.9 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 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 (Technical Refresh) 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 System was moved from a development status to an Operational Capability in June 2018. Since the upgrade, the FBI has noticed a decrease in the time required to ingest data, return errors, and identify outlier values and other data quality issues.

The FBI has 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. 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.

As of June 2018, 7,057 agencies (approximately 32.7 % 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 three years.

National Data Exchange (N-DEx): The FBI's N-DEx System is an unclassified national strategic investigative information sharing system, which 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 446 million searchable records from over 7,100 criminal justice agencies. The N-DEx System provides access to an additional 317 million records from the Department of Homeland Security, the Interstate Identification Index, the National Crime Information Center, and INTERPOL.

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 in August

2008 for meeting or exceeding the requirements for international accreditation (ISO/IEC 17025). Examinations support investigations that cross all FBI investigative programs and international, federal, state, and local boundaries. The FBI Laboratory performs free-of-charge examinations of evidence for duly constituted U.S. law enforcement agencies, whether federal, state or local, and foreign law enforcement unable to perform the examinations at their own facilities. The FBI Laboratory also provides comprehensive technical reports, training, and expert testimony to federal, state, and local agencies.

In addition to providing forensic analysis services, the FBI Laboratory also provides operational response capabilities with respect to chemical, biological, nuclear, radiological, and explosive devices/incidents and evidence collection. The Laboratory provides biometric identification services through the Combined DNA Index System (CODIS) and the Federal Convicted Offender Program (FCOP).

The 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 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 local law enforcement partners, 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 2018, 815 state and local law enforcement officers, and 90 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 international training and assistance programs.

II. Decision Unit Performance and Resources

D. Criminal Justice Services Decision Unit

1. Performance and Resource Tables

2. PERFORMANCE/RESOURCES TABLE										
Decision Unit: Criminal Justice Services										
WORKLOAD/ RESOURCES	**Target**		**Actual (To Date)**		**Projected**		**Changes**		**Requested (Total)**	
	FY 2018		**FY 2018**		**FY 2019**		**Current Services Adjustments & FY 2020 Program Changes**		**FY 2020 Request**	
Total Costs and FTE	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
	2,232	$552,491	2,122	$526,892	2,219	$555,345	20	$11,673	2,239	$567,018

DOJ Strategic Objective	PERFORMANCE MEASURE TABLE									
	Criminal Justice Services									
	Performance Report and Performance Plan Targets		FY14 Actual	FY15 Actual	FY16 Actual	FY17 Actual	FY18 Target	FY18 Actual	FY19 Target	FY20 Target
4.4	Performance Measure	Percentage of NGI System Availability	N/A	N/A	N/A	N/A	99.5%	99.7%	99.5%	99.5%
4.4	Performance Measure	Percentage of NICSSystem Availability	N/A	N/A	N/A	N/A	98%	99.7%	98%	98%
4.4	Performance Measure	Percentage of NCIC System Availability	N/A	N/A	99.8%	99.78%	99.5%	99.8%	99.5%	99.5%
4.4	Performance Measure	Average Turnaround Time for Federal DNA Sample Entry in the National DNA Index System (NDIS) of Submissions Fulfilling the Processing and Upload	N/A	N/A	N/A	N/A	15 Days	8 Days	15 Days	15 Days

3. Performance, Resources, and Strategies

Performance Plan and Report for Outcomes

Next Generation Identification

Performance Measure:
Percentage of NGI System Availability- Percentage of time the NGI system is available

FY 2018 Actual: 99.7%
FY 2019 Target: 99.5%
FY 2020 Target: 99.5%

Discussion:
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.

Performance Plan and Report for Outcomes:
This performance measure demonstrates the FBI's ability to provide exemplar system availability to ensure the most complete and up-to date records possible for criminal and noncriminal justice purposes. Timely notifications enhance public safety and give law enforcement the ability to be notified with triggering information instead of utilizing their own manpower to continuously monitor persons under investigation.

Strategies to Accomplish Outcomes:
- Minimize downtime
- Strategically plan times for system maintenance
- Monitor work flow and surges

NICS

Performance Measure:
Percentage of NICS System Availability - Percentage of time the NICS system is available

FY 2018 Actual: 99.7%
FY 2019 Target: 98%
FY 2020 Target: 98%

Discussion:
The Initial Operational Capability of the New NICS was deployed on August 9, 2016. The New NICS delivered updated capabilities, additional flexibility to make systematic and business changes, 24/7 system capability and greater operational efficiencies such as immediate denials of transactions with algorithm scoring 100 against NICS Indices records. The IT Architecture has been upgraded to include a total redesign and refresh of the NICS hardware and software. Since the deployment of the Initial Operating Capability, the NICS Section, along with IT support, have been focused on system stability and system enhancements. The Full Operational Capability (FOC) development began in June 2018,

will end in June 2019, and is utilizing the agile development framework. The FOC is highlighted by technical functionality such as computer telephony integration capabilities and increased automation of operational processes

Performance Plan and Report for Outcomes:
Provide reliable availability of the NICS to save lives and protect people from harm by ensuring the timely transfer of firearms or firearm and explosive-related permits to eligible persons. The FBI strives to begin processing background checks within the first business day.

Strategies to Accomplish Outcomes:
- Minimize downtime
- Strategically plan times for system maintenance
- Monitor work flow and surges and prepare for unforeseen system outages
- Ensure adequate testing is completed prior to deploying/implementing system changes and enhancements to avoid unplanned system outages

NCIC

Performance Measure – System Availability:
Percentage of time the NCIC system is available

FY 2018 Actual: 99.8%
FY 2019 Target: 99.5%
FY 2020 Target: 99.5%

Discussion:
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 99.8% 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. The FBI is preparing for the next major upgrade to the NCIC known as NCIC 3rd Generation (N3G). The goal of N3G is to 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.

Performance Plan and Report for Outcomes:
Provide real time, accurate, and complete criminal justice information to support law enforcement and criminal justice communities. The FBI maintains the host computer and provides a telecommunication network to the CJIS Systems Agency (CSA) that provides NCIC access to virtually all local criminal justice agencies. Through this cooperative network, law enforcement personnel have direct on-line access to enter data or search millions of records for persons and property.

Strategies to Accomplish Outcomes:
- Minimize downtime
- Strategically plan times for system maintenance
- Monitor work flow and surges

National DNA Index System (NDIS)

Performance Measure:

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

FY 2018 Actual: 8 days
FY 2019 Target: 15 days
FY 2020 Target: 15 days

Discussion:

The FBI Laboratory has established a 30-day turnaround time for processing and uploading samples based upon community expectations to receive, process, analyze, and upload samples. To reduce the turnaround time for samples requiring analysis, the Federal DNA Database (FDD) Program consistently (1) implements process improvements in how samples are analyzed/reworked to increase efficiency, and (2) specifically monitors the turnaround time of samples that require analysis/re-analysis. In FY 2017, the FDD program significantly exceeded its target of an average 30-day turnaround time for sample processing/upload by achieving an 11-day average turnaround time on first run samples.

V. PROGRAM INCREASES

Item Name: **FBI Cyber: Community, Collaboration, and Capabilities**

Strategic Goals & Objectives: 1.1, 1.2, 1.3, 3.1, 3.2, 4.1, 4.2

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

Organizational Programs: Cyber, Operational Technology

Program Increase: Positions 33 Agt 3 FTE 17 Dollars $70,477,000 ($64,413,000 non-personnel)

Description of Item

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

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

Strategic Goals & Objectives: 3.1, 4.1

Budget Decision Unit(s): Criminal Enterprises Federal Crimes

Organizational Program: Criminal Investigative

Program Increase: Positions 0 Agt 0 FTE 0 Dollars $18,200,000 (all non-personnel)

Description of Item

The FBI requests $18,200,000 (all non-personnel) to effectively address the evolving transnational organized crime (TOC) threat facing the nation. Specifically, the requested resources will be used to enhance the following three areas of the FBI's TOC program, each of which also supports the FBI's Joint Criminal Opioid Darknet Enforcement (J-CODE) initiative and the organization's other efforts to combat the opioid crisis.

- Strategic Targeting
- Data Exploitation and Analysis
- Technological Expertise

Justification

TOC poses a significant and growing threat to national and international security with implications for public safety, public health, democratic institutions, and economic stability across the globe. The TOC threat encompasses a myriad of activities which impact the United States, including drug trafficking, money laundering, human trafficking, alien smuggling, public corruption, weapons trafficking, extortion, kidnapping, criminal cyber fraud, exploitation and trafficking of natural resources, theft of cultural property such as art and antiquities, and insurance and health care frauds. The United States serves as a market and source for illicit goods and criminal services. TOC networks exploit legitimate institutions for critical financial and business services that enable the storage or transfer of illicit proceeds.

Illicit drug trafficking continues to be a growing threat. The accessibility and the convenience of the drug trade online contributes to the opioid epidemic in the United States. On January 10, 2018, the Office of the Deputy Attorney General directed the FBI and other federal law enforcement partners to develop a strategic plan to disrupt and dismantle the Darknet illicit marketplaces facilitating the distribution of fentanyl and other opioids. As a result of this request, the FBI established the J-CODE Initiative, which brings together agents, analysts, and professional staff with expertise in drugs, gangs, health care fraud, and more, and federal, state, and local law enforcement partners from across the U.S. Government. The newly-established J-CODE Team has developed a comprehensive, multi-pronged criminal enterprise strategy to target the trafficking of fentanyl and other opioids on the Darknet and Clearnet. This strategy focuses on identifying and infiltrating the marketplace administrative team, analyzing financial information, locating and exploiting marketplace infrastructure, targeting vendors and buyers, and enabling field office success in the investigation and prosecution of these marketplaces.

Strategic Targeting: $4,000,000 (all non-personnel)

In accordance with Executive Order 13773 *Enforcing Federal Law with Respect to Transnational Criminal Organizations and Preventing International Trafficking*, the U.S. law enforcement and intelligence communities are developing a "whole-of-government" approach to strategically combat the TOC threat as coordinated through the U.S. Council on TOC (USCTOC). To support these efforts, the interagency has identified the need to develop and implement a comprehensive strategy to target the most detrimental TOC networks across the globe and support major field investigations. The FBI requests $4 million for strategic and tactical capabilities to ensure there is adequate intelligence and investigative knowledge to inform and implement the TOC strategy. Of the $4 million, $2.3 million would be dedicated to support development and delivery of advanced training for investigators and analysts, operational travel, and funds to support major cases that span the U.S. and overseas, as well as contract analysis support for targeting.

The FBI coordinates operational and intelligence efforts both formally and informally with other domestic and international law enforcement partners, which include enhanced de-confliction efforts. The previously mentioned $4 million includes $1.2 million to support interagency communication and collaboration in online opioid matters, including J-CODE efforts, allowing for de-confliction and prioritization of efforts across the U.S. Government. The FBI formally leads the DOJ's (J-CODE) team, which is directed to centralize the efforts of domestic partners to more effectively target online opioid vendors. The J-CODE team includes the FBI, DOJ-Criminal Division, DEA, ATF, and the Department of Defense. The FBI is in discussions with US Postal Inspection Service, U.S. Customs and Border Protection, Homeland Security Investigations, and the Department of Treasury to joining the team. Given the international scope of TOC groups as well as the complexity of TOC cases, field office investigators, intelligence personnel, and prosecutors must conduct significant amounts of operational travel to successfully conduct these investigations.

TOC investigations frequently require extensive undercover operations. In an effort to ensure the FBI can adequately accommodate these investigative needs, $500,000, of the previously mentioned $4 million, will be required to conduct Undercover Employee Certification training for personnel. The FBI will be more successful in strategically targeting TOC actors through collaboration with other agencies and having the resources necessary to disrupt and dismantle the TOC networks.

With an enhancement to the organization's strategic capabilities, the FBI will be able to conduct more investigations, such as Operation Jumping Rooftops, that target the largest and most detrimental TOC networks. In 2015, FBI San Diego began Operation Jumping Rooftops to investigate an organization operating a large scale money-laundering and drug trafficking network based in Culiacan, Mexico. As a result of the investigation, law enforcement arrested approximately 75 subjects, seized more than $6 million dollars in US currency, seized 95 kilograms of methamphetamine, 63 kilograms of heroin, 10 kilograms of fentanyl, 92 kilograms of cocaine, 252 kilograms of marijuana and 20 firearms, including semiautomatic assault rifles and handguns.

Over the course of the last two years, undercover agents also identified multiple individuals known as "money movers." These people are responsible for collecting narcotics proceeds and disposing of those proceeds as directed by either the drug trafficking organization or the money brokers. By targeting these individuals, law enforcement was able to discover multiple drug trafficking cells across the U.S. that are responsible for importing and distributing substantial quantities of fentanyl, heroin, methamphetamine, and cocaine.

Data Exploitation and Analysis: $5,300,000 (all non-personnel)

Illicit financial networks, money movements, and investments are inherent to illegal activity and are often at the crux of the investigations of TOC networks. However, due to the international movement of illicit funds and technological developments (e.g., virtual currencies), thorough financial analysis is challenging.

The accessibility and convenience of the illicit drug trade on the Darknet, where a variety of illicit drugs can be purchased and delivered directly to consumers through the mail, contributes to the opioid epidemic in the United States. Darknet marketplaces are specialized hidden services that mediate transactions for illicit drugs and other illegal goods. The FBI and other law enforcement and intelligence agencies increasingly have access to massive data sets that document these transactions, with limited means to integrate this intelligence into investigations. These datasets include actionable information and strategic intelligence related to TOC networks such as Russian financial networks and transnational money laundering groups. The FBI, both at headquarters and throughout its field offices, needs to implement technical solutions to effectively extract this intelligence and target TOC networks.

In order to identify and target TOC networks, their facilitators, and their illegal proceeds, the FBI requests $5.3 million to develop the technology and systems required to exploit financial and other data sets and purchase software to leverage big data analytics for investigations. The FBI will use data exploitation and analysis to support investigations and operational efforts.

One example of the FBI's ongoing development of data exploitation and analytical capabilities is the targeting of criminal enterprises operating on the Darknet. Through manual data exploitation and analysis conducted by agents and analysts, the FBI has opened over 200% more investigative cases targeting these actors in FY2018 than FY2017. In March 2018, the FBI led Operation Disarray, a nationwide, joint law enforcement operation that targeted vendors and buyers of opioids and cocaine on the Darknet. The operation resulted over 160 interviews; 8 arrests; numerous search warrants; and seizures of weapons, drugs, counterfeit currency, and computer equipment. With development of big data analytics, the FBI would be able to identify and target significantly more of these actors and mitigate their criminal activities.

Technological Expertise: $8,900,000 (all non-personnel)

Technological change is reshaping the manner by which criminals operate. An ongoing evolution in communications has created new cross-border market opportunities, exposed a wider swath of society to transnational criminal activity, and fostered the growth of crime-as-a-service. Many criminals no longer require physical contact with victims, customers, or associated networks. The FBI must increasingly rely on online undercover operations and the establishment of virtual backstopping and covert identity functions to handle training, provide online backstopping, conduct research, and create products for investigators.

Because Darknet marketplaces are inherently reliant on the trust and confidence between buyers and sellers, a strategy of consistent law enforcement action against the most trusted and top drug vendors would promote the FBI's need to destabilize the Darknet and sow discord amongst its users. The FBI requests $2.7 million for the development of technical tools to exploit marketplace infrastructure and conduct more proactive outreach, while shifting law enforcement focus to target top vendors of illicit goods and services through prioritized undercover operations. The FBI needs to develop technically-

advanced solutions and expertise throughout the field to successfully conduct investigations that track, disrupt, and dismantle those TOC networks that rely on technology to obscure their criminal activities.

The FBI's Cellular Analysis Survey Team (CAST) currently provides field offices, legal attachés, and law enforcement partners with mobile telecommunications support during the course of their investigations. The FBI requests $3.8 million to better address this growing threat. Given the rapidly-changing technological environment, the FBI will establish a strategic technology team of existing personnel as well as contractors to provide technical expertise, as needed, to better assess both current and emerging capabilities to form a strategy for how to combat the use of advanced technology against law enforcement. To build the technical capabilities and platforms required to target TOC networks utilizing the internet (both Darknet and Clearnets) to distribute illicit goods (e.g., weapons, opioids, and other illegal narcotics) and conduct fraud schemes, the FBI requests $2.4 million for contract support, specialized technology and software, and additional training.

TOC networks increasingly rely on encrypted communications to plan and commit crimes, thus forcing the FBI to develop sophisticated technology and methods to disrupt their activities and dismantle their organizations. In March 2018, the FBI and international partners took down Phantom Secure, an encrypted communications service, which provided secure communications to high-level drug traffickers and other criminal organizations. Most of Phantom Secure's 10,000-20,000 users are the top-level leaders of nefarious transnational criminal organizations in the U.S. and abroad. This case is the first time the US Government targeted a company and its leaders for assisting a criminal organization by providing them with technology to evade law enforcement's detection of their crimes. By shutting down Phantom Secure, its criminal users no longer have a platform to conduct their criminal activities.

Impact on Performance

The TOC threat continues to evolve and expand through the use of advanced technologies which allows for crimes to be facilitated and obfuscated. In order to successfully target, disrupt, and dismantle TOC actors that have negative impacts on public safety, public health, and economic stability across the globe, the FBI needs additional resources. Without increased resources, the FBI will be unable to combat the growing threat emanating from abroad, as TOC groups increasingly exploit jurisdictional boundaries and technology to conduct their criminal activities outside the United States. This enhancement will enable the FBI to strategically target the largest TOC groups with the broadest reach and international impact, leading to an increased number of joint investigations with foreign partners and disruptions of criminal activity, both domestically and abroad. Furthermore, these joint efforts will serve as a force multiplier and will greatly improve the FBI's foreign partners' ability to combat TOC groups within their borders, thus mitigating the TOC threat through a minimal use of FBI resources.

With the increased scope of TOC actors, leveraging big data analytics and data exploitations is imperative. Without these resources, the most detrimental TOC groups will continue to evolve and expand, causing irreparable damage to U.S. security and interests. Exploiting new opportunities for infiltration and targeting of TOC networks, staying abreast of technological developments, and analyzing how criminals exploit new technology to advance their criminal operations is critical. Without the investment in advanced tools and training, the FBI will be unable to identify the evolving tactics, which TOC groups use to facilitate and hide their criminal activities.

Funding

Base Funding

FY 2018 Enacted				2019 Continuing Resolution				FY 2020 Current Services			
Pos	Agt	FTE	($000)	Pos	Agt	FTE	($000)	Pos	Agt	FTE	($000)
1,507	760	1,458	$231,965	1,537	792	1,480	$244,399	1,537	792	1,501	$252,097

Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2020 Request ($000)	FY 2021 Net Annualization (change from 2020) ($000)	FY 2022 Net Annualization (change from 2021) ($000)
Data Exploitation & Analysis	…	…	$5,300	($5,300)	…
Strategic Targeting	…	…	4,000	(4,000)	…
Technological Expertise	…	…	8,900	(8,900)	…
Total Non-Personnel	…	…	$18,200	$ (18,200)	…

Total Request for this Item

	Pos	Agt	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2021 Net Annualization (change from 2020) ($000)	FY 2022 Net Annualization (change from 2021) ($000)
Current Services	1,537	792	1,501	$241,187	$10,910	$252,097	…	…
Increases	…	…	…	…	18,200	18,200	(18,200)	…
Grand Total	1,537	792	1,501	$241,187	$29,110	$270,297	$(18,200)	…

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

Strategic Goals & Objectives: 1.1, 1.2, 3.1, 3.2, 4.1
Budget Decision Unit(s): Criminal Justice Services
Organizational Program: Criminal Justice Information Services

Program Increase: Positions 40 Atty 1 FTE 20 Dollars $4,228,000 ($366,000 non-personnel)

Description of Item

The FBI requests 40 positions and $4,228,000 ($366,000 non-personnel) to support the statutorily required firearm background checks conducted by the National Instant Criminal Background Check System (NICS) Section.

Justification

The FBI requests 40 positions and $4,228,000 to increase its capacity to perform NICS background checks for firearm purchases. The Brady Handgun Violence Prevention Act of 1993 allows a Federal Firearms Licensee (FFL) to legally transfer a firearm to a purchaser if the background check is not completed within three business days. The FBI has implemented technical refinements and operational efficiencies; however, the volume of calls, complexity of the work and introduction of new mandates, such as the Fix NICS Act require the FBI to request additional resources. Since FY 2017, the FBI has been able to take action on the majority of firearm background checks within the three business day mandate, as captured in the table below.

Calendar Year	Unresolved exceeded three business days
2016	303,146 (3.24%)
2017	310,232 (3.72%)
2018	275,879 (3.53%)

However, as a result of allocating additional resources to meet the statutorily mandated 3 day turnaround, backlogs have increased for other important activities, as shown below.

Activity	Backlogs Experienced		
	2016	2017	2018
Processing of Appeals	17 Months	26 Months	37 Months
Voluntary Appeal File Entries	17 Months	29 Months	37 Months
NICS Indices Updates*	NA	NA	20 Months

*The implementation of New NICS in August of 2016 caused several reports to be unavailable, the backlog statistics for NICS Indices are unavailable for 2016 and 2017.

The firearm background check volumes continue to increase and the Fix NICS Act, included in the Consolidated Appropriations Act of 2018, requires that erroneous information identified in an appeal

request must be corrected within sixty days. The requested additional staff will be used to help meet the sixty-day appeals mandate without allowing numerous firearm background checks to exceed the three business day deadline.

Additionally, for each of the positions requested, the FBI asks for an additional nearly $10,000 per employee to purchase professional call center telephone equipment. This will provide an advanced desktop phone capable of queuing calls for the next available employee and maintaining call center statistics such as length of time taken to answer each call, average hold duration for calls, and the number of dropped calls. The call center monitoring technology allows for separate statistics to be maintained for each employee so that additional training can be provided when necessary.

Impact on Performance

The FBI has identified significant performance gaps in the areas of:

- Initiating and completing NICS background checks for firearms purchases with the three-business-day timeframe;
- Conducting a search of the FBI's National Data Exchange (N-DEx);
- Completing appeals of NICS background check decisions in a timely manner; and
- Updating the NICS Indices and the Voluntary Appeal File in a timely manner.

With additional resources, FBI staff will be able to more consistently provide timely and accurate determinations of individuals' eligibility to possess firearms and/or explosives in accordance with federal law. The increase in FSL lessens the likelihood that firearm and explosives dealers could sell firearms and/or explosives to prohibited persons. Currently, the FBI redirects up to 298 personnel to assist in processing background checks, which causes an increase in backlogged work inother areas. The FSL increase would help to alleviate backlogs in NICS Appeals, the Voluntary Appeal File, explosives checks, and the NICS Indices. Additionally, the FSL increase would assist in completing a more comprehensive background check by allowing the FBI to conduct additional research during a background check by including an N-DEx search to assist in obtaining needed information. The ability to process background checks more efficiently would help to minimize the number of firearm sales to prohibited persons and decrease the workload for the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), the federal agency tasked with retrieving firearms from prohibited persons who are in possession of a firearm due to delays in a NICS final determination.

Funding

Base Funding

FY 2018 Enacted				FY 2019 Continuing Resolution				FY 2020 Current Services			
Pos	Agt/ Atty	FTE	($000)	Pos	Agt/ Atty	FTE	($000)	Pos	Agt/ Atty	FTE	($000)
679	…	662	$111,299	679	…	648	$102,964	679	…	648	$110,467

Personnel Increase Cost Summary

Type of Position/Series	Full-year Modular Cost per Position ($000)	1st Year Annual-ization	Number of Positions Requested	FY 2020 Request ($000)	2nd Year Annual-ization	FY 2021 Net Annuali-zation (change from 2020) ($000)	FY 2022 Net Annuali-zation (change from 2021) ($000)
Attorney	$256	$157	1	$157	$65	$65	$21
Professional Support	145	95	39	3,705	32	1,248	2,808
Total Personnel	**…**	**…**	**40**	**$3,862**	**…**	**$1,313**	**$2,829**

Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2020 Request ($000)	FY 2021 Net Annualization (change from 2020) ($000)	FY 2022 Net Annualization (change from 2021) ($000)
IT Equipment	10	36	$366	($366)	…
Total Non-Personnel	**…**	**…**	**$366**	**($366)**	**…**

Total Request for this Item

	Pos	Agt/ Atty	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2021 Net Annualization (change from 2020) ($000)	FY 2022 Net Annualization (change from 2021) ($000)
Current Services	679	…	648	$68,766	$41,701	$110,467	…	…
Increases	40	1	20	3,862	366	4,228	947	2,829
Grand Total	**719**	1	**668**	**$72,628**	**$42,067**	**$114,695**	**$947**	**$2,829**

Item Name: **National Vetting Center**

Strategic Goals & Objectives: 1.1, 2.1

Budget Decision Unit(s): Counterterrorism/Counterintelligence

Organizational Program: Counterterrorism

Program Increase: Positions 48 Agt 2 FTE 24 Dollars $16,595,000 ($11,515,000 non-personnel)

Description of Item

The FBI requests 48 positions (2 Special Agents) and $16,595,000 ($11,515,000 non-personnel) to effectively address the emerging requirements associated with the establishment of the National Vetting Center. Specifically, the requested resources will be used for the following efforts:

- Technical Capabilities
- Strategic Analysis

Justification

On February 6, 2018, the White House issued National Security Presidential Memorandum (NSPM)-9, *Optimizing the Use of Federal Government Information in Support of the National Vetting Enterprise*, to establish a National Vetting Center (NVC), which coordinates the efforts of federal agencies to vet people seeking to enter or remain within the United States. The NVC requires that departments and agencies improve their coordination and use of intelligence to identify potential threats to national security and public safety. The NVC will increase the government's ability to identify terrorists, criminals, and other nefarious actors, including those who seek a visa, visa waiver, an immigration benefit, or a protected status; attempt to enter the United States; or are subject to an immigration removal proceedings. In support of the NVC, the FBI is expected to provide timely information regarding the risk an individual poses.

The FBI currently participates in pre-adjudication vetting activities for Special Interest Visa (SIV) applicants, Non-immigrant Visa applicants (NIV), identified Special Interest Alien (SIA) travelers, and Security Advisory Opinion (SAO) processes, including Merlin refugees. The FBI also participates in post-adjudication vetting for visa waiver program-participating countries using the Electronic System for Travel Authorization (ESTA) and for Syrian/Iraqi Refugees and Asylees. The system assists authorities in determining whether an individual presents a law enforcement or security risk before being allowed to enter the United States. The U.S. Customs and Border Protection (CBP) is the adjudicating agency for ESTA and has established processing timeframes. The FBI's green and presumptive red responses, which are indicative of any derogatory information found in association to the applicant, must be returned to NVC within three hours of the ESTA application creation date. These preliminary findings are indicative of any derogatory information found in association to the applicant. Final determinations for presumptive red responses must be returned to NVC within 72 hours of the ESTA application creation date. ESTA applicants were prioritized for the first phase of NVC implementation; additional applicant categories will be prioritized in out-phases of NVC implementation. To meet the expected volume and timeframes for the additional applicant categories, the FBI requests additional resources.

Technical Capabilities: $10,015,000 (all non-personnel)

The FBI coordinates with other federal agencies to establish broad data and information sharing initiatives to streamline the vetting process, with the goal of ensuring that all relevant details pertaining to a foreign traveler seeking to enter the United States are known in advance. Accomplishing this goal requires the establishment of consistent vetting methodologies and the standardization of networks, systems, and data across the multi-enclave landscape of information classification.

To assist in the vetting of visa applications to the United States, the Foreign Terrorist Tracking Task Force (FTTTF) integrates the ESTA applications into a workflow to identify travelers with ties to groups, individuals, or organizations that pose potential criminal or national security threats. However, this integration is currently conducted manually and is very labor-intensive. FTTTF continues to work with US Government partners to build a program to better analyze the ESTA application data and provide a more comprehensive vetting process for applicants. The requested resources will provide the necessary infrastructure and services needed to handle receiving data from the various providers and increase procedural efficiency. Additional resources will allow for these data feeds to be consolidated, maintained, and distributed effectively. The development of complex technical tools and techniques will assist in the collection of information by automating processes and harmonizing databases. These enhanced capabilities are essential to adequately address the challenges of streamlining information and communicating to other external partners that participate in the NVC.

Strategic Analysis: 48 positions (2 Special Agents) and $6,580,000 ($1,500,000 non-personnel)

The FTTTF exploits intelligence intended to prevent travelers and their supporters, who are identified as potential threats, from entering the United States. FTTTF also leverages information that facilitates their location, detention, prosecution, removal, or other appropriate action. The FTTTF has worked the vetting mission since May 2017 and maintains a growing backlog. Each year, thousands of migrants present themselves at land-border crossings along the Southwest border, many of which qualify as special interest aliens (SIAs). Although there is no definitive government definition of an SIA, the term generally applies to persons emigrating from non-Western Hemisphere countries associated with a national security threat. The existing backlog of SIA requests will take 9 months to address with current technical capabilities and staffing levels.

Each year, the United States issues millions of Non-immigrant Visas (NIVs) to foreign nationals that intend to stay in the United States for a specified period of time, for a specific reason, without seeking permanent residency. Due to the large number of NIVs issued each year, and the numerous categories under which applicants can apply, the NIV process continues to be a primary avenue for criminal, foreign intelligence, and terrorist elements to enter the United States. As of March 2019, there was a backlog of 36,651 requests for NIV checks, which would take 231 months to eliminate with current staffing levels. SAO designations, issued by the State Department for applicants that are deemed a security concern, are a significant contributor to the backlog. These requests require in-depth review from various federal agencies, including the FBI. For SAO requests, the backlog as of March 2019 was 7,107 and would take approximately 103 months, just over eight and a half years, to eliminate at current resource levels.

The NVC's workload is anticipated to increase as its scope broadens and requests remain time consuming. The FBI requests resources for additional staffing levels and the development of new technology, in order to eliminate the backlog and to meet the NVC's adjudication timeline requirements.

If automation is funded and implemented, analysts will be able to quickly package and disseminate findings to the appropriate region for operational action. This rapid response will enable the FBI to proactively address potential national security risks.

In addition to applicant vetting, the FBI has the responsibility to investigate US based derogatory connections discovered in the vetting process. As a result, the FBI expects an increased investigative burden on agents and analysts in the field as demand increases. This enhancement will enable the FBI to research new solutions, develop new techniques, and streamline processes in order to make appropriate determinations regarding the potential threat posed by foreign travelers to the United States.

Impact on Performance

It is essential to enhance the FBI's capabilities by creating technical tools to extract and relay intelligence in a timely manner. With automation improvements, the FBI will be able to better address the backlog and reduce its response time. Additionally, streamlining the overall process and sharing information with NVC partners is critical. The ability to collect data and provide information in a timely manner is vital to protect public safety.

Funding

Base Funding

FY 2018 Enacted				FY 2019 Continuing Resolution				FY 2020 Current Services			
Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)	Pos	Agt	FTE	$(000)
87	21	81	27,897	83	20	81	38,281	83	20	81	38,610

Personnel Increase Cost Summary

Type of Position/Series	Full-year Modular Cost per Position ($000)	1st Year Annual-ization	Number of Positions Requested	FY 2020 Request ($000)	2nd Year Annual-ization	FY 2021 Net Annuali-zation (change from 2020) ($000)	FY 2022 Net Annuali-zation (change from 2021) ($000)
Special Agent	$346	$277	2	$554	($72)	($144)	$182
Intelligence Analyst	231	173	2	346	(9)	(18)	116
Professional Support	145	95	44	4,180	32	1,408	3,168
Total Personnel	**…**	**…**	**48**	**$5,080**	**…**	**$1,246**	**$3,466**

Non-Personnel Increase Cost Summary

Non-Personnel Item	Unit	Quantity	FY 2020 Request ($000)	FY 2021 Net Annualization (change from 2020) ($000)	FY 2022 Net Annualization (change from 2021) ($000)
Technical Capabilities	…	…	$10,015	($10,015)	…
Strategic Analysis	…	…	1,500	(1,500)	…
Total Non-Personnel	**…**	**…**	**$11,515**	**($11,515)**	**…**

Total Request for this Item

	Pos	Agt	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2021 Net Annualization (change from 2020) ($000)	FY 2022 Net Annualization (change from 2021) ($000)
Current Services	83	20	81	$13,465	$25,145	$38,610	…	…
Increases	48	2	24	5,080	11,515	16,595	(10,269)	3,466
Grand Total	**131**	**22**	**105**	**$18,545**	**$36,660**	**$55,205**	**($10,269)**	**$3,466**

Item Name: **Render Safe**

Strategic Goal: 1
Strategic Objective: 1.1
Budget Decision Unit(s): Counterterrorism/Counterintelligence

Organizational Program: Critical Incident Response

Program Increase: Positions 41 Agt 41 FTE 21 Dollars $17,157,000 ($5,800,000 non-personnel)

Description of Item

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

Item Name: **Counterintelligence**

Strategic Goal: 1
Strategic Objectives: 1.2, 1.3
Budget Decision Unit(s): Counterterrorism/Counterintelligence

Organizational Program: Counterintelligence

Program Increase: Positions 6 Agt 1 FTE 3 Dollars $18,266,000 ($17,202,000 non-personnel)

Description of Item

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

VII. Construction

Overview

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 FBI and DOJ look forward to working with OMB and Congress to secure the remaining funding needed for the HQ consolidation effort.

The FY 2020 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; Redstone Arsenal, Alabama; Pocatello, Idaho; and Quantico, Virginia.

FBI Clarksburg. The FBI Clarksburg campus encompasses nearly 1,000 acres in Clarksburg, West Virginia. The campus was originally the home to CJIS but has since expanded to house staff from nine other FBI Headquarters divisions and offices, including the HRD, FD, FLSD, and TSC among others. Additionally, the campus hosts staff from other government agencies, including the ATF, DHS, and Department of Defense (DoD). The campus, built on land acquired by the FBI, was completed in 1995. The heart of the complex is a 500,000-square foot main office building, which is nearly the length of three football fields. The campus also includes a central utility plant, shipping and receiving facility, visitor's center, and related support facilities. Approximately 3,600 FBI and other agency personnel work at the FBI Clarksburg campus.

With the emergence of advanced biometric technologies in law enforcement, intelligence, and defense activities, the FBI partnered with the DoD to construct the BTC at the Clarksburg campus. The BTC is a 360,000-square foot facility that houses both FBI and DoD personnel. Shortly after the BTC was completed in December 2015, the facility was renovated to accommodate a 10,000 square foot data center as part of the DOJ Data Center Transformation Initiative (DCTI).

FBI Redstone Arsenal. The U.S. Army has permitted approximately 1,600 acres of land at Redstone Arsenal to the FBI, which enables the FBI to enhance operational, operational support, technology, training, and research and development capabilities and capacities. The FBI, in close collaboration with Redstone Garrison Directorate of Public Works, seeks to leverage Redstone Arsenal's long-range goal to transform itself as a key U.S. government (defense and non-defense) research, development, test and evaluation center, and technology hub.

The FBI plan centers around three key opportunities:

- Creating a center for collocating FBI explosives and counter-IED programs and activities;
- Creating advanced and specialized training capacities and capabilities to address requirements that cannot be satisfied at the FBI Academy campus; and
- Creating options for FBI Executive management to proactively meet future operational and facilities requirements.

The FBI has secured sites in four Redstone Arsenal planning zones:

- North Campus, which presently consists of approximately 243 acres and has the potential to expand to approximately 400 acres, is located in the professional zone. The North Campus consists of three primary districts:
- South Campus, which consists of approximately 1,200 acres, is located in the industrial zone and consists of three districts:
- Academic Center is located in the city center zone. A site has been identified for a future permanent training center to replace the interim Redstone Training Center in operation near the site.
- Airfield Operations is located in the industrial zone adjacent to the Army airfield. This district is suitable for housing future FBI aviation operations and hangars. The district is also the proposed site for a future Huntsville Resident Agency (HRA). The proposed HRA would include space for the Tennessee Valley Regional Computer Forensics Laboratory (TVRCFL), currently operating in interim space, and the National Defense Cyber Alliance – an FBI/DoD/Contractor Community partnership focusing on cyber-attacks against the defense community.

FBI Pocatello. The Pocatello Information Technology Center (PITC) is an FBI-owned enterprise asset that houses over 200 employees from eight different FBI Headquarters divisions, the Salt Lake City Field Office, and the DOJ Office of the Chief Information Officer staff who support the DCTI. The FBI Pocatello site encompasses 17.5 acres of land.

The site, formerly a Naval Ordnance Plant, was purchased by the FBI in 1984 to serve as one of six planned regional computer support centers. Upon purchase, the FBI renovated the facility and constructed a data center, completed in 1987. FBI Headquarters Divisions and Offices with staff at FBI Pocatello include the OTD, ITID, ITADD, ITESD, CJIS, DI, RMD, FD, and FLSD.

Under the DOJ DCTI, the Department will reduce the number of data centers that exist today and consolidate into three Core Enterprise Facilities (CEFs) by the end of FY 2019. The FBI will host two of the three CEFs – one at FBI Clarksburg and one at FBI Pocatello. In October 2017, the FBI and local government leaders broke ground on a new 25,000 square foot data hall and 40,000 square foot office space, which will house approximately 250 staff to be relocated from the NCR under the HQ Consolidation strategy. The project includes telecommunications upgrades, parking expansion, security improvements, and related site upgrades to accommodate the increased mission and personnel. Upon completion, FBI Pocatello will support Department-wide data operations, complementing its counterpart data center at FBI Clarksburg. The new data center and office space project is expected to be completed in November 2018.

The Naval Ordnance Plant facility was constructed in 1977; the current 15,000 square foot data hall was added by the FBI in 1985. Through the years, the facility has received minimal repairs and upgrades. Consequently, the FBI has invested to upgrade and replace key elements of the campus infrastructure. The information technology systems operated from the FBI Pocatello data center are core FBI and Department systems that must be available 24x7 to satisfy mission requirements.

FBI Quantico. The journey for every FBI employee starts at the FBI Academy. It hosts world-class Special Agent, Intelligence Analyst, and Professional Staff training, equipping them with the skills to investigate the nation's most critical threats. But the Academy doesn't only train FBI employees – it is also home to the best and brightest law enforcement personnel from around the world for 10 weeks at the National Academy and 2 weeks at the Law Enforcement Executive Development Seminar, as well as critical private sector partners. Quantico has become a premier learning and research center, a model for best practices throughout the global criminal justice community, and most importantly, a place where lasting partnerships are forged among law enforcement and intelligence professionals worldwide.

Over the years, the Quantico complex has grown from supporting a single FBI entity and mission – Training Division – to a multi-tenant/multi-mission venue. In addition to serving as a national training asset, Quantico also houses key operational entities, including the FBI's Critical Incident Response Group (CIRG), the Bureau's Laboratory (LAB), Facilities and Logistics Services (FLSD), and Operational Technology Divisions (OTD). Today, the FBI Quantico site encompasses nearly 2.3 million sq. ft. of facilities and supports approximately 3,400 personnel, 13,500 students, and 20,000 visitors annually.

FBI Winchester. Construction of the Central Records Complex (CRC) in Frederick County, Winchester, Virginia began in April 2017. Facility completion is estimated in 2020. The CRC will centralize FBI records from around the world, including FBI Headquarters, field offices, and legal attaches. The CRC will ensure FBI records are stored in a facility which is compliant with the National Archives and Records Administration's federal records storage standards.

In addition to records storage, the new facility will include office space, a visitor screening area, a guard booth, and parking. The facility will house more than 400 Information Management Division personnel.

The Interim Central Records Complex and the Administration and Training Building will house the remainder of the division's personnel.

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.

(CANCELLATION)

Of the unobligated balances available under this heading, $159,000,000 are hereby permanently cancelled: Provided, That no amounts may be cancelled from amounts that were designated by the Congress as an emergency requirement pursuant to the Concurrent Resolution on the Budget or the Balanced Budget and Emergency Deficit Control Act of 1985.

Note.—A full-year 2019 appropriation for this account was not enacted at the time the budget was prepared; therefore, the budget assumes this account is operating under the Continuing Appropriations Act, 2019 (Division C of P.L. 115–245, as amended). The amounts included for 2019 reflect the annualized level provided by the continuing resolution.

Analysis of Appropriations Language

- No substantive change

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
CBP	Customs and Border Patrol
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
ESTA	Electronic System for Travel Authorization
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
MCAS	Malicious Cyber Actor System
NBTF	National Border Corruption Task Force
NCIC	National Crime Information Center
NCIJTF	National Cyber Investigative Joint Task Force
NCPC	National Counterproliferation Center
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
NIV	Non-immigrant Visa
NJTTF	National Joint Terrorism Task Force
NRES	Network Requirements and Engineering Services
NVC	National Vetting Center
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
SAO	Security Advisory Opinion
SAR	Suspicious Activity Reports
SCC	IC Security Coordination Center
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facilities
SCINet	Sensitive Compartmented Information Operations Network
SIA	Special Interest Alien
SIG	Special Interest Group
SIOC	Strategic Information and Operations Center
SIT	System Integration and Test
SIV	Special Interest Visa
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
UAS	Unmanned Aerial Surveillance
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