FY 2023 President's Budget Request

March 2022

Table of Contents

I. Overview

A. Introduction

Budget Request Summary: The Federal Bureau of Investigation's (FBI's) Fiscal Year (FY) 2023 budget request proposes a total of $10,803,573,000 in direct budget authority, of which $10,741,678,000 is for Salaries and Expenses (S&E) and $61,895,000 is for Construction.

The S&E request includes a total of 36,945 direct positions and 35,264 direct full time equivalents (FTE); the positions include:

- 13,616 Special Agents (SAs)
- 3,287 Intelligence Analysts (IAs)
- 20,042 Professional Staff (PS)

The S&E program increases total $324,556,000; 789 positions (202 SAs, 71 IAs, and 516 PS), and 401 FTE, for the following:

- $51,975,000 for cyber investigative capabilities
- $48,826,000 to counter acts of mass violence and threats to public safety
- $34,142,000 for counterintelligence matters
- $20,574,000 to combat crime and corruption
- $17,786,000 for civil rights
- $36,948,000 for cybersecurity
- $16,928,000 for data analytics and the development of technical tools
- $8,092,000 for UTS
- $27,351,000 for implementation of a federal body worn camera program
- $39,420,000 for the operations and maintenance of the 21st century facilities program
- $22,513,000 to address resource needs resulting from *McGirt*

The request includes $0 in technical adjustments and $203,265,000 adjustments to base (ATBs) for continued support of the FBI's base resources.

The $61,895,000 requested in the Construction account will maintain the Secure Work Environment (SWE) program.

The FBI continues to strategically assess current and prospective operations to ensure it meets mission requirements at the lowest possible cost to the U.S. taxpayer. The FY 2023 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 submissions can be viewed or downloaded from the Internet at: http://www.justice.gov/doj/budget-and-performance.

The FBI's Mission: To protect the American people and uphold the Constitution.

The FBI Vision: Ahead of the threat.

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

- Strategic Goal 1: Uphold the rule of law
- Strategic Goal 2: Keep our country safe
- Strategic Goal 3: Protect civil rights
- Strategic Goal 4: Ensure economic opportunity and fairness
- Strategic Goal 5: Administer just court and correctional systems

The FBI Strategy: The FBI Strategy includes several integrated elements: Mission, Vision, Mission Priorities, and Enterprise Objectives. The mission of the FBI is to *Protect the American People and Uphold the Constitution*, with a vision to stay *Ahead of the Threat*. The vision specifies the FBI's desired strategic direction, accomplished by continuously evolving the organization to mitigate existing threats and anticipate future threats. Focusing strategic efforts across the enterprise, the FBI has eight mission priorities and thirteen enterprise objectives, organized by four guiding principles.

Mission Priorities:

1. Protect the U.S. from terrorist attack
2. Protect the U.S. against foreign intelligence, espionage, and cyber operations
3. Combat significant criminal cyber activity
4. Combat public corruption at all levels
5. Protect civil rights
6. Combat transnational criminal enterprises
7. Combat significant white-collar crime
8. Combat significant violent crime

Enterprise Objectives:

People

- Promote a culture of development and resilience
- Assemble diverse teams
- Cultivate leadership and mentorship
- Recruit for the future

Partnerships

- Integrate meaningful partnerships
- Improve information sharing
- Increase community engagement

Process

- Strengthen confidence and trust
- Enhance rigor and accountability
- Align resources to priorities

Innovation

- Foster innovation and creativity
- Enhance data capabilities and digital expertise
- Promote user-driven technology

The FBI's tracks the execution of its enterprise objectives - via the Enterprise Strategy process - by cascading enterprise objectives and executing strategic initiatives towards these objectives within branch and division strategies. This vertical alignment within the organization ensures the FBI enterprise is strategically focused on the same objectives and working collectively towards the FBI mission and vision. Strategy review meetings are held with the Director and each branch and division to discuss progress towards the enterprise objectives throughout the fiscal year, and the FBI's executive management routinely evaluates the organization's progress.

The FBI tracks the execution of its mission priorities via national threat strategies across headquarters operational and intelligence programs, field offices, and legal attaché (legat) offices through the Integrated Program Management (IPM) and Threat Review and Prioritization (TRP) processes. These processes enable threat issues to be identified across the organization to subsequently develop accompanying threat mitigation strategies. Every two years, headquarters operational divisions prioritize national threats, determine FBI National Threat Priorities (NTPs), and develop national threat strategies and guidance for threat mitigation. The 56 field offices and 60+ legat offices use this national guidance to formulate a field and legat office threat prioritization and complete their own specific strategies. These threat and program strategies undergo mid-year and end-of-year evaluations, and each individual field and legat office is held accountable to their performance targets. FBI executives and program managers hold regular meetings to review and evaluate field office and legat office effectiveness throughout the fiscal year, providing feedback to offices to align their work with national strategies or platforms.

The FBI's budget strategy and future resource requirements and requests are designed to enable the FBI to address the current range of threats while also focusing on the future needs of the FBI. An increasing number of the FBI's programs and initiatives are multi-year in nature, and require phased development, deployment, and operations or maintenance funding. Moreover, a multi-year planning approach allows FBI management to better understand the implications of proposed initiatives. This FY 2023 budget request is designed to promote capabilities and strategies that are sufficiently agile to meet ongoing, emerging, and unknown national security, cyber, and criminal threat.

Organization of the FBI: The FBI operates field offices in 56 major U.S. cities and approximately 350 resident agencies (RAs) throughout the country. RAs are satellite offices, typically staffed with fewer than 20 people, 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 (SACs) and Assistant Directors in Charge (ADICs) of FBI field offices report directly to the Director and Deputy Director.

The FBI also operates 63 legat offices and 34 sub-offices in more than 79 countries around the world. These offices are typically staffed with fewer than 10 people who enable the FBI's presence in these countries and liaise with foreign counterparts and partners. These numbers fluctuate based on the global threat environment.

FBI Headquarters, located in Washington, D.C., provides centralized operational, policy, and administrative support to FBI investigations and programs. 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), the Counterintelligence Division (CD), and the Weapons of Mass Destruction Directorate (WMDD).
- The Intelligence Branch (IB), which includes the Directorate of Intelligence (DI), the Office of Partner Engagement (OPE), and the Office of Private Sector (OPS).
- 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), the International Operations Division (IOD), and the Victims Services Division (VSD).

- 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).

Several other headquarters offices also provide FBI-wide mission support:

- The Information and Technology Branch (ITB) oversees the IT Enterprise Services Division (ITESD), the IT Applications and Data Division (ITADD), and the IT Infrastructure Division (ITID).
- The Human Resources Branch (HRB) includes the Human Resources Division (HRD), the Training Division (TD), and the Security Division (SecD).
- Administrative and Financial Management Support is provided by the Finance and Facilities Division (FFD), the Information Management Division (IMD), the Resource Planning Office (RPO), the Office of Internal Auditing (OIA), the Office of Integrity and Compliance (OIC), the Insider Threat Office (InTO), the Office of Chief Information Officer (OCIO), 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), and the Office of the Ombudsman.

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

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

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

- Based on core mission function: Certain FBI divisions support one mission area exclusively, and thus are allocated entirely to the corresponding decision unit. For example, all of the resources of the DI are allocated to the Intelligence Decision Unit, while all of the resources of the CJIS Division are allocated to the CJS decision unit.

- Based on workload: Critical investigative enablers, such as the LD, the 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 FFD, 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

To better address all aspects of the FBI's mission requirements, the FBI formulates and structures its budget according to the threats the FBI works to detect, deter, disrupt, and dismantle. The FBI identifies and aligns resources to the top priority threats through the IPM and TRP processes.

Domestic Terrorism (DT): For more than a century, the FBI has occupied a critical role in protecting the U.S. from threats to American public safety, borders, economy, and way of life.

Domestic terrorists who are motivated by a range of ideologies and galvanized by recent political and societal events in the United States pose an elevated threat to the Homeland in 2023. Enduring DT motivations pertaining to biases against minority populations and perceived government overreach will almost certainly continue to drive DT radicalization and mobilization to violence. Newer sociopolitical developments—such as narratives of fraud in the recent general election, the emboldening impact of the violent breach of the U.S. Capitol, conditions related to the COVID-19 pandemic, and conspiracy theories promoting violence—will almost certainly spur some domestic terrorists to try to engage in violence this year.

Domestic terrorists exploit a variety of popular social media platforms, smaller websites with targeted audiences, and encrypted chat applications. They use these platforms to recruit new adherents, plan and rally support for in-person actions, and disseminate materials that contribute to radicalization and mobilization to violence.

Several factors could increase the likelihood or lethality of DT attacks in 2023 and beyond, including escalating support from persons in the United States or abroad, growing perceptions of government overreach related to legal or policy changes and disruptions, and high-profile attacks spurring follow-on attacks and innovations in targeting and attack tactics.

DT lone offenders will continue to pose significant detection and disruption challenges because of their capacity for independent radicalization to violence, ability to mobilize discretely, and access to firearms.

Terrorism: The FBI continues to work to identify individuals who seek to join the ranks of foreign fighters traveling in support of the Islamic State of Iraq and ash-Sham (ISIS), as well as homegrown violent extremists (HVE) who may aspire to attack the U.S. from within. These terrorism threats remain among the highest priorities for the FBI and the U.S. Intelligence Community (USIC).

The conflicts in Syria and Iraq have served as the most attractive overseas theaters for Western 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 have used these travelers to facilitate terrorist activity beyond Iraq and Syria, particularly in their home countries, because returning foreign fighters can radicalize members of the communities that they came from originally.

ISIS has aggressively promoted its hateful message – attracting like-minded extremists, including Westerners – and has persistently used the Internet to communicate. 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 now spreads faster than thought possible just a few years ago through all forms of technology.

ISIS remains a highly agile, resilient, and adaptive adversary. ISIS – which currently operates in at least 20 countries – continues to pose a threat to U.S. interests, both domestically and abroad, through the group's ability to drive attacks, provision of tactical guidance, and contribution to the radicalization and mobilization of U.S. persons, primarily through its official and unofficial online propaganda. ISIS continues to call on its worldwide members and supporters to launch attacks where they are located, using any means available, and virtual networks of ISIS members and supporters continue to collaborate and share tactics in efforts to promote attacks around the globe.

As a communication medium, social media is a critical tool exploited by terror groups. One recent example includes an individual 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 networking site with other like-minded individuals.

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 HVEs often act with little to no warning. The FBI has HVE cases that span all 56 FBI field offices across all 50 states.

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 – for example, students and visiting scientists, scholars, and business executives – as well as cyber-based tools to target, penetrate, and influence U.S. institutions.

Notable successes include espionage convictions of three former USIC officers in cases demonstrating the threat posed by Chinese intelligence services targeting former U.S. security clearance holders for recruitment. In March 2019, former Defense Intelligence Agency (DIA) officer and retired U.S. Army warrant officer Ron Rockwell Hansen pleaded guilty to attempted espionage, admitting he regularly met with Chinese intelligence officers in China and received hundreds of thousands of dollars in compensation for information he illegally provided. In May 2019, former Central Intelligence Agency (CIA) officer Jerry Chun Shing Lee pleaded guilty to conspiring to commit espionage, admitting he created documents detailing intelligence provided by CIA assets, including true names of assets, operational meeting locations, and phone numbers, and information about covert facilities in response to taskings from Chinese intelligence officers, who paid him hundreds of thousands of dollars and offered to take care of him "for life" in exchange for his cooperation. Also in May 2019, former CIA case officer and DIA intelligence officer Kevin P. Mallory was sentenced to 20 years in prison after a federal jury convicted him of conspiring to transmit national defense information – including unique

identifiers for confidential human sources who had helped the USG – to a Chinese intelligence officer.

Cyber: China, Russia, Iran, and North Korea pose the highest threat to the U.S. for cyber espionage, theft, and attacks. The FBI anticipates all U.S. adversaries and strategic competitors will increasingly build and integrate cyber capabilities to influence U.S. policies and advance their national security interests. In FY 2020-2021, both cyber criminals and foreign states used cyber intrusions to exploit the COVID-19 pandemic for their own gain, taking advantage of vulnerabilities presented by the rapid shift to increased online activity, public appetite for pandemic-related information, and the criticality of essential services and infrastructure networks. Threatening safe and efficient delivery of therapy options, several of China's most effective and prolific cyber actors have focused their efforts to target companies, universities, and laboratories reportedly working on COVID vaccines and treatments.

COVID-related cyber intrusions are just the latest example of how criminals and states use cyber capabilities to exploit perceived gaps in the U.S. system: between foreign and domestic authorities, national security and criminal law enforcement, and government and private sector stewardship of critical networks. The FBI is uniquely positioned to bridge the gaps.

In FY 2021, the SolarWinds hacks and Microsoft Exchange zero-day vulnerabilities demonstrated that the U.S.'s adversaries are investing significant resources to plan and conceal their malicious operations. Nation-state actors also are collaborating with profit-motivated hackers to form a blended threat against the U.S.—one that the FBI's blend of criminal and intelligence authorities is uniquely positioned to address.

The FBI's strategy to impose risk and consequences on cyber adversaries focuses on disrupting threats not only through our own actions but also by sharing information and conducting joint, sequenced operations with partners.

The FBI is implementing a strategy to impose risk and consequences on cyber adversaries through unique authorities, world-class capabilities, and enduring partnerships. The strategy provides needed human and technical resources to enable FBI partners to defend networks, attribute malicious activity, sanction bad behavior, and attack adversaries overseas.
As part of this strategy, and consistent with recommendations of the U.S. Cyberspace Solarium Commission, the FBI has elevated the leadership, engagement, and coordination assets of the FBI-led multiagency National Cyber Investigative Joint Task Force, creating new mission centers based on key cyber threat areas. These mission centers are led by senior executives from partner agencies, integrating operations and intelligence across agency lines to sequence actions for maximum impact against cyber adversaries.

For example, a FY 2020 joint FBI/NSA Cybersecurity Advisory disclosed a significant tool developed by Russian Military Intelligence (GRU). The FBI used criminal processes, including close coordination with foreign partners, to obtain key data for the report that corroborated NSA's findings and allowed an unclassified release. The timing created a painful disruption to a well-known adversary, as development of the tool required significant investment by GRU, and reconstituting their capabilities will require substantial time and resources.

White Collar Crime: The White Collar Crime (WCC) program addresses public corruption, border corruption, corporate fraud, securities/commodities fraud, mortgage fraud and other

financial institution fraud, health care fraud, other complex financial crimes (insurance, bankruptcy, and mass marketing fraud), and intellectual property rights.

Public corruption, the FBI's number one criminal investigative priority, involves the corruption of local, state, and federally elected, appointed, or contracted officials who undermine our democratic institutions and threaten public safety and national security. U.S. public officials and employees are vulnerable to exploitation from individual actors, businesses, corporations, foreign actors, and criminal organizations who seek to use the official's access and influence over government spending, policies, and processes. Government fraud such as this can severely damage and impede U.S. border security, electoral processes, neighborhood safety, judicial integrity, and public infrastructure quality (such as schools and roads). To counter this threat, the FBI cooperates and coordinates with its state, local, and tribal law enforcement partners.

The FBI's public corruption program also focuses on border corruption. The documented presence of corrupt border officials facilitates a wide range of illegal activities along both 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 facilitating the movement of contraband across the borders. To help address this threat, the FBI established the Border Corruption Initiative, which has developed a threat-tiered methodology that targets border corruption at all land, air, and seaport, with the idea of mitigating the threat posed to national security.

The FBI has investigated election-related crimes, which are also covered under the public corruption program, for over three decades. These frauds and schemes run the gamut – they include ballot fraud, election or polling place abuses, false voter registration, violations of campaign finance laws, bribes of public officials, and voter intimidation and suppression (covered under the FBI's civil rights program). These crimes can have a devastating effect on elections, as well as the public's faith in electoral processes. If a voter receives threats or is otherwise prevented from voting, this constitutes a civil rights violation. The FBI is focused on preventing and stopping these crimes and has election crimes coordinators in all 56 field offices who regularly receive specialized training on election crimes and voter fraud.

The FBI investigates a variety of financial crimes, including money laundering, health care fraud, elder fraud, corporate fraud, securities/commodities fraud, bank fraud, financial institution fraud, investment fraud, and intellectual property rights crimes.

The FBI is committed to rooting out money laundering facilitators and organizations, which involves masking the source of criminally derived proceeds so the proceeds appear legitimate or masking the source of money used to promote illegal conduct. Money laundering generally involves three steps: placing illicit proceeds (which could include virtual assets and currencies) into legitimate financial systems; layering, or the separation of the criminal proceeds from their origin; and integration, or the use of apparently legitimate transactions to disguise the illicit proceeds. Once criminal funds have entered legitimate financial systems, the layering and integration phases make it difficult to trace the money. The FBI combats these illicit activities by working with the financial industry and its law enforcement partners to trace money flows and identify launderers. Specifically, the FBI targets professional money laundering gatekeepers/controllers, such as attorneys and financial institutions, since addressing these

enablers has a larger disruption and dismantlement effect on criminal activities than focusing exclusively on the underlying unlawful activity.

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. The FBI also actively investigates crimes targeting and disproportionately affecting seniors, in support of the Elder Abuse Prevention and Prosecution Act. Many of these crimes are linked to health care, but they can include a host of other scams. To counter these threats, the FBI participates in several working groups and task forces, including health care fraud task forces.

Corporate fraud encompasses numerous schemes, including falsifying financial information with bogus accounting, fraudulent trades that inflate profit or hide loss, illicit transactions to evade regulatory oversight, self-dealing by corporate insiders, including embezzlement, misuse of corporate property for personal gain, and solicitation, offer, receipt, or provision of kickbacks for corrupt corporate activity. Fabricating financial documents to obscure or elevate the perception of a corporation threatens the integrity of regulatory processes, investment activities, and long-term corporate viability. The FBI has worked with numerous organizations in the private industry to increase public awareness about combatting corporate fraud and has also formed partnerships with various agencies, including the Securities and Exchange Commission, to increase expertise in this area, facilitate case referrals, and foster technical assistance. In addition, the FBI coordinates with its law enforcement partners to investigates insider trading, which is the purchase or sale of securities based on material, non-public information.

To enforce intellectual property rights, the FBI disrupts and dismantles international and domestic criminal organizations that manufacture or traffic in counterfeit and pirated goods and/or steal, distribute, or otherwise profit from the theft of intellectual property. The FBI works to combat these types of crimes by collaborating with the public and private sectors, to include third-party entities like online marketplaces, payment service providers, and advertisers to obtain intelligence, gather leads, and identify criminal activities.

Transnational Criminal Organizations (TCOs): More than a decade ago, organized crime was characterized by hierarchical organizations, or families, that exerted influence over criminal activities in neighborhoods, cities, or states. But organized crime has changed dramatically. Today, international criminal enterprises run multi-national, multi-billion-dollar schemes from start to finish. Modern-day criminal enterprises are flat, fluid networks with global reaches. While still engaged in many of the "traditional" organized crime activities of loansharking, extortion, and murder, modern criminal enterprises target stock market fraud and manipulation, cyber-facilitated bank fraud and embezzlement, drug trafficking, identity theft, human trafficking, money laundering, alien smuggling, public corruption, weapons trafficking, kidnapping, and other illegal activities. TCOs exploit legitimate institutions for critical financial and business services to store or transfer illicit proceeds.

Preventing and combatting transnational organized crime demands a concentrated effort by the FBI and federal, state, local, tribal, and international partners. In FY 2020, the FBI led over 100 organized crime and major theft task forces targeting TCO networks based in the Eastern and Western Hemispheres. The FBI has also focused on improving and expanding domestic and

international partnerships and optimizing intelligence and operations collaboration through assistant legal attachés and overseas vetted teams or task forces to support efforts against transnational criminal organizations abroad.

Illicit drug trafficking continues to be a growing threat. Large amounts of high-quality, low-cost heroin and illicit fentanyl are contributing to record numbers of overdose deaths and life-threatening addictions nationwide. The accessibility and convenience of the drug trade online contributes to the opioid epidemic in the U.S. TCOs introduce synthetic opioids to the country's market, including fentanyl and fentanyl analogues. To address this evolving threat, the FBI is taking a multi-faceted approach with multiple initiatives and units across the criminal program. For example, in January 2018, the DOJ's Office of the Deputy Attorney General directed the FBI and other federal law enforcement partners to develop a strategic plan to disrupt and dismantle marketplaces facilitating fentanyl and opioid distribution. As a result, the FBI established the Joint Criminal Opioid Darknet Enforcement (J-CODE) Initiative, which brings together agents, analysts, and professional staff with expertise in drugs, gangs, health care fraud, and more, with federal, state, and local law enforcement partners from across the U.S. government. J-CODE developed a comprehensive, multi-pronged criminal enterprise strategy to target fentanyl and opioid trafficking on 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 the investigation and prosecution of these marketplaces.

Violent Crime and Gangs: Violent crime and gang activities exact a high toll on individuals and communities. Many of today's violent actors and gangs are sophisticated and well organized. They use violence to control neighborhoods and boost illegal money-making activities, including robbery, drug and gun trafficking, fraud, extortion, and prostitution. These violent actors do not limit their illegal activities to single communities. The FBI works across jurisdictions, which is vital to the fight against violent crime in big cities and small towns across the nation. FBI agents work in daily partnerships with federal, state, local, and tribal officers and deputies on joint task forces and individual investigations.

FBI joint Violent Crime and Safe Streets Gang Task Forces (VGSSTFs) identify and target major groups operating as criminal enterprises. In FY 2020, the FBI led 173 VGSSTFs and 52 Violent Crime Task Forces. Much of the FBI's criminal intelligence is derived from state, local, and tribal law enforcement partners with in-depth community knowledge. Joint task forces benefit from FBI investigative expertise, surveillance, technical, and intelligence resources, while FBI confidential sources track gangs and violent actors to identify emerging trends. Through multi-subject and multi-jurisdictional investigations, the FBI concentrates efforts on high-level groups and crime engaged in patterns of racketeering. This investigative model enables the FBI to target senior gang leadership and develop enterprise-based prosecutions.

The FBI has dedicated resources to combat the threat of violence posed by MS-13. The atypical nature of this gang has required a multi-pronged approach, working through U.S. task forces, and simultaneously gathering intelligence and aiding international law enforcement partners through the FBI's Transnational Anti-Gang Task Forces (TAGs). Initially established in El Salvador in 2007 through the FBI's National Gang Task Force, the San Salvador legat, and the U.S. Department of State, each TAG is a fully operational unit responsible for investigating MS-13 operating in the Northern Triangle of Central America and threatening the U.S. This program combines the expertise, resources, and jurisdiction of participating agencies involved in

investigating and countering transnational criminal gang activity in the U.S. and Central America. There are TAGs in El Salvador, Guatemala, and Honduras, and they are achieving substantial success in countering the MS-13 threat.

Crimes Against Children and Human Trafficking: The FBI has several programs to arrest child predators and recover missing and endangered children, including the Child Abduction Rapid Deployment (CARD) Team, the Child Sex Tourism (CST) Initiative, the Innocence Lost National Initiative (ILNI), the Innocent Images National Initiative (IINI), 86 Child Exploitation and Human Trafficking Task Forces, and 65 international violent crimes against children task force officers. The FBI has nationwide capacity to:

- Provide rapid, proactive, intelligence-driven investigative response to sexual victimization of children, other crimes against children, and human trafficking
- Identify and recover victims of child exploitation and human trafficking
- Reduce the vulnerability of children and adults to sexual exploitation and abuse
- Reduce the negative impact of domestic and international parental rights disputes
- Strengthen federal, state, local, tribal, and international law enforcement agencies through training, intelligence-sharing, technical support, and investigative assistance

In 2005, the FBI created the CARD Team to provide a nationwide resource to support investigations of child abductions and critically missing children. CARD is composed of agents and intelligence analysts who provide investigative and technical resources to law enforcement agencies following a child abduction. CARD members attend specialized training on child abduction investigative search techniques and technology and develop best practices through operational experience. CARD is supported by the FBI's Behavioral Analysis Unit: Crimes Against Children, which assists with offender characteristics, victimology, and investigative, interview, and media strategies. CARD is a nationwide resource to law enforcement at no cost to the requesting agency. The CARD priority is to provide timely response to recover abducted children and arrest abductors. Deployed 174 times since its inception, CARD has aided in rescuing 80 live children, as well as arresting numerous offenders.

The CST Initiative is a collaborative effort with multiple foreign partners that identifies and prosecutes Americans who travel overseas to engage in sexual activity with minors or who cause the sexual abuse of a child located overseas, and rescues the child victims. CST has successfully organized and participated in capacity-building for foreign law enforcement, prosecutors, and non-government organizations to better address this threat.

In June 2003, the FBI, with support from DOJ and technical assistance from the National Center for Missing and Exploited Children (NCMEC), implemented the ILNI to address children recruited into commercial sex by sex traffickers. Under the ILNI, the FBI conducts nationwide operations to recover children from sex traffickers and coordinate victim services for identified victims. In coordination with federal, state, local, and tribal law enforcement partners, the FBI uses sophisticated investigative techniques in an intelligence-driven approach to dismantle sex trafficking organizations.

Indian Country Crimes: 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 native subjects, and state and local law enforcement generally do not have jurisdiction within reservation boundaries. In FY 2020 (as of August 20), there had been 935 arrests, 882 indictments/informations/complaints, and 545 convictions in Indian Country.

The Indian Country and Special Jurisdiction Unit (ICSJU) 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. ICSJU supports joint investigative efforts with the Bureau of Indian Affairs and tribal law enforcement agencies and manages and conducts essential investigative training for 21 Safe Trails Task Forces, as well as approximately 150 FBI agents and law enforcement partners focused on Indian Country crimes. Although Indian Country cases are generally reactive, many are cross-programmatic in nature, including Indian gaming, public corruption, and complex financial fraud.

Civil Rights: The FBI has primary responsibility to investigate all alleged violations of federal civil rights laws that protect all citizens and persons within the U.S., including hate crimes, color of law (COL), and the Freedom of Access to Clinic Entrance (FACE) Act. The FBI is also the lead investigative agency responsible for investigating election fraud and voter suppression.

A hate crime is a traditional criminal offense, such as murder, arson, or vandalism, motivated wholly 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. Investigating hate crimes is the leading priority of the FBI's civil rights program, due to the devastating physical, emotional, and psychological toll these crimes take on individuals, families, and communities. Through training, public outreach, law enforcement support, and investigations, the FBI takes a multi-faceted approach to detect, deter, and investigate hate crimes.

COL violations are actions taken by any person using the authority given them by a government agency to willfully deprive someone of a right, privilege, or immunity secured or protected by the Constitution of the United States. 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. To prevent these types of crimes, the FBI is focused on training and educating state, local, and federal law enforcement agencies as to the role of the FBI in investigating violations under the federal color of law statute.

Under the FACE Act, the FBI has the sole investigative responsibility for conducting investigations of intimidation including murder, death threats, invasions, burglaries, and other acts. The number of FACE Act violations remains relatively low, with occasional spikes during dates marking significant events in the pro-choice and pro-life movements. The FBI's civil rights program investigates FACE Act violations in conjunction with its domestic terrorism counterparts.

The civil rights program also investigates voter suppression, as it is a civil rights violation to cause any individual to desist from voting or to pressure an individual to vote a certain way. The FBI investigates any tactics designed to prevent qualified voters from effectively voting by deceiving them as to the time, place, or manner of an election.

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 partners in federal, state, and local law enforcement, and the U.S. intelligence and private-sector communities. The IB oversees the intelligence program implementation of its six areas of focus: workforce success, culture and mindset, technology capabilities, information sharing, collection, and exploitation and analysis.

The Executive Assistant Directors (EADs) for the IB, NSB, and CCRSB work closely to manage all the FBI's intelligence and national security operational components, including the CD, the CTD, the CyD, the DI, the High-Value Detainee Interrogation Group (HIG), the Terrorist Screening Center (TSC), and the WMDD. Additionally, the IB coordinates the management of the FBI's National Intelligence Program (NIP)-scored resources, supporting engagement with FBI partners as well as intelligence-related training, technology, and secure work environments.

The IB EAD heads the FBI intelligence program, ensuring national security and law enforcement intelligence collection, production, and domain management are consistent with national priorities and adhere to tradecraft standards, policies, and processes. The EAD 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 EAD provides oversight of the FBI intelligence workforce, serves as Executive Agent for the National Virtual Translation Center, and is responsible for the FBI's foreign language program.

The FBI uses intelligence to understand criminal and national security threats and to conduct operations to dismantle or disrupt those threats. Two ways the FBI does this are:

- The FBI uses a standardized model for field intelligence that can adapt to the size and complexity of small, medium, and large offices. There are 56 intelligence programs, with one in each FBI field office.
- Fusion cells are intelligence teams in operational divisions designed to integrate all aspects of the intelligence cycle for a unique threat. Fusion cells integrate intelligence and operations and collaborate across work roles to ensure intelligence drives and supports operations. Fusion Cells consist of intelligence analysts who perform 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 operational personnel.

II. Summary of Program Changes

Item Name	Description	Pos.	FTE	Dollars ($000)	Page
Salaries and Expenses Enhancements					
Cyber	The requested resources will increase the FBI's capacity for unilateral, joint, and enabled operations with other federal, state, local and international partners. The request focuses on the development of three critical areas: cyber threat identification, analysis, and attribution; cyber threat intelligence platform; and incident response.	137	70	$51,975	61
Countering Acts of Mass Violence and Threats to Public Safety	With the requested resources, the FBI will be able to better address national security threats by detecting and disrupting domestic terrorism activities, increasing information sharing with law enforcement partners, and expanding the capacity to handle incoming tips from the public and to perform firearms background checks.	208	105	48,826	62
Counterintelligence	This request is classified.	88	46	$34,142	75
Combatting Crime and Corruption	This request will allow the FBI to develop and maintain the technical expertise and investigative tools to address the increasing threats of criminal organizations and violent crime.	22	12	$20,574	76
Civil Rights	The request will allow the FBI to address the recent increases in civil rights violations and proactively mitigate them before they occur through increased investigative and tactical support and greater community outreach and engagement.	92	46	$17,786	78

Item Name	Description	Pos.	FTE	Dollars ($000)	Page
Salaries and Expenses Enhancements					
Cybersecurity	The requested funding will not only allow the FBI to increase its cybersecurity posture, but it will also allow the FBI to proactively address cybersecurity vulnerabilities and the growing cyber threats posed by internal and external threats.	9	5	$36,948	82
Data Analytics and Technical Tools	The new funding will support the development of enterprise tools to enhance investigative capabilities throughout the enterprise.	0	0	$16,928	91
UTS	This request is classified.	8	4	$8,092	95
Body Worn Cameras	The requested funding will support the FBI's implementation of a body worn camera program for all FBI Special Agents.	102	51	$27,351	96
21st Century Facilities O&M	The request will support the substantial personnel, structural, and security requirements of the newly constructed buildings at Redstone Arsenal in Huntsville, Alabama.	47	24	$39,420	101
McGirt	The requested resources will allow the FBI to effectively address the increased operational need in the state of Oklahoma following the Supreme Court decision on *McGirt v. Oklahoma*. This ruling significantly expanded federal jurisdiction for crimes committed on tribal lands, and the resources will enhance the FBI's capacity to address the large increase in investigations.	76	38	$22,513	110
Salaries and Expenses Enhancements Total		**789**	401	**$324,556**	

III. Appropriations Language and Analysis of Appropriations Language

For necessary expenses of the Federal Bureau of Investigation for detection, investigation, and prosecution of crimes against the United States, $10,741,678,000, of which not to exceed $216,900,000 shall remain available until expended: Provided, that not to exceed $284,000 shall be available for official reception and representation expenses.

IV. Program Activity Justification

A. Intelligence Decision Unit

Intelligence Decision Unit Total	Direct Pos.	Estimate FTE	Amount ($000s)
2021 Enacted	6,644	6,207	$1,839,900
2022 President's Budget	6,757	6,374	$1,884,475
Adjustments to Base and Technical Adjustments	0	55	$41,857
2023 Current Services	6,757	6,429	$1,926,332
2023 Program Increases	100	50	$44,528
2023 Request	6,857	6,479	$1,970,860
Total Change 2022-2023	**100**	**105**	**$86,385**

Intelligence - Information Technology Breakout (of Decision Unit Total)	Direct Pos.	Estimate FTE	Amount ($000s)
2021 Enacted			$180,996
2022 President's Budget			$165,422
Adjustments to Base and Technical Adjustments			($530)
2023 Current Services			$164,891
2023 Program Increases			$17,953
2023 Request			**$182,844**

1. Program Description

The FBI's IDU is comprised of the entirety of the IB, including the Strategic Intelligence Issues Group (SIIG), DI, OPE, and OPS; the intelligence functions within CTD, CD, CyD, CID, and WMDD; field office intelligence programs, the TSC, infrastructure and technology (e.g., Sensitive Compartmented Information Facilities, or SCIFs, and the Sensitive Compartmented Information Network, or SCINet), and intelligence training. The IDU also includes a portion of CIRG, LD, and IOD based on the work that those divisions complete 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 TD, LD, and SecD; the administrative and information technology divisions; and staff offices) are calculated and scored to this DU.

Intelligence Branch
As the leader of the FBI's intelligence program, IB drives collaboration to achieve the full integration of intelligence and operations throughout the FBI. 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, LE, and private sector communities. The FBI's Intelligence Program Strategy guides IB direction and oversight of all aspects of the FBI's intelligence work.

The SIIG provides FBI leaders with a consolidated, integrated perspective on threats while helping to integrate and balance the FBI's priorities with those of the broader USIC and USG. Led by a Deputy Assistant Director, the SIIG 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 SIIG also houses the Bureau Control Office, which manages the FBI's sensitive compartmented information program.

Directorate of Intelligence
DI is the FBI's dedicated national intelligence workforce, with clear authority and responsibility for all FBI intelligence functions. DI's mission is to provide strategic support, direction, and oversight to the FBI's intelligence program, and its vision is to drive the complete integration of intelligence and operations within the FBI. DI carries out these functions through embedded intelligence elements at HQ and in each FO.

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

The FBI's IA cadre 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 a FO area of responsibility;
- Performing strategic analysis at 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. FBI intelligence products also serve to inform the FBI's partners about ongoing and emerging threats.

Foreign Language Program
The FLP provides quality language solutions, analysis, and cultural expertise to the FBI and its partners. The FBI's success at protecting the U.S. from future terrorist attacks, countering foreign intelligence operations and espionage, and dismantling transnational criminal enterprises is increasingly dependent upon maximizing the use and deployment of its linguist workforce, language tools, and technology. The FBI workforce has qualified capabilities in 142 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

ongoing 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 Analysts and English Monitoring Analysts are 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 Analysts address the highest priority foreign language collection and processing requirements in the FBI's counterterrorism, cyber, counterintelligence, and criminal investigative missions.

National Virtual Translation Center
The NVTC provides timely and accurate translation services to support national intelligence priorities and protect the nation and its interests. NVTC was established under Section 907 of the USA Patriot Act (2001) and designated a USIC service of common concern in 2014. Since its inception, NVTC has complemented USIC elements' foreign language translation capabilities by supporting tasks ranging from high-volume surges to immediate translation requirements in 142 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 the FBI's intelligence workforce is prepared with the necessary specialized skills and expertise is crucial to the FBI's ability to successfully fulfill its mission. The FBI's extensive intelligence training program leverages expertise within the organization and its partners in the intelligence and academic communities and private industry to ensure the best educational opportunities are available to the FBI's workforce. The FBI's training program identifies and coordinates the certification of adjunct faculty, communicates educational and developmental opportunities outside the FBI, and facilitates opportunities for research related to intelligence analysis. Moreover, the FBI uses an integrated approach to training bringing employees together at the beginning of their careers to help them understand the importance and impact of an integrated intelligence and operational methodology – a model that continues across the FBI's intermediate and advanced courses of instruction.

Office of Partner Engagement
OPE implements initiatives and strategies that support engagement, communication, coordination, and cooperation efforts with federal, state, local, tribal, and territorial (SLTT) LE, and intelligence information sharing in an ongoing effort to enhance the FBI's capabilities in the Domestic Information-Sharing Architecture. OPE accomplishes this mission by establishing and maintaining key partner relationships, methods, and practices to enhance engagement, coordination, and information sharing with the IC and SLTT LE. OPE leads the FBI's approach to intelligence supporting the Domestic Information-Sharing Architecture, providing program management for the FBI's engagement with state and local fusion centers, and proactively reviewing and disseminating relevant and appropriate threat information to FBI, federal, and SLTT partners.

Office of Private Sector
The primary mission of OPS is to protect the nation's economy and national security by strengthening the FBI's relationships with the U.S. private sector partners. OPS builds, supports, facilitates, and enhances strategic relationships between the FBI, private industry, and academia. OPS also develops tools to support those relationships, and facilitates information sharing, while maintaining an enterprise focus of the FBI's engagement efforts. OPS enhances understanding of the private sector, to include academia and associations, increasing 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; and assisting companies whose innovative technologies may be targeted. OPS focusses on engaging the private sector on priorities including insider threat, emerging technologies, foreign influence, and lawful access. In addition to its main office at FBI HQ, OPS is represented in each FBI FO by at least one Private Sector Coordinator (PSC) to develop and maintain private sector partnerships in each FO's Area of Responsibility (AOR). OPS also manages two private sector information-sharing programs: The Domestic Security Alliance Council (DSAC) and InfraGard, promoting effective information exchanges through public-private partnerships.

Foreign Terrorist Tracking Task Force
The Foreign Terrorist Tracking Task Force (FTTTF) exploits intelligence intended to prevent travelers and their supporters, who are identified as potential threats, from entering the U.S. FTTTF leverages this information, when appropriate, to facilitate these individuals' location, detention, prosecution, removal, or other appropriate action. FTTTF uses specialized analytical techniques, technologies, and data analysis to enhance terrorist identification, tracking, and risk assessments.

Terrorist Screening Center
TSC consolidates and coordinates the USG's approach to threat screening and facilitates the sharing of information to protect the nation and its foreign partners. This effort provides direct support for the FBI, DOJ, Department of Homeland Security (DHS), Department of State, the ODNI, the IC, and other major federal LE, screening, and regulatory agencies. The TSC accomplishes this mission through a unique, interagency business model that incorporates IT and information sharing, as well as operational and analytical expertise from its interagency specialists.

Infrastructure and Technology
The FBI's information technology infrastructure and technology help 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 part 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.

The unclassified part 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 CJIS' Law Enforcement Enterprise Portal (LEEP) system and its Unclassified Network (UNet), the FBI's unclassified network which includes connection to the public internet.

Secure Work Environment

SWE includes two main components - SCIFs 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 SCI. SCIFs are outfitted with IT, telecommunications, and requisite infrastructure to process unclassified through TS information. SCIFs are equipped with intrusion detection and access control systems to prevent the entry of unauthorized personnel. SCINet is a compartmented network for TS information, which is administered by employing increased security measures, enforcing user accountability, and enhancing information assurance methodology.

2. Performance and Resource Tables

PERFORMANCE AND RESOURCES TABLE										
Decision Unit: Intelligence										
RESOURCES	**Target**		**Actual**		**Target**		**Changes**		**Requested (Total)**	
	FY 2021		**FY 2021**		**FY 2022**		**Current Services Adjustments and FY 2023 Program Change**		**FY 2023 Request**	
Total Costs and FTE (reimbursable FTE are included, but reimbursable costs are bracketed and not included in the total)	**FTE**	**$0**	**FTE**	**$0**	**FTE**	**$0**	**FTE**	**$0**	**FTE**	**$0**
	6,316	$1,817,342	6,316	$1,817,342	6,410	$1,909,652	103	$86,385	6,514	$1,996,037

Strategic Objective	PERFORMANCE MEASURE TABLE										
	Decision Unit: Intelligence										
	Performance Report and Performance Plan Targets	**FY 2020**		**FY 2021**		**FY 2022**	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**
		Target	**Actual**	**Target**	**Actual**	**Target**	**Target**	**Target**	**Target**	**Goal**
Measure (DOJ Objective 2.2)	Percentage of FBI Intelligence Information Reports (IIRs) used in the development of United States Intelligence Community (USIC) Intelligence Products (KPI)	15%	16%	15%	7%	15%	15%	15%	15%	15%

3. Resources and Strategies

Directorate of Intelligence (DI)

a. Performance Plan and Report for Outcomes

The Intelligence Program's Five-Year Strategy aims to create a more secure nation through an integrated, agile, and innovative Intelligence Program that drives the FBI's ability to address current and emerging threats. The FBI's DI will continue to support the complete integration of the Intelligence and Operations through the sharing of intelligence to enable FBI and Intelligence Community partners to identify and mitigate current and emerging threats. Progress towards this goal is reflected by the increased inclusion of FBI-originated reporting in USIC Intelligence Products. Increased inclusion drives the development of high-quality intelligence while mitigating risk.

Performance Measure: Percentage of FBI IIRs used in the development of USIC intelligence products.
FY21 Target: 15%
FY21 Actual: 7%
FY22 Target: 15%
FY23 Target: 15%
FY24 Target: 15%

Discussion
Percentage of FBI Intelligence Information Reports (IIRs) is calculated by measuring the number of FBI IIRs used in the development of USIC intelligence products against the total number of USIC intelligence products.

b. Strategies to Accomplish Outcomes

The FBI Intelligence Program's Five-Year Strategy outlines the direction for moving forward in an ever-changing threat environment. The program's primary mission, as a part of this strategy, is to provide insightful, timely and actionable intelligence in direct support of the FBI's mission to protect the American people and uphold the Constitution. Successful execution of this strategy will result in an integrated, agile and innovative Intelligence Program that will directly bolster the FBI's ability to address current and emerging threats. By prioritizing the incorporation of intelligence in all FBI undertakings and strengthening of partnerships with law enforcement and USIC partners, the Intelligence Program will further enhancement its successful operating posture.

B. Counterterrorism/Counterintelligence Decision Unit

Counterterrorism/Counterintelligence Decision Unit Total	Direct Pos.	Estimate FTE	Amount ($000s)
2021 Enacted	13,713	12,735	$3,957,553
2022 President's Budget	13,912	13,190	$4,124,461
Adjustments to Base and Technical Adjustments	0	91	$85,412
2023 Current Services	13,912	13,281	$4,209,873
2023 Program Increases	275	142	$147,289
2023 Request	14,187	13,423	$4,357,162
Total Change 2022-2023	**275**	**233**	**$232,701**

Counterterrorism/Counterintelligence - Information Technology Breakout (of Decision Unit Total)	Direct Pos.	Estimate FTE	Amount ($000s)
2021 Enacted			$329,790
2022 President's Budget			$248,794
Adjustments to Base and Technical Adjustments			($1,461)
2023 Current Services			$247,334
2023 Program Increases			$54,968
2023 Request			**$302,301**

1. Program Description

The FBI's CT/CI Decision Unit comprises the counterterrorism (CT) program, the WMDD, the counterintelligence (CI) program, a portion of the computer intrusion (cyber) program (CIP), a portion of the CIRG, and the portion of the 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 the Training, Laboratory, and Security Divisions; the administrative and information technology divisions; and staff offices) are calculated and scored to the decision unit.

Counterterrorism Program
The mission of the FBI's CT program is to lead LE and domestic intelligence efforts to:

- Prevent, disrupt, and defeat terrorist operations before they occur,
- Pursue the appropriate sanctions for those who have conducted, aided, and abetted those engaged in terrorist acts, and
- Provide crisis management following acts of terrorism against the U.S. and its interests.

The FBI aims to eliminate the risk of international and domestic terrorism. The FBI accomplishes this by gathering intelligence from all sources and using 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 USIC 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 those who provide financial or other support to terrorist operations. FBI Headquarters maintains oversight of all CT investigations, 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 building a comprehensive intelligence base to exploit these vulnerabilities.

The FBI has a multi-year CT strategic plan with the following areas of focus:

- Rigorous program management to ensure standardization of the FBI's policies and procedures related to countering terrorism.
- Development of technical tools to collect and exploit data, in order to enhance targeting and overcome barriers to intelligence gathering.
- Provision of training opportunities to ensure the workforce can successfully mitigate national security threats in a dynamic operational environment.
- Evaluation of human intelligence (HUMINT) to effect disruptions and help anticipate adversaries' future intentions.
- Development of intelligence products to inform both strategic and tactical operational decisions and ensure the FBI remains agile in its mitigation efforts against threats to the homeland and U.S. interests abroad.

The CT strategy puts the FBI in a position to achieve long-term agility and flexibility to meet the changing needs of the CT mission space and larger FBI priorities.

The FBI has divided CT operations geographically and by threat, with each program focusing on different aspects of terrorism threats. These components are staffed with Special Agents, analysts, and subject matter experts (SME) who work closely with investigators in the field and integrate intelligence across multiple organizations. This integration allows for real-time responses to threat information and quick communication with decision-makers and the field.

The FBI has established strong working relationships with other members of the USIC. Through daily meetings with other USIC executives, the regular exchange of personnel among agencies, joint efforts in specific investigations and in the NCTC, the TSC, other multi-agency entities, and the collocation of personnel at Liberty Crossing, the FBI and its partners in the USIC are integrated at every level of operations.

With terrorists international reach, coordination with foreign partners is crucial. The FBI has increased its overseas presence and now routinely deploys Special Agents 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 WMDD's mission is to lead USG LE and domestic intelligence efforts to prevent and neutralize weapons of mass destruction (WMD) threats against the homeland and support interests abroad. The WMDD unifies LE 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 events and its responses are unique. To accomplish its mission, the WMDD integrates the necessary counterterrorism, intelligence, counterintelligence, and scientific and technological components in direct WMD cases and in support of its partners (CTD, CD, DI, CID, and CyD).

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	The WMDD incorporates the development of comprehensive plans and policies into its preparedness activities. The WMDD implements planning, training, and practice exercises to ensure that the FBI and its USG partners are ready to respond to WMD threats in a highly cohesive and efficient manner.
Countermeasures	The WMDD takes proactive measures to actively and passively prevent, prepare, and mitigate chemical, biological, radiological, nuclear, and explosive WMD-related threats. WMDD works with its partners via outreach activities and establishes tripwires to address "existing" threats and collaboratively develops specialized countermeasures to address "over the horizon" threats. The implementation of each countermeasure reduces the ability of bad actors to obtain, create, and use a WMD.
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. The 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 (C2) support in on-scene situations.
Intelligence	The WMDD proactively leverages timely, relevant, and actionable intelligence to collaborate with key stakeholders – other FBI divisions, and USIC, LE, 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 CD's counterproliferation (CP) programs with the subject matter expertise of the WMDD, and the analytical capabilities of the DI, to create specialized CP units 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 hybrid nature of CP operations incorporates aggressive counterintelligence and criminal investigative techniques, to prevent the acquisition of WMDs and dismantle the

transfer of the most sensitive technologies. The FBI's CP program works closely with the National Counterproliferation Center (NCPC) to manage these high impact investigations and collection platforms, which if not fully mitigated, pose the highest threat to US national security.

Since the transfer of bomb-related matters to the WMDD in FY 2017, WMDD disrupted 30 WMD incidents and made 143 arrests, 84 indictments, 67 convictions, and 57 sentencings, which is on pace with prior-year activity. Despite profound disruptions experienced throughout the country as a result of the COVID-19 pandemic, WMDD has not experienced a decrease in cases within its purview when compared to previous FYs.

Counterintelligence Program
Executive Order (EO) 12333 assigns to the Director of the FBI, under the Attorney General, oversight and supervision responsibility for conducting and coordinating CI activities within the U.S. The FBI's CI mission is to defeat hostile intelligence activities targeting the U.S. The FBI works to identify and understand threats while protecting vital U.S. entities – in particular, state secrets, intellectual property, and democratic values – through a culture of sharing, collaboration, and integration with private, public, and international partners.

The domestic CI environment is more complex than ever, posing a continuous threat to U.S. national security and its economy by targeting strategic technologies, industries, sectors, and critical infrastructures. Historically, asymmetric CI threats involved foreign intelligence service officers seeking USG and USIC information. The FBI has observed foreign adversaries employing a wide range of nontraditional collection techniques, including the use of human collectors not affiliated with intelligence services, foreign investment in critical U.S. sectors, and infiltration of U.S. supply chains. The FBI continues to adjust its CI priorities and posture to address the evolving and multifaceted threat.

Computer Intrusion Program (Cyber)
Malicious cyber activity threatens the US' public health and safety, national security, and economic security. The FBI adopted a new cyber strategy in FY 2020 to change the cost–benefit for criminals and foreign states who attempt to compromise U.S. networks, steal U.S. financial and intellectual property, and hold U.S. critical infrastructure at risk.

The FBI uses its role as the lead federal agency with LE and intelligence responsibilities to pursue its own actions against cyber adversaries, but also to help partners to defend networks, attribute malicious activity, punish bad behavior, and counter adversaries overseas. The FBI operationalizes the team approach through unique hubs where government, industry, and academia can work alongside each other in long-term trusted relationships to combine efforts against cyber threats.

Within the government, that hub is the National Cyber Investigative Joint Task Force (NCIJTF), which the FBI leads with more than 30 co-located USIC and LE agencies. The NCIJTF is organized around new mission centers based on key cyber threat areas and led by senior executives from partner agencies. Through these mission centers, operations and intelligence are integrated to sequence unilateral, joint, and enabled operations for maximum impact against our adversaries.

The FBI also leads the National Defense Cyber Alliance, where experts from the government and cleared defense contractors share threat intelligence in real time, and is co-located with partners in industry, academia, and the financial sector as part of the National Cyber-Forensics and Training Alliance in Pittsburgh and New York City.

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. CIRG personnel are on call around the clock to respond to crisis incidents requiring an immediate LE response and to support FBI planning and coordination of special events. CIRG also furnishes distinctive training to FBI field personnel, as well as state, local, federal, tribal, and international LE partners in support of this mission. This includes Hazardous Device School (HDS) certification and recertification, as well as advanced training to all U.S. public safety bomb technicians and accreditation of all U.S. public safety bomb squads.

CIRG encompasses the Hostage Rescue Team (HRT), a full-time national tactical counterterrorism team, and manages the SWAT program in all FBI field offices. 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 aircraft systems (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. CIRG is responsible for managing the FBI's counter-unmanned aircraft systems (C-UAS) program, performing both detect, track, locate, and identify (DTLI) and mitigation missions. CIRG operates the Strategic Information and Operations Center (SIOC) to maintain 24/7/365 enterprise-wide situational awareness. In addition, CIRG oversees the National Center for the Analysis of Violent Crime (NCAVC) Program and provides behavioral analysis and assessments for complex and time-sensitive investigations across multiple programs.

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 CIRG encompasses all of these elements.

Legal Attaché Program
Legats are the forward element of the FBI's international LE 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 Special Agents 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.

2. Performance and Resource Tables

PERFORMANCE AND RESOURCES TABLE										
Decision Unit: Counterterrorism/Counterintelligence										
RESOURCES	**Target**		**Actual**		**Target**		**Changes**		**Requested (Total)**	
	FY 2021		**FY 2021**		**FY 2022**		**Current Services Adjustments and FY 2023 Program Change**		**FY 2023 Request**	
Total Costs and FTE (reimbursable FTE are included, but reimbursable costs are bracketed and not included in the total)	**FTE**	**$0**	**FTE**	**$0**	**FTE**	**$0**	**FTE**	**$0**	**FTE**	**$0**
	13,060	$3,924,373	13,060	$3,924,373	13,374	$4,104,166	233	$232,703	13,607	$4,336,869

Strategic Objective	**PERFORMANCE MEASURE TABLE**									
	Decision Unit: Counterterrorism/Counterintelligence									
	Performance Report and Performance Plan Targets	**FY 2020**		**FY 2021**		**FY 2022**	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**
		Target	**Actual**	**Target**	**Actual**	**Target**	**Target**	**Target**	**Target**	**Goal**
KPI (DOJ Objective 2.2)	Number of terrorism disruptions effected through investigations.	400	561	450	793	600	600	600	600	600
KPI (DOJ Objective 2.1)	Number of counterintelligence program disruptions or dismantlements.	400	365	400	447	400	400	400	400	400
KPI (DOJ Objective 2.4)	Percent increase in disruptions of malicious cyber actors use of online infrastructure through proactive operations and judicial means.	N/A	N/A	N/A	N/A	5%	10%	15%	20%	25%
KPI/Agency Priority Goal (2.4)	Percent of reported ransomware incidents from which cases are opened, added to existing cases, or resolved within 72 hours.	N/A	N/A	N/A	42.7					65%
KPI (DOJ Objective 2.4)	Percent increase in operations conducted jointly with strategic partners.	N/A	N/A	N/A	N/A	3%	6%	9%	12%	15%
KPI (DOJ Objective 2.4)	Number of threat advisories disseminated to the private sector.	N/A	N/A	N/A	N/A	72	80	88	94	100
Agency Priority Goal (2.4)	Increasing the number of ransomware matters in which seizures or forfeitures are occurring by 10%.	N/A	N/A	N/A	N/A					10%
*N/A is listed above when the measure was not readily tracked by FBI prior to the new DOJ Strategic Plan for FY2022-FY2026.										

3. Resources and Strategies

Counterterrorism Division (CTD)

a. Performance Plan and Report for Outcomes

Disrupting terrorist operations is a core priority of the FBI in preserving national security and protecting the American people. CTD streamlines its efforts to thwart terrorist operations with multiple strategic objectives advanced through various intiatives. In support of DOJ Strategic Objective 2.2 *Counter Foreign and Domestic Terrorism*, CTD focuses on the disruption of financial, weaponry, and material support sources and the prosecution of those who plot or act to threaten our national security. In support of its proactive posture, CTD targets the methods and technologies terrorist networks and organizations rely upon for radicalization and recruitment and uses all available tools to monitor terrorist threats—from developing sources to court-authorized electronic surveillance. CTD iteratively evalautes its ability to meet the threat of terrorism, and will continue to measure progress through the number of terrorism disruptions accomplished.

Performance Measure: Number of terrorism disruptions effected through investigations.
FY21 Target: 450
FY21 Actual: 793
FY22 Target: 600
FY23 Target: 600
FY24 Target: 600

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 threat actors.

b. Strategies to Accomplish Outcomes

CTD will advance its strategic objectives for partnerships and information-sharing as a means to maximize the FBI's impact the terrorism threat. Commitment to strengthening partnerships is not exlusive to national security entities, but also includes private sector organizations to improve the FBI's ability to share and receive information. This objective directly supports DOJ Strategic Objective 2.2 Strategy 2: *Strengthen Federal, Tribal, State, Local, and International Counterrorism Partnerships*. To faciliate increased reporting by the public, which can lead to disruptions of threat actors before they commit violence, the FBI regularly updates its Homegrown Violent Extremist Mobilization Indicator booklet, published jointly with the National Counterterrorism Center (NCTC) and the Department of Homeland Security (DHS). Pursuant to this strategy, CTD will continue to build information sharing capacity with foreign governments to investigate and prosecute, in their own courts, threat actors who threaten U.S. national security. Additionally, CTD will continue to pursue opportunities in data science, analytics, and building capabilities.

CTD will continue to address ongoing risks, including data structure and complexity. As such, CTD will align its strategy with a personnel request for information technology skills required to conduct data science and technical tool development necessary to mitigate terrorism threats. Additionally, another personnel and financial enhancement request will be submitted to address opportunities with large, complex datasets and how they relate to ongoing and potential FBI investigations.

Counterintelligence Division (CD)

a. Performance Plan and Report for Outcomes

The FBI's statutory counterintelligence authorities make it the lead U.S. government (USG) agency to address threats to America's national and economic security. Disruptions and dismantlements are high-value outcome accomplishments: measures of the effectiveness of a wide scope of FBI and USG activities. Even a complex network case, with multiple arrests and asset seizures, would qualify as only a single "dismantle" operational outcome. CD seeks a sustained level of counterintelligence disruption and dismantlement accomplishments over time, continuing to make the U.S. operating environment more difficult for foreign intelligence services and their witting and unwitting collaborators despite their technological and tactical innovations. Accordingly, counterintelligence disruptions and dismantlements demonstrate effective loss prevention and proactive disruption of intelligence threats from hostile actors, theft of U.S. assets, violations of export control laws or sanctions, and related crimes. Disruptions and dismantlements are an indicator of how well the USG (and the FBI) is mitigating the negative risks of new technologies, globalization of threat actors and activities, and the emergence of new security vulnerabilities as an integral part of DOJ's risk mitigation strategy.

The expanded scope of sensitive American assets of interest to strategic competitor states coupled with a continually evolving technological environment opens new security vulnerabilities. As such, continual changes to federal resource allocations must be supported to successfully address constantly evolving threat actors. The amount and type of resources allocated directly to the DOJ and FBI, (leveraged in tandem with a whole-of-government approach to combine USG authorities and resources) has a determinative impact on the ability of the FBI to meet its disruption and dismantlement goals.

Performance Measure: Number of counterintelligence program disruptions or dismantlements.
FY21 Target: 400
FY21 Actual: 447
FY22 Target: 400
FY23 Target: 400
FY24 Target: 400

Discussion
A **disruption** is interrupting or inhibiting a threat actor from engaging in national security related activity. Disruptions are the primary accomplishment that demonstrates how the FBI has stopped or mitigated threat activities against U.S. targets, and disruptions vary in size of impact. The target remains stable so that investigators can focus on impact to the threat actor rather than the total number of disruptions each year.

A **dismantlement** occurs when the targeted organization's leadership, financial base, and supply network has been destroyed, such that the organization or active cell is incapable of operating and/or reconstituting itself. By this definition, dismantlements are relatively rare.

b. Strategies to Accomplish Outcomes

Consistent with its responsibility for all of the strategies under DOJ Objective 2.1: *Protect National Security*, CD operational strategies seek to protect U.S. information, items, and other assets by disrupting hostile foreign actors and dismantling organizations that further the hostile activities. Preventing the loss of assets and proactively disrupting threat actors are essential parts of a counterintelligence strategy; once a hostile foreign nation has acquired U.S. assets, this damage cannot be undone. CD periodically reviews and modernizes operational strategies to understand and counter these evolving threats. In addition, CD has supported an increased whole-of-government coordination through the National Counterintelligence Task Force (NCITF), providing nationwide coordination with federal law enforcement and Intelligence Community partners on the model of successful drug and counterterrorism joint task forces. The NCITF supports counterintelligence task forces in all 56 field offices, allowing the FBI to leverage additional federal, state and local law enforcement personnel to bring additional resources to bear on counterintelligence threats. CD provides expertise to the Committee on Foreign Investment in the United States in support of DOJ Objective 2.1 Strategy 3: *Prevent the Theft of Technology*. These collaborative approaches to identifying and publicizing threat actors stop current threats from further damage to U.S. assets and deter future threats by driving up the cost and risks of these activities.

CD has requested budget enhancements to increase the resources available to tackle emerging and changing counterintelligence threats, such as economic security, threat finance, and the protection of critical infrastructure. These resources will better position CD to identify potential assets targeted by hostile foreign actors or insider threats and disrupt any malign activity against them in accordance to DOJ Objective 2.1 Strategy 4: *Protect sensitive assets*.

<u>Cyber Division (CyD)</u>

a. Performance Plan and Report for Outcomes

CyD's strategy to combat cyber-based threats and attacks focuses on imposing risk and consequences on cyber adversaries through the FBI's unique authorities, world-class capabilities, and enduring partnerships. CyD will bring cyber adversaries to justice by increasing: (1) disruptions of malicious cyber actors' use of online infrastructure through proactive FBI cyber operations to slow, frustrate, and stop cyber adversaries' ability to conduct their operations; and, (2) joint, sequenced operations that rely on cooperation and coordination across many public, private, and international stakeholders in order to aid attribution, defend networks, sanction bad behavior, build coalitions of like-minded countries, and otherwise deter or disrupt cyber adversaries overseas.

CyD seeks to combat significant cybercriminal activity and impose risks by making it more difficult for cyber adversaries to conduct operations against U.S. networks, specifically by increasing: (1) the number of threat advisories disseminated to share vital information that the private sector can use to strengthen their cyber defenses and resilience; and (2) reported

incidents— for both ransomware and overall—from which cases are opened, added to existing cases, or resolved within 72 hours to encourage the private sector and the public to report suspected criminal and other hostile cyber activity.

CyD aims to combat significant cybercriminal activity by increasing prosecutions of ransomware defendants in which seizures or forfeitures are used to reduce cyber actors' ability and willingness to conduct future operations. CyD's strategy focuses on mitigating enterprise risks of technology, the emergence of new security vulnerabilities, fragmentation and globalization of the threat, coordination challenges, and building trust.

Performance Measure: Percent increase in disruptions of malicious cyber actors' use of online infrastructure through proactive operations and judicial means.
FY21 Target: N/A
FY21 Actual: N/A
FY22 Target: 5%
FY23 Target: 10%
FY24 Target: 15%

Performance Measure: Percent of reported incidents from which cases are opened, added to existing cases,or resolved within 72 hours.
FY21 Target: N/A
FY21 Actual: 43%
FY22 Target: 65%
FY23 Target: 65%
FY24 Target: 65%

Performance Measure: Percent increase in operations conducted jointly with strategic partners.
FY21 Target: N/A
FY21 Actual: Not Tracked
FY22 Target: 3%
FY23 Target: 6%
FY24 Target: 9%

Performance Measure: Number of threat advisories disseminated to the private sector.
FY21 Target: N/A
FY21 Actual: Not Tracked
FY22 Target: 72
FY23 Target: 80
FY24 Target: 88

Discussion
Proactive operations are defined as proactive cyber operations and judicial outcomes involving use of seizures, forfeitures, and use of criminal, civil, and administrative authorities designed to disrupt online infrastructure used by malicious cyber actors including outcomes resulting from collaboration with interagency and international partners.

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 impairment of the operational capabilities of threat actors.

Reported incidents are defined as incidents reported to the FBI by the public.

Strategic partners in cyber operations are defined as the FBI working cooperatively with other federal, state, local, or tribal government agencies; non-governmental organizations; or foreign governments.

A **joint operation** is a cooperative effort among the FBI and other federal, state, local, or tribal government agencies; non-governmental organizations; or foreign governments for investigative, intelligence, security, or incident management purposes to achieve a law enforcement, regulatory, or intelligence outcome.

Threat advisories are defined as network defense products such as Private Industry Notices (PINs), FLASH reports, Public Service Announcements, and Joint Cybersecurity Advisories.

Asset seizures are defined as taking possession of property by legal process.

b. Strategies to Accomplish Outcomes

As technology rapidly develops, the cyber threats we face are more diverse, more sophisticated, and more dangerous. Nation state, surrogate, and criminal hackers operate across the globe exploiting technology to obfuscate their activity, the legal limits of law enforcement authority and capabilities, and gaps between inter-government cooperation as they target U.S. victims for financial gain, espionage, or attack. Cyber-based threats come from all corners, ranging from nation states and their surrogates to criminal hackers or terrorist groups, all of whom are constantly adapting their tools and methods to evade detection and attribution.

CyD continues to focus on advancing strategic partnerships and technical innovation to maximize the FBI's impact and ability to dismantle cybercriminal organizations and nation-state actors alike. To achieve greater arrests, indictments, and organizational dismantlement's against our cyber adversaries, the FBI relies on a unique blend of technical equipment and specially trained personnel. As such, CyD submitted a personnel request to support an initiative to cultivate a standardized team of technically trained personnel in each of the 56 field offices. This initiative ensures each field office has the necessary investigative, analytical, technical, and administrative personnel to adequately address the significant cyber threats and enable interagency operations for a whole-of-government approach to combating cyber-based threats, attacks, and terrorist operations.

Disrupting, dismantling, and targeting cybercriminal organizations and nation-state actors requires collaboration across the USIC and private industry, specializing in network defense, intelligence, investigation, and offensive action to combat these threats. CyD is uniquely positioned at the center of these efforts as a component of the lead domestic law enforcement and intelligence agency. As such, CyD has requested funding to support the development and maintenance of a universal environment to integrate cyber threat intelligence and operational information, while providing access to relevant intelligence and analytical tools. This approach

streamlines the way in which CyD conducts and will conduct future cyber investigations, increasing efficiency and collaboration across not only the FBI but also the USIC.

c. Strategies to Accomplish Agency Priority Goals

The FBI's focus is on imposing risk and consequences on cyber adversaries to stay ahead of the threat; however, it must effectively respond to ransomware events at an increased pace that mitigates impacts to victims and effects positive outcomes. FBI's strategy to increase the percentage of reported ransomware incidents from which cases are opened, added to existing cases, or resolved within 72 hours, and subsequently increase the percentage of seizures and forfeitures in these matters is two-fold. First, FBI Cyber Division will prioritize response time to reported incidents through its network of cyber-trained special agents across 56 field offices and accompanying resident agencies. This will continue to be supported through training resources and learning opportunities that equip cyber workforce to respond to all significant cyber incidents, whenever and wherever they happen. Second, in conjunction with the Bureau at large, FBI Cyber Division will directly support proactive liaison activities across the country with private sector, academia, and other potential target institutions. True for all threats the American people face, partnerships are critical to both maintaining a posture ahead of the threat and establishing a robust response to mitigate damage and hold malicious actors responsible – these principles were never more relevant to Cyber Division than today. As a guiding principle for the FBI's enterprise strategy, partnerships provide an FBI face to external partners to which victims should feel empowered to report incidents as soon as detected. In tandem, internal prioritization and external relationship-building will result in a greater share of reported ransomware incidents actioned within 72 hours, directly supporting the FBI's ability to identify malicious actors and seize stolen or forfeited property.

C. Criminal Enterprises/Federal Crimes Decision Unit

Criminal Enterprises/Federal Crimes Decision Unit Total	Direct Pos.	Estimate FTE	Amount ($000s)
2021 Enacted	12,924	12,648	$3,381,449
2022 President's Budget	12,993	12,653	$3,589,759
Adjustments to Base and Technical Adjustments	7	38	$55,209
2023 Current Services	13,000	12,691	$3,644,968
2023 Program Increases	340	172	$117,257
2023 Request	13,340	12,863	$3,762,225
Total Change 2022-2023	**347**	**210**	**$172,466**

Criminal Enterprises/Federal Crimes Decision Unit - Information Technology Breakout (of Decision Unit Total)	Direct Pos.	Estimate FTE	Amount ($000s)
2021 Enacted			$233,462
2022 President's Budget			$198,786
Adjustments to Base and Technical Adjustments			($1,623)
2023 Current Services			$197,163
2023 Program Increases			$42,495
2023 Request			**$239,659**

1. Program Description

The CEFC Decision Unit comprises all headquarters and field programs that support the FBI's criminal investigative missions, which are managed by CID. The DU includes:

- The FBI's organized crime, gang/criminal enterprise, 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 crimes program, which investigate state, local, and federal government acts of impropriety, including federal and state legislative corruption;
- The criminal investigative components of the CyD's programs, including criminal computer intrusions, the IC3, and a share of the FBI's legat program.

Additionally, to capture all resources that support these programs, a prorated share of resources from the FBI's operational support divisions (including the Training, Laboratory, and Security Divisions; the administrative and information technology divisions; and staff offices) are calculated and scored to the decision unit.

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 Crimes
The WCC program addresses threats including public corruption (e.g., government fraud and border corruption), corporate fraud, securities and commodities fraud, mortgage fraud, financial institution fraud, health care fraud, money laundering, and other complex financial crimes.

Violent Crime and Gang Threats
The FBI's violent crime and gang program aims 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 violent crime 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 LE 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 CyD and IC3.

Legal Attaché Program
Crime-fighting in an era of increasing globalization and interconnectivity is a truly international effort, and the people who make up the 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 LE personnel throughout the world. Special Agents working in the 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 LE, 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 international LE academies and teaching LE partners about proper investigation techniques at crime scenes or crisis management.

2. Performance and Resource Tables

PERFORMANCE AND RESOURCES TABLE										
Decision Unit: Criminal Enterprises/Federal Crimes										
RESOURCES	**Target**		**Actual**		**Target**		**Changes**		**Requested (Total)**	
	FY 2021		**FY 2021**		**FY 2022**		**Current Services Adjustments and FY 2023 Program Change**		**FY 2023 Request**	
Total Costs and FTE (reimbursable FTE are included, but reimbursable costs are bracketed and not included in the total)	**FTE**	**$0**	**FTE**	**$0**	**FTE**	**$0**	**FTE**	**$0**	**FTE**	**$0**
	12,608	$3,416,096	12,608	$3,416,096	13,226	$3,578,907	187	$172,466	13,413	$3,751,372

Strategic Objective	PERFORMANCE MEASURE TABLE									
	Decision Unit: Criminal Enterprises/Federal Crimes									
	Performance Report and Performance Plan Targets	**FY 2020**		**FY 2021**		**FY 2022**	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**
		Target	**Actual**	**Target**	**Actual**	**Target**	**Target**	**Target**	**Target**	**Goal**
Measure (DOJ Objective 2.6)	Number of gender-based violence outreach efforts and engagement with state and local governments, federal government partners and other stakeholders, covering protections against gender-based hate crimes.	N/A	N/A	N/A	140	140	140	140	140	140
KPI (DOJ Objective 2.6)	Percent of crimes-against-children FBI cases which address abductions, hands-on offenders, sextortion, or enticement.	N/A	N/A	N/A	42%	44%	46%	48%	50%	52%
KPI (DOJ Objective 4.2)	Percent of new contacts by the FBI with foreign anti-corruption agencies that progress to mutual sharing of information or assistance or result in a new international corruption case.	N/A	N/A	N/A	70%	60%	60%	60%	60%	60%
KPI (DOJ Objective 4.2)	Number of criminal disruptions or dismantlements in public corruption and fraud against the government	N/A	N/A	N/A	N/A	468	487			545

3. Resources and Strategies

Criminal Investigative Division (CID)

The FBI's CID addresses numerous criminal threats, to include violent crimes, violent gangs, transnational organized crime, violent crimes against children, Indian Country crimes, human trafficking, complex financial crimes, fraud, money laundering, public corruption, and civil rights.

CID's measures, as identified by DOJ and FBI strategic priorities, provide a snapshot of the FBI's work within the Criminal Program. As such, the measures cannot adequately demonstrate all the work performed within CID's budget or resources, which is allocated across all criminal threats. Gangs, criminal enterprises, criminal organizations engaging in white-collar crime and money laundering, and drug-trafficking organizations remain some of the highest priority threats, as identified by DOJ and FBI. Performance will continue to be measured by the magnitude of the disruptions and dismantlements of these criminal groups, as such actions effecitvely hinder or eliminate their ability to commit crimes.

Violent Crime Section

a. Performance Plan and Report for Outcomes

CID addresses numerous criminal threats, to include violent crimes, violent gangs, transnational organized crime, violent crimes against children, Indian Country crimes, human trafficking, complex financial crimes, fraud, money laundering, public corruption, and civil rights.

Pursuant to DOJ Strategic Objective 2.6: *Protect Vulnerable Populations* CID will measure investigations involving abductions, hands-on offenders, sextortion, and enticement as a part of DOJ's effort to strengthen programs which decrease victimization. Prioritizing this subset of Crimes Against Children (CAC) cases will ensure the FBI is leveraging its resources against the most egregious child sexual exploitation groups and offenders. This directly supports DOJ Strategic Objective 2.6 Strategy 3: *Protect Children from Crime and Exploitation*.

CID anticipates field offices will continue to open a variety of CAC cases in FY 2023 in order to achieve judicial and preventative outcomes. Leveraging future resources and focusing investigators' efforts will increase the number of cases targeting abductions, hands-on offenders, sextortion, and enticement creating a direct impact on the CAC threat, as well as inform national understanding of the threat. Those cases' percentage of overall casework measures progress.

Performance Measure: Percent of crimes-against-children FBI cases which address abductions, hands-on offenders, sextortion, or enticement.
FY21 Target: N/A
FY21 Actual: N/A
FY22 Target: 42%
FY23 Target: 44%
FY24 Target: 46%

Discussion
Abduction involves the mysterious disappearance of a minor, especially a "child of tender years" (12 years of age or younger), under circumstances that suggest involuntariness.

A **hands-on offender** is an individual who has engaged in or plans to engage in sexual acts or sexual contact with a child, often in order to produce child sexual abuse material (CSAM).

Sextortion is a form of online exploitation directed towards children in which non-physical forms of coercion are used, such as blackmail, to acquire sexual content from a child, engage in sex with a child, or obtain money from a child.

Enticement involves an individual communicating with someone believed to be a child via the internet with the intent to commit a sexual offense or abduction.

For Violent Criminal Threat matters, an **organization** is a group of three or more individuals knowingly involved in a criminal activity.

b. Strategies to Accomplish Outcomes

The FBI takes a targeted, intelligence-driven investigative approach to the Crimes Against Children (CAC) threats, leading to broadly scoped, multi-jurisdictional cases targeting the most egregious offenders. The FBI uses sophisticated and proactive investigative techniques, to include undercover operations, to prioritize investigations targeting hands-on offenders and to disrupt and dismantle identified CAC networks. The FBI also maintains extensive partnerships with other law enforcement agencies, NGOs, and private industry to identify and address all aspects of the CAC threat, including through its 85 Child Exploitation and Human Trafficking Task Forces across the nation.

Technological developments and encrypted communications have made the investigation of CAC more difficult and complex, as child sex offenders are more likely to employ sophisticated encryption methods, exploit covert communication techniques, and operate on illicit Dark Web networks. As investigations reveal techniques and technologies used by CAC/HT offenders to operate anonymously, the FBI develops technical tools to identify and locate them. For example, the FBI submitted a budget enhancement request for FY 2023 to further develop a suite of investigative tools designed to help investigators identify and locate the most technically proficient offenders and generate additional targeting capabilities against the data currently in FBI holdings.

Financial Crimes Section

a. Performance Plan and Report for Outcomes

The prioritization of CID's strategy into elder financial investigations, outreach, training events, awareness briefings, and using Internet Crime Complaint Center (IC3) data to disseminate investigative referrals directly supports the DOJ Elder Justice Initiative (EJI) and Elder Fraud Strike Force Initiative. These strategies help the FBI achieve its mission priority of combatting transnational/national criminal organizations and enterprises and significant white-collar crime while supporting federal, state, local and international partners. CID will continue to allocate

resources towards EJI investigations and expanding awareness of the threat streams to citizens, the private and public sectors, and law enforcement partners in effort to detect, deter, disrupt and dismantle transnational and national threat actors.

b. Strategies to Accomplish Outcomes

CID has allocated specific personnel to undertake the following actions: collaborate with DOJ Consumer Protection Branch, support the EJI investigative interests on an international and national level, collaborate and coordinate with FBI Victim Services Division (VSD), FBI Office of Public Affairs (OPA), and FBI operational sections, conduct outreach on a national level, issue Public Service Announcements, and provide training, guidance, and coordination to field offices in furtherance of the EJI on a state and local level.

In FY 2022, the FBI launched a joint venture between CID and CyD to provide investigative and analytical expertise on virtual asset exploitation to the FBI, intelligence, and law enforcement communities through enterprise collaboration, and relationships with the public and private sectors. FBI CID anticipates this collaboration will further EJI investigations connected to virtual assets.

The FBI is a leader in investigations of fraud against the elderly and all field offices are strongly encouraged to place an increased emphasis on elder fraud prosecutions, training, and outreach. Specific field office personnel are assigned to all offices and focus FBI efforts to efficiently reach target audiences (victims, potential victims, caretakers, financial institutions and financial advisors). The FBI also places specific personnel abroad to further international investigations where applicable.

Additionally, CID places a focus on disseminating joint intelligence products to address fraud schemes involving the elderly to highlight the national scope and impact on the elderly population.

Public Corruption and Civil Rights Section

Performance Measure: Percent of new contacts by the FBI with foreign anti-corruption agencies that progress to mutual sharing of information or assistance or result in a new international corruption case.
FY21 Target: N/A
FY21 Actual: 70%
FY22 Target: 60%
FY23 Target: 60%
FY24 Target: 60%

Performance Measure: Number of criminal disruptions or dismantlements in public corruption and fraud against the government.
FY21 Target: N/A
FY21 Actual: N/A
FY22 Target: 468
FY23 Target: 487
FY24 Target: N/A

Performance Measure: Number of gender-based violence outreach efforts and engagement with state and local governments, federal government partners and other stakeholders, covering protections against gender-based hate crimes.
FY21 Target: *N/A*
FY21 Actual: *140*
FY22 Target: *140*
FY23 Target: *140*
FY24 Target: *140*

Performance Measure: Number of gender-based violence outreach efforts and engagement with other partners conducted, relevant to Female Genital Mutilation (FGM).
FY21 Target: N/A
FY21 Actual: 21
FY22 Target: 25
FY23 Target: 25
FY24 Target: 25

Transnational Organized Crime (TOC) Global Section

a. 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 known as the Consolidated Priority Organization Target (CPOT) list.[1] CID is committed to vigorous enforcement efforts against these violent transnational criminal organizations and gangs, and uses all available tools, to include developing relationships with foreign law enforcement partners and targeting the most egregious criminal acts, to disrupt and dismantle criminal organizations. CID is also committed to combatting the threat drug related crimes pose to the U.S. which result in addiction and overdose deaths.

The FBI focuses heavily on maintaining and enhancing relationships with federal, foreign, state and local, partners; developing advanced analytical capabilities to identify criminal activity; thereby targeting the most egregious criminal actors to disrupt and dismantle transnational criminal organizations.

CID anticipates the number of disruptions, dismantlements, and case initiations will continually be claimed in FY 2023 because of the continued emphasis to achieve judicial and preventative outcomes. These quantitative outcomes will largely reflect the work performed and progress toward meeting and exceeding the relevant performance measure targets or goals. By leveraging all available resources and focusing our efforts the FBI strives to ensure increased public safety.

Performance Measure: Number of CPOT-linked Drug Trafficking Organizations (DTOs) disrupted or dismantled.

[1] This list reflects the most significant international narcotic manufacturers, poly-drug traffickers, suppliers, transporters, and money laundering organizations.

FY21 Target: 90
FY21 Actual: 57
FY22 Target: 90
FY23 Target: 90
FY24 Target: 90

Discussion
A **dismantlement** occurs when the targeted organization's[2] leadership, financial base and supply network has been destroyed, such that the organization is incapable of operating and/or reconstituting itself. By definition, an organization can only be dismantled once. However, in the case of large organizations, a number of individual identifiable cells or subgroups may be present. Each of these cells or subgroups maintains and provides a distinct function supporting the entire organization. The point in which a dismantlement will be claimed is only at the time of the conviction of the last subject in the organization and/or the conviction of the primary target of the organization/identifiable cell or subgroups.

A **disruption** is 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. A disruption should be claimed in conjunction with an affirmative law enforcement action (e.g. Arrest, Indictment, Conviction, Seizures) and/or regulatory action that impedes the normal and effective operation of the targeted criminal enterprise as indicated by changes in the organizational leadership or methods of operation (e.g., including but not limited to financing, trafficking patterns, communications, or drug production). An affirmative law enforcement action resulting in multiple arrests, seizures, indictments, or convictions of an organization's members should be reported as one disruption of that organization.

b. Strategies to Accomplish Outcomes

The FBI has developed, implemented, and prioritized strategies in support of DOJ's Strategic Objective 2.5: *Combat Drug Trafficking and Prevent Overdose Deaths*, specifically for Strategy 1: *Disrupt and Dismantle Drug Trafficking Organizations*. The FBI uses the Enterprise Theory of Investigation, which focuses on disrupting and dismantling the entire criminal organization through intelligence-based targeting and execution of coordinated investigations against the high value subjects.

CID has developed a strategy to investigate and prosecute illegal drug traffickers and distributors, reduce drug related crime and violence, aid other law enforcement agencies, and strengthen international cooperation. The strategy focuses FBI's counter-drug resources on identified CPOT organizations with the most adverse impact on U.S. national interests. CID prioritizes efforts to combat the nationwide opioid epidemic, including addressing traditional

[2] For Violent Criminal Threat matters, an organization is a group of three or more individuals knowingly involved in a criminal activity.

criminal enterprises and dark web vendors importing, distributing, and selling fentanyl and illegal opioids, as well as sources of illegitimate prescription opioids.

CID continues to increase its global footprint to mitigate the myriad activities encompassing the transnational organized crime threat that impacts the U.S. Successful FBI investigations rely heavily on an overseas presence and coordination with host countries and vetted teams. CID will request personnel and financial enhancements necessary to strategically combat TOC actors and their activity, aid in detection of emerging unconventional trafficking technologies, and provide financial analysis and data exploitation to aid in targeting subjects for investigation. Additionally, CID strives to improve capabilities to combat the threat of emerging technologies as well as the evolving opioid threat emanating from both domestic and international TOC actors. Financial and personnel enhancements will assist the FBI in staying ahead of technological advancements exploited by illicit actors. Resources will focus on increased strategic tool development, broadened coordination and training of additional federal, state, local and tribal agencies.

D. Criminal Justice Services Decision Unit

Criminal Justice Services Decision Unit Total	Direct Pos.	Estimate FTE	Amount ($000s)
2021 Enacted	2,461	2,262	$748,784
2022 President's Budget	2,487	2,402	$615,163
Adjustments to Base and Technical Adjustments	0	60	$20,787
2023 Current Services	2,487	2,462	$635,950
2023 Program Increases	75	37	$15,481
2023 Request	2,561	2,499	$651,431
Total Change 2022-2023	**74**	**97**	**$36,268**

Criminal Justice Services -Information Technology Breakout (of Decision Unit Total)	Direct Pos.	Estimate FTE	Amount ($000s)
2021 Enacted			$125,375
2022 President's Budget			$127,716
Adjustments to Base and Technical Adjustments			($173)
2023 Current Services			$127,544
2023 Program Increases			$6,170
2023 Request			**$133,714**

1. Program Description

The CJS Decision Unit comprises the following:

- All programs of the CJIS Division
- The portion of the LD that provides criminal justice information and forensic services (U) to the FBI's state and local LE partners, as well as the state and local training programs of TD
- International training program of IOD
- A prorated share of resources from the FBI's operational support divisions (including TD, LD, SecD, the administrative and IT divisions, and other)

Criminal Justice Information Services Division

The mission of CJIS is to equip LE, national security, and IC partners with the criminal justice information needed to protect the U.S. while preserving civil liberties. CJIS 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 identity history information.

The NGI services connectivity for 106,981 federal, state, local, and tribal LE customers. These customers have existing statutory authorization to conduct background checks using the NGI system; however only about one third, 38,108, of those regularly do so.

The NGI also improved major features such as system flexibility, storage capacity, accuracy, and timeliness of responses, as well as the interoperability with the biometric matching systems of DHS and the DOD.

The NGI system's operating efficiency is an assessment of the overall availability, accuracy, and its robustness. The NGI's operating efficiency has increased along with its overall biometric capacity.

Availability – The NGI system continues to operate at a high-performance level and exceeds all availability and accuracy performance goals. The NGI had a 100 percent availability rate in two of the 10 months through July of FY 2020, while the remaining eight months averaged a 99.72 percent availability rate. The overall system availability for the first 10 months of FY 2020 was 99.77 percent. This is a 0.13 percent decrease from FY 2019.

Accuracy – The NGI system is still very similar to when it was deployed. From a tenprint perspective, the NGI system algorithm, when combined with human examiners, continues to satisfy the 99.999 percent accuracy rate. The latent match system continues to exceed the required 85 percent accuracy rate requirement, and facial recognition searches continue to meet the 85 percent accuracy rate requirement. A new facial recognition algorithm is in the final stages of acceptance, which is expected to increase accuracy to 99.1 percent.

The following is a snapshot of the contents of the NGI:

Tenprint Fingerprint - The NGI system contains over 198 million unique fingerprint identity records, and fingerprint responses continue to exceed customer expectations. During an average day in FY 2020, Ten Print Rap Sheet (TPRS) submissions are processed within six seconds. CAR submissions are processed within six minutes, and civil submissions are processed within 18 minutes.

The total number of fingerprint submissions processed by the NGI system were 76,769,505 in FY 2017, 70,074,260 in FY 2018, 69,232,790in FY 2019, and 45,734,030 for all of FY 2020. The reduction in volume seen during FY 2018 and FY 2019 is the result of several factors including, but not limited to, the adaption of the "best seven of 10 fingerprint solutions" to allow the sytem to raise the image quality score by removing up to three of the lowest quality fingerprints. This was implemented during FY 2017 to reduce rejects and retain more fingerprint submissions. Since CJIS is rejecting less back to customers, a subsequent secondary submission is not needed. Additionally, the addition of Rap Back Services (RBS) and legislative changes have reduced the number of subsequent checks. The drastic reduction in volume experienced between FY 2019 and the first 11 months of FY 2020 was the direct result of the COVID-19 global pandemic.

Latent Fingerprint - In May 2013, the FBI enhanced legacy latent investigative services within the Integrated Automated Fingerprint Identification System (IAFIS) and deployed new investigative tools within the NGI system to provide LE and national security partners with the ability to search latent prints obtained from crime scene evidence against a national repository of retained criminal and civil biometric identities, as well as unidentified latent prints to produce new leads within criminal, terrorism, and cold case/unknown deceased investigations.

The NGI system also expanded cascade or reverse search services to include newly submitted criminal, select civil, and other investigative biometric events to produce new investigative leads after initial search and retention of latent prints within the Unsolved Latent File (ULF). The ULF contains latent finger and palm prints from criminal and terrorist subjects that have searched against the legacy IAFIS and/or the NGI system but remain unidentified. As of July 31, 2020, the ULF consisted of 945,031 unidentified latent prints contributed by local, state, federal, and international LE agencies, as well as LD and members of the USIC from evidence within both criminal and terrorism investigations.

National Palm Print System (NPPS) and Interstate Photo System (IPS) - In FY 2013, NGI added the NPPS, containing over 20 million biometric images, and the 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 a method to search over 43 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.

RBS - In September 2014, the NGI RBS were deployed with the implementation of the "Increment 4" enhancement. There are two domains within the NGI RBS: NCJ and CJ.

The NGI NCJ RBS is designed to assist local, state, and federal agencies in the continuous vetting of individuals in positions of trust. Once the initial fingerprint is retained in the NGI system and a Rap Back subscription is set on the NGI Identity, any activity on the identity history for that individual subscribed will immediately be released to the subscriber. This service alleviates the re-fingerprinting of an individual for the same position over a period of time.

The NGI CJ RBS is designed to provide immediate notifications to LE 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, the State of Texas, and the Transportation Security Administration (TSA). Utah has enrolled 337,720 active Rap Back subscriptions, and Texas has enrolled 2,249,873 Rap Back subscriptions, to include teachers, nurses, and EMS workers. The TSA has enrolled 625,195 Rap Back subscriptions from numerous airports and airlines throughout the U.S.

IRIS Services - The NGI system was designed to allow the addition of future biometric modalities. A pilot has been completed, and a nationwide iris identification system will be operational in the future.

Interstate Identification Index (III or "Triple I") – The III is an integral part of the NGI system and coordinates the exchange of Criminal History Record Information (CHRI). The III can be accessed after positive identification has been made via fingerprint identification or by name-based direct queries of the index. The name based (QH) query will determine whether the III contains a record matching the descriptive information provided. A positive result will return a unique identifying number referred to as a Universal Control Number (UCN). A Quoted UCN or

State Identification Number (SID) (QR) query can be made with a UCN or a SID to request the CHRI of a specific individual.

The following is a snapshot of the activity related to the III for FY 2020:

Name Based Queries (QH) – 275,101,769
Quoted UCN or SID Queries - (QR) – 46,132,649
Total number of incoming III transactions –321,234,418

Electronic Departmental Order (eDO) – The NGI eDO system is utilized by private citizens to 1) request a DO (copy of their identity history summary, or proof that one does not exist), 2) challenge the information on their identity history summary, 3) request the reason for their firearm-related denial, and 4) challenge/appeal the reason for their firearm-related denial. The eDO system allows for less than a 24-hour response time.

National Crime Information Center (NCIC): The NCIC is a computerized database of documented criminal justice information available to LE agencies nationwide, 24 hours a day, 365 days a year, with an average up-time of 99.67 percent in the last 12 months. Providing essential information to LE officers, investigators, judges, prosecutors, correction officers, court administrators, and other LE and criminal justice agency officials in the execution of their day-to-day operations, the NCIC contains over 16.6 million active records and processes an average of 8.8 million transactions a day.

The NCIC became operational on January 27, 1967, with the goal of assisting LE in apprehending fugitives and locating stolen property. With data organized into 21 files (14 person files and seven property files), the NCIC system contains information on wanted persons, missing persons and sex offenders.

NCIC is a valuable tool that aids LE officers, investigators, judges, prosecutors, correction officers, court administrators, and other LE and criminal justice agency officials in the execution of their day-to-day operations. The NCIC contains over 15.4 million active records and processes an average of 10.6 million transactions a day.

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

The goal of N3G is to improve, modernize, and expand the existing NCIC system so it will continue to provide real-time, accurate, and complete criminal justice information to support the LE and criminal justice communities.

National Instant Criminal Background Check System: The NICS is a national system established to enforce the provisions of the Brady Handgun Violence Prevention Act of 1993. Federal Firearms Licensees (FFL) utilize the NICS to determine whether receipt of a firearm by a prospective purchaser would violate state or federal law. The system ensures the timely transfer

of firearms to individuals who are not specifically prohibited and denies transfer to prohibited persons.

The Brady Handgun Violence Prevention Act of 1993 created a very time-sensitive component to the NICS. It gives the FBI three business days to make a determination on a person's eligibility to purchase a firearm. After the close of the third business day, the FFL may legally transfer the firearm at their discretion without a response from the NICS. The NICS Section's mission is to complete as many checks as possible prior to the third business day.

Firearm background checks may be conducted by either the CJIS NICS Section or a state or local LE agency serving as an intermediary between an FFL and the NICS Section. These intermediaries are referred to as POCs. The NICS Section provides full service to the FFLs in 30 states, five U.S. territories, and the District of Columbia. The NICS provides partial service to seven states. The remaining 13 states perform their own checks through the NICS.

NICS checks can be initiated in two ways: 1) via the NICS contracted call center, or 2) via the NICS E-Check, which is a web-based automated option. When an FFL initiates a NICS background check through the FBI or designated agency in a POC state, a prospective firearm transferee's name and descriptive information (as provided on ATF (Bureau of Alcohol, Tobacco, Firearms and Explosives) Form 4473) is searched against the records maintained in three national databases, which may reveal state and federal records prohibiting receipt or possession of firearms. The ATF Form 4473, or Firearm Transaction Record, is a form that FFLs must utilize and maintain as documentation of the firearm transfer from their inventory.

The NICS is customarily available by phone 17 hours a day, seven days a week, including holidays (except Christmas). Calls may be monitored and recorded for any authorized purpose. The NICS E-Check is available 24/7.

During FY 2020, the NICS experienced its highest transaction volume to date. In FY 2020, the NICS processed over 34,000,000 total transactions compared to 27,487,818 in FY 2019, a 24 percent increase.

Uniform Crime Reporting: The FBI's UCR program has served as the national clearinghouse for the collection of data regarding crimes reported to LE since 1930. The FBI collects, analyzes, reviews, and publishes the data collected from participating federal SLTT. The UCR program has two types of collections —SRS and the NIBRS. The transition to a NIBRS-only collection began on January 1, 2021. Information derived from the data collected within the UCR Program is the basis for the annual publications: *Crime in the United States, Law Enforcement Officers Killed and Assaulted*, *Hate Crime Statistics, National Incident-Based Reporting System,* and the *National Use-of-Force Data Collection* publication. 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; hate crime statistics; and use-of-force incidents. These publications also fulfill the FBI's obligations under Title 28, U.S. Code, Section 534.

The FBI Crime Data Explorer serves as the digital front door for the UCR data. This interactive online tool enables LE and the general public to easily access, use, and understand the massive

amounts of UCR data currently collected. With it, users can view charts and agency-level data without having to mine through data tables.

The UCR program initiated the Beyond 2021 project, which will engage the broader stakeholder community (LE, general public, media, research, intelligence, and policy) through a targeted UCR Subcommittee Task Force to include SME groups to ensure value is realized by all consumers of UCR data. This task force and these SME groups will develop recommendations for data publication and the application of imputed and estimated data, changes for the data collected, data utilization use cases, and alignment of data definitions throughout all UCR collections.

Law Enforcement Enterprise Portal: 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 the 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 the 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.

National Data Exchange: 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 release 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 538 million searchable records from over 7,500 criminal justice agencies and provides access to an additional 336 million records from DHS, the Interstate Identification Index, NCIC, and INTERPOL.

National Threat Operations Center: NTOC serves as the FBI's central intake point for the general public and other government agencies to provide information about potential or ongoing crimes, threats-to-life (TTL), and national security threats. NTOC centralizes the flow of information from the public to the FBI by handling calls from all FBI field offices, the Major Case Contact Center, the IC3, the WMD tip line, and all FBI electronic information submissions (E-Tips). The NTOC's threat intake examiners (TIEs) receive threat information from individuals around the

globe, completing preliminary research and analysis on the information received and documenting all relevant information in the Threat Intake Processing Systems (TIPS) database. The TIEs make a determination on the threat level associated with the information provided, determine if the information needs immediate action (such as TTLs), and refer the information to the appropriate FBI entity or other appropriate LE agency for action. NTOC works 24/7/365 to provide reliable, actionable, and high-value information to the field and other partner agencies.

Additionally, NTOC is a key component in the FBI's initiative to provide timely and direct notification of every TTL complaint received by NTOC to the appropriate field office operations center. NTOC also provides direct communication to state, local, and tribal partners on emergent TTL matters to ensure a timely response. The TIEs receive, analyze, and disseminate information pertaining to potential and actual emergencies and national security situations using probing questions to determine the existence of a threat or crime. The TIEs are supervised by Supervisory Special Agents (SSAs), who are trained to handle the triage of national security and emergency situations such as cyber threats, bomb threats, active shooter incidents, and hostage situations; take appropriate actions; and carry out established procedures to ensure timely responses.

From October 1, 2019, through August 31, 2020, NTOC processed 944,722 tips, resulting in 37,313 Guardian entries (referrals to a field office for further action). Of these tips, 89 percent were criminal, five percent were counterterrorism, and approximately six percent were counterintelligence, weapons of mass destruction, or cyber referrals. Of the 37,313 Guardians generated, 77 percent were referred to other LE agencies, 12 percent were used to open new FBI cases, and 11 percent added information to existing FBI cases.

In addition, NTOC holdings are made available to all FBI FOs via "read-only" access through the LEEP. This unprecedented access allows field office more opportunities to enhance ongoing investigations/assessments and provide better situational awareness in individual field office area of responsibility. NTOC also provides a routine weekly report via email regarding Domain Awareness information submissions in each area of responsibility.

Laboratory Division

The FBI Laboratory is a full-service civilian federal forensic laboratory that applies scientific capabilities and technical services to the collection, processing, and exploitation of evidence to support the FBI, other duly constituted LE and intelligence agencies, and some foreign LE agencies unable to perform the examinations on their own in support of investigative and intelligence priorities.

Training Division

In addition to training FBI Special Agents, the FBI provides instruction for state and local LE 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 LE officers is the 10-week multi-disciplinary course at the FBI National Academy. These training sessions cover the full range of LE training topics, such as hostage negotiation, computer-related crimes, and arson.

Due to the ongoing pandemic, Training Division has not held a National Academy session in FY21. The next session of NA is currently scheduled to begin in September of 2021, comprised

of 100 students (no foreign nationals due to travel restrictions). TD is watching closely and will revise the start date if necessary, to accommodate ongoing pandemic concerns.

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 LE partners through the international training and assistance program.

2. Performance and Resource Tables

PERFORMANCE AND RESOURCES TABLE										
Decision Unit: Criminal Justice Services										
RESOURCES	**Target**		**Actual**		**Target**		**Changes**		**Requested (Total)**	
	FY 2021		**FY 2021**		**FY 2022**		**Current Services Adjustments and FY 2023 Program Change**		**FY 2023 Request**	
Total Costs and FTE (reimbursable FTE are included, but reimbursable costs are bracketed and not included in the total)	**FTE**	**$0**	**FTE**	**$0**	**FTE**	**$0**	**FTE**	**$0**	**FTE**	**$0**
	2,363	$590,876	2,363	$590,876	3,172	$621,133	97	$36,268	3,269	$657,401

E. All Decision Units

1. Performance Table

Strategic Objective	PERFORMANCE MEASURE TABLE									
	Decision Unit: All Decision Units									
	Performance Report and Performance Plan Targets	FY 2020		FY 2021		FY 2022	FY 2023	FY 2024	FY 2025	FY 2026
		Target	Actual	Target	Actual	Target	Target	Target	Target	Goal
KPI/Agency Priority Goal (3.3)	Percent of federal law enforcement officers equipped with Body Worn Cameras (BWCs) and associated training.	N/A	0%	N/A	1%	5%	50%	75%	100%	100%
KPI/Agency Priority Goal (3.3)	Percent of Special Agents who receive Use of Force Sustained Training within a 3-year period.	100%	N/A	100%	N/A	100%	100%	100%	100%	100%

2. Resources and Strategies

Director's Office

a. Performance Plan and Report for Outcomes

In response to the June 6, 2021 mandate from the Deputy Attorney General to devise, construct and implement a Body Worn Camera (BWC) capability within the FBI, the BWC Program was initiated to develop and spearhead a multi-phase roll-out strategy designed to deliver a fully operational, enterprise-wide BWC capability in FY 2023. This aligns with the FBI enterprise objective to *Strengthen Confidence and Trust* by allowing for more transparency in interactions with the public.

Rather than accept the risks and limitations inherent in a non-proprietary, off-the-shelf product, the FBI elected to pioneer a secure in-house solution that eliminates any risk of data loss, spillover or exploitation. The BWC initiative involves the coordinated efforts of stakeholders throughout the FBI, including representatives from Operational Technology Division (OTD), Information Technology Applications and Data Division (ITADD), Critical Incident Response Group (CIRG), Criminal Investigative Division (CID), Training Division, Resource Planning Office (RPO), Office of the General Council (OGC), and Finance and Facilities Division (FFD), as well as multiple field offices. To date, the BWC program has met or exceeded multiple benchmarks relating to the selection and procurement of BWC hardware, the development of BWC policy and software/data storage solutions, the creation and implementation of both virtual and in-person training platforms. and the effective launch of the Phase I pilot program in which all 73 agents assigned to WFO's nine Violent Crime squads were trained and authorized to use BWC and utilized BWC on five arrest or search operations. Beginning in April 2022, the BWC program will launch a Phase II expansion that will deliver a BWC capability to four additional field offices (Miami, Milwaukee, Atlanta, and New York) and two FBIHQ components

(CIRG/SWAT/HRT and the FBI Academy New Agent Training Program). Phase II is predicated on the procurement of 500 additional BWC camera systems, currently on schedule to occur in late February 2022. Phase III in 2023 will expand the BWC program to the entire FBI enterprise.

The FBI is implementing BWC to increase transparency to the public and build public trust. BWCs are a widely accepted step in the right direction toward these goals. At this stage, BWC implementation is the primary goal, as BWCs are a new process for the FBI.

Performance Measure: Percent of federal law enforcement officers equipped with Body Worn Cameras (BWCs) and associated training.
FY21 Target: N/A
FY21 Actual: 1%
FY22 Target: 5%
FY23 Target: 50%
FY24 Target: 75%

Discussion
This measure is calculated based on the number of FBI agents that have completed BWC training and the number of BWC devices that have been provisioned and delivered to Field Offices. These numbers are controlled by BWC program management and are reported weekly.

b. Strategies to Accomplish Outcomes

The overriding performance measure relating to the BWC program is to deliver a fully secure and fully operational, enterprise-wide BWC capability. While the back-end infrastructure must be fully operational (and is therefore most of the workload in starting this initiative), the measure for BWCs is the number of FBI agents who are trained to use and equipped with BWCs. In order to meet this ultimate objective, the BWC program established interim timetables and benchmarks, all of which are on schedule to be met or exceeded. Prior to the initiation of the Phase I pilot program in October 2021, the BWC program established multiple working groups with distinct taskings aimed at establishing BWC Tools, Techniques, and Procedures. These initiatives have yielded a BWC Policy Guide that is currently in circulation for comment and final review and the development of an individualized framework for the collection and storage of digital evidence of the type generated by BWC.

Additionally, BWC conducted product selection that culminated in the award of a contract in February 2022 and the scheduled initial delivery of 500 camera systems by late February 2022. The continued success of the BWC initiative remains contingent upon the program receiving the requested $27.4 million in FY 2023. The $6.2 million appropriated in FY 2022 is for equipment, travel and contract staff associated with the execution of Phase II expansion. The FY 2023 funds are for costs associated with the Phase III enterprise-wide rollout.

Training Division (TD) and Office of the General Counsel (OGC):

a. Performance Plan and Report for Outcomes

In support of DOJ Strategic Objective 3: *Reform and Strengthen the Criminal and Juvenile Justice Systems to Ensure Fair and Just Treatment*, specifically the APG: *Promoting Trust in Law Enforcement through Transparency*, TD provides Use of Force training to all new agents at the FBI Academy, which teaches proper use of force for escalation and de-escalation. To ensure continued adherence to use of force protocols, and in support of FBI's fifth mission priority, *Protect Civil Rights*, TD provides, at minimum, mandatory annual training on use of force to all field agents. This training is typically organized and offered by field legal program personnel, in coordination with FBI's OGC. FBI's continued prioritization of of civil rights, equity, and justice is also in direct support of DOJ Strategic Goal 3: *Protect Civil Rights*. Additionally, this training supports the goals of FBI enterprise objective *Strengthen Confidence and Trust*.

Performance Measure: Percent of Special Agents who receive Use of Force Sustained Training within a 3 year period.
FY21 Target: *100%*
FY21 Actual: N/A
FY22 Target: 100%
FY23 Target: 100%
FY24 Target: 100%

Discussion
The measure is defined by how many new agents are trained in Use of Force each year, and the continuation of recurring mandatory annual training for onboard agents.

b. Strategies to Accomplish Outcomes

On September 13, 2021, the Deputy Attorney General issued a memorandum to the FBI and components related to the use of force, emphasizing a shared obligation to lead by example in a way that engenders the trust and confidence of the communities that it serves. The FBI's existing and continued training to both new and onboard special agents on proper use of force directly supports this obligation. FBI's culture of development and resilience encapsulates this operating posture and is consistent with the mission priority of protecting civil rights. TD will continue to teach proper use of force for escalation and de-escalation to all new agents at the FBI Academy and at a minimum provide Use of Force training annually for onboard field agents.

V. Program Increases by Item

Item Name: **Cyber**

Budget Decision Unit(s): All

Organizational Programs: Cyber

Program Increase: Positions 137 Agt 38 FTE 70 Dollars $51,975,000 ($21,069,000 non-personnel)

Description of Item

The FBI requests 137 positions (38 Special Agents (SAs)) and $51,975,000 ($21,069,000 non-personnel) to address the rapidly evolving cyber threats facing the nation.

The requested resources will strengthen the foundation needed for the FBI to remain the world's premier cyber investigative agency. These enhancements will better equip the FBI to work with allies and partners to impose risk and consequences on cyber adversaries through joint, sequenced operations. This request focuses on the development of three critical areas:

- Cyber Threat Identification, Analysis, and Attribution
- Cyber Threat Intelligence Platform
- Incident Response

This cyber enhancement request represents a continuation of the multi-year plan that positions the FBI to meet the demands of the present day's cyber threats. With the requested additional resources for cyber threat identification, analysis, and attribution, the FBI will be able to organize and analyze data to identify and act on adversary activity more quickly, enabling faster response throughout the USG. It will also develop and sharpen the FBI's cyber team's skills to help meet new threats head-on. Lastly, the FBI will be able to stop adversaries from escalating their attacks on U.S. infrastructure, public works, and private industry. The recent events of 2021 have made it clear that cyber threats are dynamic and constantly escalating. Having a synchronized, innovative, and interagency approach is necessary to impose a real and lasting impact on U.S. adversaries.

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

Item Name:	**Countering Acts of Mass Violence and Threats to Public Safety**
Budget Decision Units:	All
Organizational Programs:	Criminal Justice Information Services, Counterterrorism, Laboratory, Operational Technology

Program Increase: Positions 208 Agt 55 FTE 105 Dollars $48,826,000 ($11,741,000 non-personnel)

Description of Item

The FBI requests 208 positions (55 SAs) and $48,826,000 ($11,741,000 non-personnel) to effectively counter terrorism and the increasing acts of mass violence that threaten national security and public safety. The FBI must be able to identify, assess, collect intelligence on, and respond to potential threats. Specifically, the requested resources will be used to enhance the following areas:

- **DNA Capability Expansion:** The FBI requests $10,108,000 (all non-personnel) to effectively address the emerging requirements associated with the biometric identification capabilities to maintain public safety.
- **The National Instant Criminal Background Check System (NICS):** The FBI requests 70 positions and $6,234,000 (all personnel) to increase its capacity to enhance national security and public safety by conducting background checks to determine a person's eligibility to possess firearms or explosives in accordance with federal and state laws.
- **Combatting Domestic Terrorism and Hate Crimes:** The FBI requests 138 positions (55 SAs) and $32,484,000 ($1,633,000 non-personnel) to enhance its ability to detect and disrupt domestic terrorism (DT) threats across the nation.

Justification

The FBI holds a critical role in protecting the U.S. from threats to public safety, border security, the economy, and way of life. Fulfilling this role requires the FBI to further develop and use advanced methods to detect, prevent, and disrupt threats, leveraging human capital, information, and technology. Investment in these methods is critical to maintaining and enhancing the FBI's ability to address emerging and changing threats. Additionally, investments in this realm will help mission-critical information reach investigators, analysts, and partners and allow them to complete holistic strategic analysis and take action to prevent acts of violence and terror.

DNA Capability Expansion: $10,108,000 (all non-personnel)

DNA Expansion Capability: $10,108,000 (all non-personnel)

Recent changes in federal implementing regulations have increased the requirements for biometric identification capabilities to maintain public safety. Enacted in 2009, the DNA Fingerprint Act (in 34 U.S.C. § 40702(a)(1)(A) and (B)) authorized the Attorney General (AG) to collect DNA samples from individuals who are arrested, facing charges, or convicted, and from non-U.S. persons detained under U.S. authority. The law mandates Federal DNA collection agencies submit their arrestee collections to the FBI Laboratory for analysis and entry into the Combined DNA Index System (CODIS). In April 2020, the Department of Justice (DOJ) amended the DNA Fingerprint Act's implementing rule that now precludes the Department of Homeland Security (DHS) from waiving DNA collections on over 700,000 individuals per year.

The FBI has seen a significant increase in DNA databasing samples in FY 2021-FY 2022 (seven times the historical average, through December 2021) and requires additional funding to process and enter the increased number of genetic profiles into CODIS. The FBI estimates thousands of unsolved crimes would be resolved by full DHS DNA collections. The FBI coordinated with DOJ to plan for the impact of fully implemented DNA collections. As one part of this effort, DOJ commissioned an economist to develop cost models for the forecasted work expansion. The FBI has been working with DHS component agencies and built automated and streamlined workflows to minimize costs and administrative efforts for both agencies. However, without additional funding, a large backlog will continue to develop, putting stress on personnel, workflows, and equipment needed to upload DNA profiles into CODIS. This will also lead to a significant delay in adding new DNA profiles into CODIS and increase the likelihood of arrestees being released before identification through investigative leads. The number of samples receivedhas increased from 7,000 to 8,000 to approximately 50,000 to 60,000 per month since April 2021. With the requested enhancement funding, FDDU would have the ability to efficiently process an additional 228,000 samples into the national database each year.

The second DNA legislative change requiring FBI action is the Rapid DNA Act of 2017. This Act allows federal, state, and local booking agencies to process DNA samples taken from qualifying arrestees/detainees using a Rapid DNA device. The DNA samples are uploaded, and the DNA profile is queried against unsolved crimes of special concern in the national DNA database within CODIS. The results are returned within minutes, allowing for the immediate detention of these individuals. As stated in the Act, the FBI is required to build infrastructure and provide oversight of Rapid DNA technologies and capabilities. To maintain standardization and consistent performance for this national program, the FBI must also implement this technology in federal booking stations. As the lead agency for Rapid DNA, it is imperative the FBI implement the new technology in FBI booking locations.

The USG has a need for a robust DNA database to protect the public and quickly identify individuals who have committed violent crimes in the past and may commit similar acts in the future. Successful delivery on these key initiatives will lead to significant benefits to public safety through increasing the size of the national DNA database and the speed of analysis through modern technology. Both efforts yield dividends for federal, state, and local law enforcement agencies and, when combined, have the potential to revolutionize border security and the speed with which perpetrators are identified. The FBI requests $10,108,000 in non-personnel funding.

Table 1 provides the detailed requirements to address both legislative initiatives and the capability expansions required to fulfill the statutory requirements.

Table 1: Non-Personnel Request Summary				
Item	**Details**	**Rapid DNA**	**DHS-related DNA**	**Total Cost**
Contract - Services	Contractor support	$0	$388,000	$388,000
Supplies - Laboratory	Consumable reagents/supplies	$312,500	$5,519,600	$5,832,100
IT Hardware	Lab instruments	$937,500	$393,800	$1,331,300
Other	Instrument service maintenance agreements	$312,500		$312,500
Other	Collection kits	$0	$1,808,100	$1,808,100
Other	Storage	$0	$60,500	$60,500
IT Maintenance	IT maintenance enhancements	$312,500	$0	$312,500
Travel - Training	Instrument guidance	$31,500	$0	$31,500
Travel	Audits	$31,500	$0	$31,500
Total		**$1,938,000**	**$8,170,000**	**$10,108,000**

The ability to successfully implement Rapid DNA in booking stations requires considerable planning and training. This enhancement will enable the FBI to continue the implementation of its Rapid program. The FBI has conducted successful Rapid DNA pilots in four states and has recently completed all legislatively mandated tasks required by the Rapid DNA Act of 2017. The FBI is ready for the implementation of Rapid DNA for qualifying arrestees at the booking station.

This enhancement is based on logical implementation using historical process rates and operational tempo as a guide. As it pertains to the DHS-related DNA initiative, in FY 2019, the FDDU received over 94,000 samples from federal law enforcement agencies and was appropriately resourced for that volume. DOJ has estimated upon full implementation the FBI Laboratory would be receiving up to 748,000 additional samples per year. In FY 2021, the FDDU saw sample volumes increasing to 40,000 per month and estimates maximum collections at 60,000 per month (i.e., 600,000-720,000 per year) in coming months. The demand signal from DHS is not scalable but is based on the number of samples received and the capacity output of existing personnel and instruments. With the requested enhancement funding, FDDU would have the ability to efficiently process an additional 228,000 samples into the national database each year. For Rapid DNA, the enhancement allows for a scalable implementation. The scaling refers directly to the idea of adding additional FBI booking locations each year of Rapid deployment (instruments, instrument service agreements, and deployment into the out-years).

NICS: 70 positions and $6,234,000 (all personnel)

The FBI recognizes and appreciates the $125 million in supplemental funding provided by Congress for NICS in FY 2021 (two-year funds). This funding continues to be instrumental in adding much needed personnel resources, augmenting IT development staff, and enhancing the productivity of NICS through an improved telework posture. This significant infusion of much needed resources is making a difference in the timeliness and effectiveness of processing gun background checks. The workloads have been sustained at record breaking volume that still require additional government staff above the 146 positions provided through the FY 2021 appropriation and supplemental. The workload models, productivity numbers, and other NICS work beyond gun background checks indicate additional positions are still needed to properly staff NICS. The FBI acknowledges the ongoing system improvements and enhancements being performed with the FY 2021 supplemental funds will lead to system efficiencies, and this has been considered when requesting the FY 2023 enhancement.

The Brady Handgun Violence Prevention Act of 1993 added a time sensitive component to NICS operations, giving the FBI three business days to determine a person's eligibility to purchase a firearm. After the close of the third business day, the Federal Firearms Licensee (FFL) may legally transfer the firearm, at their discretion, without a response from the NICS. The FBI's NICS mission is to complete as many checks as possible prior to the third business day; however, as depicted in Table 2 below, there are transactions that go unresolved after the third business day. The transactions and percentage of transactions in this category increased in Calendar Year (CY) 2020.

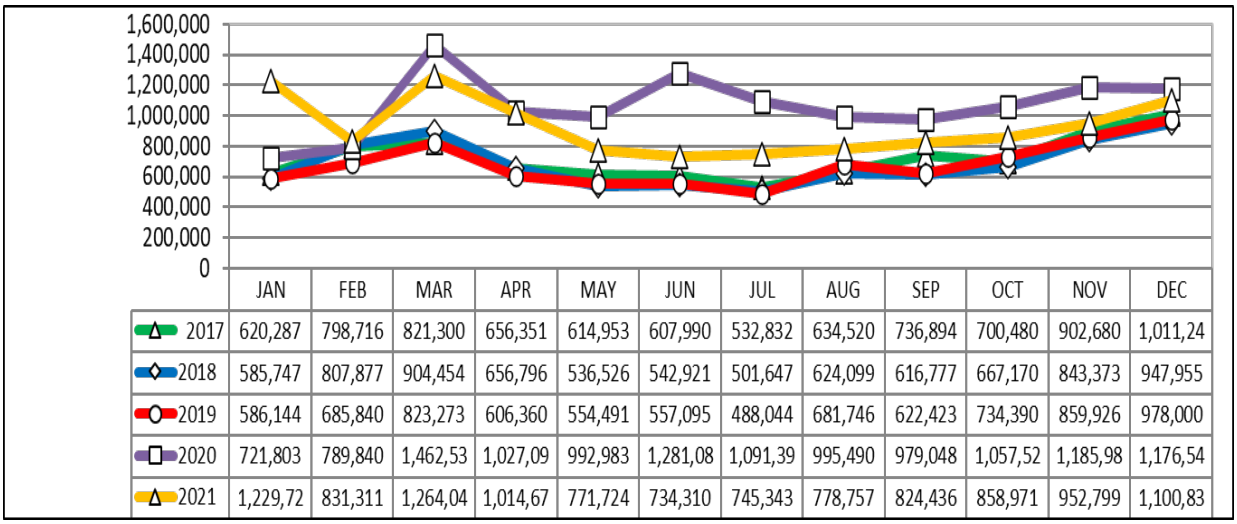
Table 2: Unresolved Transactions Exceeding Three-Business Days

Unresolved Transactions Exceeding Three-Business Days						
Calendar Year	2019		2020		2021	
January	18,624	3.26%	20,759	3.09%	43,584	3.64%
February	23,281	3.53%	26,149	3.42%	30,762	3.93%
March	28,089	3.59%	76,558	5.37%	61,763	5.09%
April	19,540	3.39%	48,519	4.90%	48,772	4.95%
May	17,947	3.42%	50,280	5.20%	36,249	4.80%
June	17,337	3.24%	64,086	5.10%	37,191	5.16%
July	16,155	3.51%	55,240	5.19%	32,419	4.49%
August	21,688	3.32%	40,923	4.24%	31,415	4.13%
September	20,581	3.41%	36,969	3.92%	34,594	4.33%
October	23,640	3.55%	37,645	3.69%	34,896	4.14%
November	26,784	3.23%	41,164	3.55%	36,039	3.89%
December	27,646	2.95%	37,494	3.28%	38,804	3.59%
Total	**261,312**	**3.35%**	**535,786**	**4.33%**	**466,488**	**4.32%**

The FBI requests 70 positions and $6,234,000 (all personnel) to increase its capacity to perform NICS background checks for firearm purchases. The additional positions will enhance the NICS Program's ability to complete transactions within three business days, meet service levels of the

NICS E-Check and telephone responses, effectively provide additional services to the law enforcement community and its customers, and lead system development efforts. Since the beginning of CY 2020, the NICS Program has seen a considerable increase in incoming federal firearms background checks, illustrated in the table below.

Table 3: Federal Transaction Volume



	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC
2017	620,287	798,716	821,300	656,351	614,953	607,990	532,832	634,520	736,894	700,480	902,680	1,011,24
2018	585,747	807,877	904,454	656,796	536,526	542,921	501,647	624,099	616,777	667,170	843,373	947,955
2019	586,144	685,840	823,273	606,360	554,491	557,095	488,044	681,746	622,423	734,390	859,926	978,000
2020	721,803	789,840	1,462,53	1,027,09	992,983	1,281,08	1,091,39	995,490	979,048	1,057,52	1,185,98	1,176,54
2021	1,229,72	831,311	1,264,04	1,014,67	771,724	734,310	745,343	778,757	824,436	858,971	952,799	1,100,83

In CY 2020, and the beginning of CY 2021, the NICS set records for transaction volume, with multiple days, weeks, and months ranking in the top ten, as reflected in Table 4. The increase has severely pressured the NICS Section to complete firearm transactions within three business days. In CY 2021, the NICS Program's transaction volume continues to remain at a high level.

Table 4: NICS Firearm Background Checks Top 10 Highest (Days/Weeks/Months)

NICS Firearm Background Checks
Top 10 Highest Days

November 30, 1998 - February 28, 2022

Rank	Date	Total Checks
1	Wed, Mar 17, 2021	236,295
2	Tue, Mar 30, 2021	220,655
3	Thu, Mar 25, 2021	212,008
4	Fri, Mar 20, 2020	210,308
5	Thu, Mar 18, 2021	209,332
6	Mon, Mar 29, 2021	208,002
7	Fri, Nov 24, 2017	203,086
8	Fri, Nov 29, 2019	202,465
9	Fri, Mar 19, 2021	195,983
10	Fri, Nov 26, 2021	187,585

NICS Firearm Background Checks
Top 10 Highest Weeks

November 30, 1998 - February 28, 2022

Rank	Dates	Total Checks
1	03/15/2021 - 03/21/2021	1,218,002
2	03/16/2020 - 03/22/2020	1,197,788
3	01/11/2021 - 01/17/2021	1,082,449
4	03/22/2021 - 03/28/2021	1,080,245
5	01/04/2021 - 01/10/2021	1,071,820
6	03/29/2021 - 04/04/2021	1,037,344
7	06/01/2020 - 06/07/2020	1,004,798
8	01/18/2021 - 01/24/2021	976,637
9	12/14/2020 - 12/20/2020	973,470
10	12/17/2012 - 12/23/2012	953,613

NICS Firearm Background Checks
Top 10 Highest Months

November 30, 1998 - February 28, 2022

Rank	Month	Year	Total Checks
1	March	2021	4,691,738
2	January	2021	4,317,804
3	December	2020	3,937,066
4	June	2020	3,931,607
5	March	2020	3,740,688
6	July	2020	3,639,224
7	November	2020	3,626,335
8	April	2021	3,514,070
9	February	2021	3,442,777
10	December	2015	3,314,594

NOTE: These statistics represent the number of firearm background checks initiated through the NICS. They do not represent the number of firearms sold. Based on varying state laws and purchase scenarios, a one-to-one correlation cannot be made between a firearm background check and a firearm sale.

Once a transaction receives a delay status, it is assigned to the Delay Queue for the NICS Legal Instrument Examiner (LIE) to conduct research. To correctly process NICS transactions, with minimal impact to public safety, the NICS LIEs should begin processing Delay Queue transactions on the first business day; however, due to the heightened volume, many transactions

are not pulled to work until the second or third business day. During CY 2020, there were 79 days in which the NICS Delay Queue had untouched transactions waiting to be worked that were in the third business day. This reduces the time for LIEs to perform external research to obtain dispositions, court documents, or police reports on thousands of transactions. After the close of the third business day, the FFL may legally transfer the firearm, at their discretion, without a response from the NICS, creating a potential public risk.

Due to the high transaction volume, there are instances where the NICS Program is unable to begin a review of a transaction and complete it prior to the third business day. If an FFL releases a firearm without a determination from the NICS, a risk is created to law enforcement and the public as a potentially prohibited person may be in possession of a firearm. There were zero days of transactions not being reviewed prior to the third business day in CY 2019; however, there were six days involving 5,844 transactions in CY 2020 (see table below).

Table 5: Transactions Not Reviewed within 3 Business Days

Date	Transactions 4th Day
March 26, 2020	1,802
June 6, 2020	161
June 11, 2020	1,762
June 18, 2020	1,447
June 19, 2020	180
June 25, 2020	492

Although there has been progress in obtaining FSL increases and making technological improvements, the NICS Program still has a personnel requirement to process the increasingly demanding workload. The FBI continues to mitigate the staffing shortfall through the following efforts:

- Redirecting approximately 140 FBI employees from other NICS support functions such as processing Voluntary Appeal File (VAF) requests, updating the NICS Indices, and handling explosive checks. This occurred during 196 days of CY 2020.
- Restricting employee leave during peak volume periods, including eliminating almost all leave between Thanksgiving and New Year's Day.
- Instituting mandatory overtime (a total of 156,000 hours of overtime was used in FY 2020 and 143,600 hours of overtime were used during FY 2021).
- Utilizing contractor support to perform limited portions of the background check process such as research that is not inherently governmental in nature.

The NICS Program has a known staffing shortfall, but when national emergencies arise, needs are further exacerbated due to the intensified workload and increased volume of firearm background checks. Additional staff must be provided to ensure the FBI can process the incoming volume of firearm background check transactions in a timely manner. Accelerating the completion of NICS firearm checks has a negative impact on the quality of the checks. This, in turn, has a direct public safety correlation and thus is not a viable strategy. Additional personnel are essential to maintain the integrity of the NICS Program.

Combatting Domestic Terrorism (DT) and Hate Crimes: 138 positions (55 SAs) and $32,484,000 ($1,633,000 non-personnel)

Combatting DT: 131 positions (55 SAs) and $28,741,000 ($596,000 non-personnel)

The DT threat has expanded significantly in the past year, as seen in civil unrest and rioting arising from an increase in Anti-Government or Anti-Authority Violent Extremism (AGAAVE). In 2020, the FBI saw more DT investigative activity in the U.S. than any year for the previous 25 years. The heightened threat posed by Domestic Violent Extremists (DVEs) has been recognized at the highest levels of the US Government, as evidenced by the first ever inclusion of DT threats in the October 2018 National Strategy for Counterterrorism, the April 2020 designation of the Russian Imperial Movement – which promotes racially or ethnically motivated violent extremism (RMVE) – as a Specially Designated Global Terrorist, and the White House's June 2021 release of the National Strategy for Countering DT.

To mitigate this violent criminal activity, the FBI's DT program took tangible actions over the past year. The FBI elevated AGAAVE to the highest threat priority, on par with RMVE (elevated in 2019) and expanded the use of advanced investigative techniques. The FBI also enhanced its partnerships across multiple sectors through continuing to consistently collaborate with established partners (e.g., state/local law enforcement) and strengthening coordination and communication with other partners (e.g., the National Counterterrorism Center, DHS, private sector/academia). These measures directly contributed to significant disruptions of DVEs, to include RMVEs associated with groups such as the The Base and Atomwaffen Division and AGAAVEs involved with the Wolverine Watchmen. However, over the same period, FBI resources dedicated to combatting DT remained flat.

The greatest terrorism threat facing our Homeland is posed by lone actors or small cells, who typically radicalize online, and who primarily look to use easily accessible weapons to attack soft targets. In 2021, DVEs' continued use of encrypted communication applications and utilization of operational security required the FBI's DT program to employ more resource-intensive investigative techniques than in years past, to include long-running undercover operations. Given many DVEs' propensity to seek out easily accessible weapons, the DT program has been forced to increase its surveillance coverage of subjects to mitigate potentially lethal threats. The aforementioned investigative techniques, as well as many others that are regularly employed, necessitate more advanced technical capabilities and increased manpower, which require additional case funds to enable the FBI's DT program to effectively execute operations and monitor potentially violent threat actors more effectively.

.

Positions	Field	HQ
Special Agents	40	15
Intelligence Analyst	12	6
Staff Operations Specialist	24	14
Professional Staff (MAPAs)	0	20

The additional personnel would more appropriately staff the DT-focused workforce in both Field Offices and Headquarters to meet the ever-growing DT threat. There is a need to provide analytic and other intelligence-related support to all levels of the FBI, as well as other government agencies, law enforcement partners, and others, and assist with preparing strategic and programmatic products. It is also necessary to establish close working relationships with investigative managers, Field Offices, and analytic elements to facilitate information sharing across programs. An increase in personnel will improve the ability to conduct research and analysis to identify emerging trends on the various domestic violent extremism movements and maintain a close liaison with law enforcement, private sector, and the US Intelligence Community. This will also maximize analytic information exchange and continue to build and maintain a cadre of highly skilled professional analysts with substantive expertise through recruitment efforts and career enhancement opportunities.

The FBI request for additional DT resources in FY 2023 is similar to the requested combatting DT resources in FY 2022. However, the FY 2022 request was formulated with data reflecting the DT landscape in FY 2020, while the FY 2023 request is built upon the rapidly evolving DT landscape in FY 2021. During this time, the FBI has seen a nearly 200% increase in caseload, increased sophistication in DT use of technology, and heightened activity by violent DT actors. The threat of further escalation in the DT landscape between FY 2021 and FY 2023, without an appropriate increase in resources, can create the perfect storm for threat actors to exploit US vulnerabilities against the safety of the public. The requested funding will support FBI efforts to identify and investigate other DT threats, making the United States safer.

Response to Domestic Terrorism and Hate Crimes: 7 positions and $2,706,000 (all personnel)

The FBI requests 7 professional staff positions and $2,706,000 (all personnel) to effectively respond to the growing instances of incidents related to DT and hate crimes. This request will enhance the FBI's ability to effectively respond to crime scenes and complete the exams, documentation, trial exhibits, and reports that require months, even years of work, following the incident. Mass violence incidents like those at the Charleston church, Pittsburgh Synagogue, Gilroy Festival, and the El Paso Walmart are stark reminders of the broad and substantial occurrences of DT and hate crime incidents. The increase in occurrences of mass shootings is further compounded by the proliferation of military grade assault weapons with high-capacity magazines carrying high velocity ammunition resulting in larger and more complex shooting scenes. The increase in both frequency and scope of shootings has impacted several response functions supported by the FBI, resulting in a significant strain on available resources to respond, conduct laboratory examinations, generate follow-on products, and support prosecution and courtroom testimony.

FBI response personnel perform a unique set of specialized functions when deployed to scenes of mass violence and are additionally tasked with other mission-critical duties, such as generating reports, product creation, testifying in criminal cases, and providing training related to their areas of expertise. These tasks place additional demands on a limited number of responders. Table 6 provides the requested position enhancement by response functional area. While the increase in DT and hate crimes has driven the increased need for response personnel, the employees in the

requested 7 positions would deploy for other cases in addition to DT and hate crime cases where their expertise and skills are required.

Position Enhancement Request

Function	Current Responder Count	Requested Positions
Firearms/Toolmarks Crime Scene Examination Support	15	3
Complex Evidence Access and On-Site Safety Function	34	2
Operational Projects Unit -Advanced Documentation and Imaging	32	2
Total Personnel	**81**	**7**

The FBI's Firearms/Toolmarks Unit (FTU) has 15 responders that provide on-scene analysis of bullet holes and impacts. Through this analysis, they can determine the number of shots fired and the direction from which shots originated. A small shooting scene could involve a single responder for one day plus travel time, whereas a large shooting scene could require a team of four responders for up to two weeks. In 2019, FTU conducted 17 on-scene responses, requiring 229 "personnel workdays" deployed. The pandemic decreased the number of deployments in 2020. In 2021, FTU participated in 17 laboratory shooting reconstruction team deployments, involving 30 FTU personnel and requiring 126 "personnel workdays" deployed.

The FBI's Operational Projects Unit (OPU) which is responsible for providing advanced, on-site crime scene documentation and re-construction services utilizing technical imagery and modeling, has experienced a 50% increase in DT and Hate Crime related deployments. This mission is accomplished by highly skilled personnel specialized in accurate and responsive technical documentation, laser scanning, drone operations, and photographic, graphic, and physical modeling, in support of FBI investigations and subsequent prosecutions. The OPU personnel responsible for these services have subject matter expertise in crime scene documentation, photography, demonstrative exhibit creation, apparatus development, and forensic facial imaging. Crime scene support includes aerial photography for geo-referenced overhead imagery used to prepare crime scene diagrams, digitally interactive maps, and scenario reconstruction. It also includes metrology and advanced photography services used to create highly accurate and detailed visual records of scenes produced in concert with other FBI response functions.

The FBI's Technical Hazards Response Unit (THRU) provides complex evidence access and on-site safety functions. THRU is responsible for providing advanced on-site crime scene support including rapid movement of all deployment platforms and equipment, establishing on-site base of operations and logistics, complex evidence access (rope operations, confined spaces, heavy tools, excavations), secret and unclassified internet and radio communications, site safety, and paramedical medical care. Post-deployment, the unit is responsible for demobilization and reconstitution of equipment used in support of FBI operations. For large deployments, this

process is completed in an average of approximately three days. The process is accomplished through the subject matter expertise of Forensic Operations Specialists and Telecommunications Specialists within THRU.

THRU teams must be staffed for immediate support to two National Security Mission sets, WMD and Domestic/International Terrorism as well as complex crime scenes in support of criminal investigations. THRU is operating at deficient staffing levels and additional staff would reduce the number of times individual staff are unexpectedly rotated into a deployment status and enable the unit to cover concurrent and back-to-back deployments.

Domestic Terrorism (Technical Capabilities): $1,037,000 (all non-personnel)

The FBI requests $1,037,000 (all non-personnel) to effectively counter terrorism and the increasing acts of domestic violent extremists. The FBI must be able to identify, assess, and respond to potential threats. Specifically, the requested resources will be used to enhance the DT program and support the FBI's multimedia processing.

The FBI requests funding to continue the procurement of cloud services necessary to build, operate, and manage the FBI's multimedia processing and exploitation enterprise. The major components of the enterprise include the Triage Toolkit (TTK), Multimedia Processing Framework (MPF), biometric systems, and the forensic exploitation tool Analog.

The TTK program is the flagship application for multimedia exploitation, review, and analysis. It automates processes that were previously manual and labor intensive, and it enables collaboration during exploitation to a degree not before possible. MPF is an application that allows for plug and play inclusion of computer vision tools to intelligently locate pertinent content in large multimedia collections. It performs functions such as person, vehicle, and motion detection.

Additionally, the FBI develops and maintains biometric systems for operational use. Systems such as the Sensitive Data Exploitation Lab provide facial recognition of pertinent subject data harvested from digital evidence and can compare those faces against millions of individuals in partner agency systems. Analog is a forensic exploitation tool developed to exploit digital evidence. It allows for the forensic extraction and review of data from hard drives, cell phones and other digital media. It also allows users to recover deleted data such as text messages, exposes chat applications and call lists, and much more.

The FBI provides these tool kits and services on the Operational Wide Area Network (OPWAN) and the Digital Collection and Analysis Platform (DCAP) to state and local partners. The requested funds will be used to continue to provide and expand the program's service offering to all levels of law enforcement through the platform. DCAP has been used to support cases such as the Capitol Riots. Without this funding, the FBI will not be able to support the expanding DCAP initiative and will result in serious mission hinderance at Regional Computer Forensic Laboratory (RCFL) locations.

The FBI must have technical tools and personnel in place to address grave threats to national and public safety, from initial information or tip intake, through analysis, sharing, and investigation. With these enhanced capabilities, the FBI will be able to better address national security threats in part by eliminating backlogs, reducing response time to partners, illuminating trends, identifying new targets, and increasing information sharing.

Impact on Performance

The technological demands, vast volumes of data, and grave threats posed to national security require the FBI to continually evolve to protect the American people. FBI investigators cannot continue to rely solely on the tools, investigative methods, and resource levels of the past to address threats to national and international security with implications to public safety, public health, democratic institutions, and economic stability across the globe. The FBI must have the technical tools and personnel in place to address these threats from initial information or tip intake, through analysis and sharing, and finally investigation. With these enhanced capabilities, the FBI will be able to better address national security threats in part by eliminating backlogs, reducing its response time to partners, completing mandated checks within the required timeframe, illuminating trends, identifying new targets, and increasing information sharing.

Funding

1. **Base Funding**

FY 2021 Enacted				FY 2022 President's Budget				FY 2023 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
2,643	757	2,628	$444,682	2,790	837	2,805	$494,297	2,769	836	2,768	$494,097

2. **Personnel Increase Cost Summary**

Type of Position/Series	Positions Requested	Annual Costs per Position ($000)			FY 2023 Request ($000)	Annualizations ($000)	
		1st Year Adjusted Cost	2nd Year Adjusted Cost	3rd Year Full Cost (Modular)		FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Special Agent, Field	55	$328	$276	$397	$18,063	($2,867)	$6,710
Intelligence Analyst	18	$183	$192	$258	$3,295	$158	$1,188
Clerical	59	$84	$114	$156	$4,966	$1,741	$2,537
Information Technology	10	$115	$219	$254	$1,150	$1,037	$360
Professional Support	21	$118	$158	$227	$2,485	$853	$1,470
Forensic Examiner	3	$408	$335	$374	$1,224	($215)	$120
Non-Agent Responder	4	$370	$250	$284	$1,482	($479)	$136
Staff Operations Specialist	38	$116	$155	$189	$4,420	$1,467	$1,330
Total Personnel	**208**	**$1,724**	**$1,698**	**$2,138**	**$37,085**	**$1,695**	**$13,851**

3. Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	FY 2023 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Case Funds	$596	N/A	N/A	$0	$0
Contract – Service	$388	N/A	N/A	$0	$0
Contract – Training	$32	N/A	N/A	$0	$0
Equipment	$2,181	N/A	N/A	$0	$0
IT-Services	$1,350	N/A	N/A	$0	$0
IT-Supplies	$1,331	N/A	N/A	$0	$0
Supplies	$5,832	N/A	N/A	$0	$0
Travel	$32	N/A	N/A	$0	$0
Total Non-Personnel	**$11,741**	**N/A**	**N/A**	**$0**	**$0**

4. Justification for Non-Personnel Annualizations

FBI costs related to countering acts of mass violence has been driven by a 57% increase in domestic terrorism cases, which involve actors with a high propensity for violence. The non-personnel costs are primarily attributed to enhancing technical capabilities, consumption of supplies for rapid DNA testing, and investigative work expenses required to sustain the growth for supporting personnel in the field and at HQ. Due to the increase in cases and domestic terrorism activity not expected to subside during outyears, the FBI requests that non-personnel costs recur in 2024 and 2025 to continue the mitigation of violent activity.

5. Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Current Services	2,769	836	2,768	$449,234	$44,863	$494,097	N/A	N/A
Increases	208	55	105	$37,085	$11,741	$48,826	$1,695	$13,851
Grand Total	**2,977**	**891**	**2,873**	**$486,319**	**$56,603**	**$542,922**	**$1,695**	**$13,851**

Item Name: **Counterintelligence**

Budget Decision Unit(s): All

Organizational Program: Counterintelligence, Operational Technology

Program Increase: Positions 88 Agt 14 FTE 46 Dollars $34,142,000 ($16,759,000 non-personnel)

Description of Item

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

Item Name: **Combatting Crime and Corruption**

Budget Decision Unit: All

Organizational Programs: Criminal Investigative, Critical Incident Response, International Operations, and Operational Technology

Program Increase: Positions 22 Agt 15 FTE 12 Dollars $20,574,000 ($13,258,000 non-personnel)

Description of Item

The FBI requests 22 positions (15 SAs) and $20,574,000 ($13,258,000 non-personnel) to effectively address the increasing threat posed by criminal organizations, including those that utilize advanced technology to further nefarious agendas detrimental to public safety and economic stability. Specifically, the requested resources will be used to enhance the following areas:

- **Transnational Organized Crime (TOC):** The FBI requests three (3) positions (3 SAs) and $5,476,000 ($3,213,000 non-personnel) to combat the TOC threat. The TOC threat poses significant and growing national and international threats to security with implications for public safety, public health, democratic institutions, and economic stability. The TOC threat encompasses a myriad of activities impacting the U.S., including drug and weapons trafficking, human trafficking and smuggling, violence, corruption, money laundering, cultural artifact trafficking, and fraud. TOC groups increasingly exploit jurisdictional boundaries to conduct their criminal activities overseas. Furthermore, they are expanding their use of emerging technology to traffic illicit drugs and contraband across international borders and into the U.S.
- **Sophisticated Tools to Combat Child Sex Offender Technology:** The FBI requests four (4) positions (2 SAs) and $6,080,000 ($5,026,000 non-personnel) to increase the FBI's investigative capacity and capabilities to mitigate technologically advanced and complex criminal activities, such as criminal organizations utilizing encrypted communications and illicit activities on the Dark Web. These crimes are difficult to address through traditional methods.
- **Combatting Violence Against Women:** The FBI requests 15 positions (10 SAs) and $5,337,000 ($1,338,000 non-personnel) to support the Combatting Violence Against Women initiative to best address the inadequacies in conducting investigations of missing or murdered indigenous persons in the U.S.
- **Cell Site Simulators (CSS)**: The FBI requests $3,681,000 (all non-personnel) for CSS. Additional details are law enforcement sensitive (LES) and are included in the FBI's classified addendum.

Impact on Performance

The resources requested here will significantly improve the FBI's technical expertise, foster innovation, and enhance staffing levels to effectively tackle the most detrimental criminal activities and threats to the safety and security of the American people and U.S. equities abroad.

These enhancements further the FBI's priorities and directly support the Department's updated strategic goals and objectives for FY 2022 – FY 2026. These resources will allow the FBI to develop, increase, and maintain technical expertise on specialized teams, develop the necessary investigative tools for these teams to use, and stay ahead of future criminal threats.

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

(U) Item Name: **Civil Rights Crimes**

Budget Decision Unit(s): All

Organizational Programs: Criminal Investigative

Program Increase: Positions 92 Agt 33 FTE 46 Dollars $17,786,000 (all personnel)

Description of Item

The FBI requests 92 positions (33 Special Agents) and $17,786,000 to support its Civil Rights Program by adding tactical specialists, FBI personnel, and training law enforcement partners. This enhancement is necessary for the FBI to effectively address the recent increases in civil rights violations and proactively mitigate them before they occur.

Justification

Civil Rights Crimes (CRC): 92 positions (33 Special Agents) and $17,786,000 (all personnel)

Civil rights crimes are among the most egregious violations of federal law—they include color of law violations, hate crimes, Free Access to Clinic Entrances (FACE) Act violations, and voter suppression. These crimes cause long-term, enduring damage to communities and economic infrastructure, compromise law enforcement and judicial system capabilities, and provoke widespread fear and trauma. The FBI has witnessed a stark increase in civil rights crimes in recent years. In FY 2020, the FBI initiated 271 color of law cases, a 24% increase from FY 2019. Color of law incidents serve as a catalyst for mass demonstrations, shown by the civil unrest experienced across the U.S. from May through September 2020. During this time, there was a 49% increase from the number of FY 2019 cases initiated during the same timeframe. Hate crime investigations also increased in FY 2020, with a total of 207 total cases that year (a 63% increase over FY 2019); of those, 125 were initiated during the civil unrest from May through September. The investigation of civil rights crimes is a top criminal priority, and the FBI has committed to dedicating additional resources and efforts to investigating these crimes.

To provide more support to field offices, the FBI requests funding for 56 Staff Operations Specialists-Tactical Specialists (SOS/TS), one for each field office. These SOS/TSs are responsible for providing tactical support to operational squads in field offices to further case development. They conduct extensive research of a multitude of datasets and produce reports that initiate new investigations; construct link charts, timelines, and other analytical tools for investigators; participate in investigative strategy and prosecution discussions and briefings; and draw conclusions from digital and other collected evidence. Specific to the CRC threat, field offices can use SOS/TSs in all aspects of their efforts to initiate new investigations, work and advance existing investigations, and conduct outreach and liaison activity with law enforcement, nongovernmental organizations, academic, and private sector partners. By way of example, during March and April 2019, three Baptist and predominantly African American churches were

the victims of suspicious fires. During and after the command posts, which were convened to investigate these incidents, SOS/TSs conducted open-source checks, FBI record checks, and social media exploitation. They also authored a product identifying Holden Matthews as the perpetrator. Their work was critical to Matthews' indictment under the Church Arson statutes. He received a federal sentence of 282 months in prison and was ordered to pay $2.66 million in restitution.

To meet the expected increase in workload and demand, the FBI is also requesting 28 Special Agents to go to those FBI field offices with the greatest need for additional Agent support on their civil rights squads. These SAs will work together with the SOS/TSs mentioned above to identify and follow leads, open new investigations, and conduct community outreach. To meet the ongoing needs of the field and continue support for these programs, the FBI also requests funding for 5 Supervisory Special Agents (SSAs), 1 Management and Program Analyst (MAPA), 1 Data Analyst, and 1 SOS/TS for the Civil Rights Unit and Civil and Human Rights Intelligence programs at FBI Headquarters (HQ). These added positions will ensure investigations are nationally coordinated and provide tactical and case management support to field offices.

Beyond investigative work, the FBI recognizes proper and thorough handling of civil rights crimes does not begin the moment they are reported—it begins before they occur, with a solid and trusting relationship between the community and law enforcement. Since civil rights crimes are now one of the highest criminal priorities, each field office will be instructed to take specific actions to combat civil rights crimes in their area of responsibility (AOR) to encourage systemic change. These actions will include a task to identify the appropriate partner agencies and local groups to assist with development of outreach relationships in the AOR at all levels, focusing on executives, with the goal of sparking institutional change. It is anticipated that this emphasis on executive-level outreach will result in an increase in civil rights-focused working groups and task forces with state, local, private, public, and non-profit partners. These collaborative settings will lead to more opportunities for reporting and case initiations and offer a platform to identify and discuss trends. The proposed outreach plan will also drive increased enhanced trainings for state and local agencies and community groups centered on color of law investigations and hate crimes statutes. The aim of these trainings is to provide education to partners about civil rights violations, promote increased reporting of hate crimes, and rebuild community trust in law enforcement.

Impact on Performance

These requested resources are paramount for the FBI to continue its mission to reach vulnerable communities and reinforce the FBI's dedication to investigating and bringing to justice the perpetrators of civil rights crimes. Additional personnel will provide a necessary increase to the investigative and tactical support of FBI field operations.

Funding

1. **Base Funding**

FY 2021 Enacted				FY 2022 President's Budget				FY 2023 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
299	178	294	$57,177	299	178	285	$53,142	315	185	319	$63,575

2. **Personnel Increase Cost Summary**

Type of Position/Series	Positions Requested	Annual Costs per Position ($000)			FY 2023 Request ($000)	Annualizations ($000)	
		1st Year Adjusted Cost	2nd Year Adjusted Cost	3rd Year Full Cost (Modular)		FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Data Analyst	1	$199	$219	$265	$199	$21	$47
Professional Support	1	$118	$158	$227	$118	$41	$70
Special Agent, Field	33	$328	$276	$397	$10,838	($1,720)	$4,026
Staff Operations Specialist	57	$116	$155	$189	$6,631	$2,201	$1,995
Total Personnel	**92**	**$762**	**$808**	**$1,078**	**$17,786**	**$542**	**$6,138**

3. **Non-Personnel Increase/Reduction Cost Summary**

Non-Personnel Item	FY 2023 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
N/A	$0	N/A	N/A	$0	$0
Total Non-Personnel	**$0**	**N/A**	**N/A**	**$0**	**$0**

4. **Justification for Non-Personnel Annualizations**

5. **Total Request for this Item**

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Current Services	315	185	319	$61,435	$2,140	$63,575	N/A	N/A
Increases	92	33	46	$17,786	$0	$17,786	$542	$6,138
Grand Total	**407**	**218**	**365**	**$79,221**	**$2,140**	**$81,361**	**$542**	**$6,138**

Item Name: **Cybersecurity**

Budget Decision Unit: All

Organizational Programs: Office of the Chief Information Officer, Information Technology

Program Increase: Positions 9 Agt 1 FTE 5 Dollars $36,948,000 ($35,686,000 non-personnel)

Description of Item

The FBI requests 9 positions and $36,948,000 ($35,686,000 non-personnel) to enhance its cybersecurity posture. FBI data, including national security data, is vulnerable to external cyber and insider threat attacks. Current tools are not capable of fully monitoring the numerous enterprise systems in place across the FBI and are not entirely prepared for the ever-changing technological landscape, including the emergence of the cloud and the increase in mobile platforms. The FBI must invest in tools to enhance its cybersecurity posture to meet federal mandates for a secure IT enterprise.

The requested resources will enhance the following areas:

- **Cybersecurity Posture:** the FBI requests 6 positions and $32,990,000 ($32,287,000 non-personnel) to ensure robust cybersecurity through targeted investments in IT asset monitoring and risk assessment of FBI systems.
- **Cybersecurity Threat Assessment Program:** the FBI requests 3 positions (1 Special Agent) and $3,958,000 ($3,399,000 non-personnel) to proactively address the growing cyber threat posed by groups that exploit technology to breach FBI technical systems and networks with the intent to cause harm to the FBI's mission and reputation.

The FBI's FY 2023 request builds off the enhancement resources requested in the FY 2022 President's Budget. Though the requested FY 2022 enhancement met the requested need, a number of critical cybersecurity requirements remain to address the growing threats facing the FBI. The FY 2023 request seeks to provide additional resources to further meet these requirements and combat evolving vulnerabilities. These emergent threats were made evident by recent events associated with Solarwinds, the Colonial pipeline attacks, Buffalo Public Schools, and others.

None of the FBI's FY 2023 enhancement request is duplicative of the FY 2022 President's Budget request. Though both years augment the agency's Cybersecurity Posture and the Threat Assessment Program, the two requests are separate and distinct. The largest example is the portion of the FY 2023 request boosting the Bureau's Central Logging and Analysis capabilities, unaddressed in FY 2022. Further, though the FY 2023 Threat Assessment Program request is similar in approach and subject matter, its goal is to build off the FY 2022 request to foster the FBI's ability to assess internal threats.

Justification

To keep pace with today's emerging threats and fully implement requirements in the recent Cybersecurity Executive Order (EO 14028), the FBI must make substantial cybersecurity improvements to ensure a more secure infrastructure and limit vulnerabilities threatening the FBI mission.

Asset Management: Industry reports 60% of security breaches in 2020 involved unpatched vulnerabilities; such breaches constitute a high risk to the FBI's cybersecurity posture. The FBI must use reporting and server ownership information to identify, communicate, and escalate non-compliance for remediation. The FBI assesses, based on its current cybersecurity posture, it must invest additional resources in efforts to combat potential breaches and vulnerabilities. The FBI maintains over 500 systems with immeasurable interconnections and interdependencies. These systems are primarily supported by contractors (85%) sourced from over 20 decentralized contract vehicles. The attrition rate for contractors is high, as they possess highly marketable skillsets. As a result, the FBI's IT security workforce is understaffed to sufficiently protect the FBI's information systems and keep up with information system security assessment and authorization process.

Security & Compliance: At present, there are over 300 FBI IT systems that require security assessments. The FBI has approximately 140 cloud services that will require a security review to ensure they are configured in accordance with cloud service providers best security practices. The current resource level does not allow the FBI to provide the necessary review and oversight. Without an automated means of validating these settings/services, the FBI risks possible data compromise as it migrates IT systems into cloud environments.

Agility: With the number of cyberattacks against the FBI increasing every year, sophisticated identification and prevention are required to extricate threats from benign network activity. Cyber threats constantly evolve, and the FBI's cybersecurity defense must evolve with it. The FBI must keep up with the new technologies posing a threat to its IT infrastructure and deploy new defensive tools to stay current with innovation and technological advances in the cyber environment.

Cybersecurity Posture: 6 positions and $32,990,000 ($32,287,000 non-personnel)

The FBI requests resources to protect IT assets vulnerable to cyberattacks and insider threats. The cyber defense landscape is constantly changing, and new technologies and techniques are constantly emerging. Better systems are required to address the current gaps in monitoring, analysis, and system logging. Personnel are requested to perform day-to-day monitoring, development, and compliance procedures. Funding is also requested to cover sustainment costs from initial investments into cybersecurity modernization efforts. The requested resources will ensure the FBI is current with security technologies and practices to protect its systems and data.

IT Asset Monitoring: 6 positions and $3,068,000 ($2,365,000 non-personnel)

The FBI requests 6 positions and $3,068,000 ($2,365,000 non-personnel) to address foundational cybersecurity monitoring capabilities for the FBI's IT infrastructure, as well as the needed personnel to effectively and efficiently monitor FBI assets for cyberattacks. It will also provide technologies for the FBI's cyber defenders to prevent and respond to attacks against the FBI's infrastructure. Specifically, the requested resources will be used to enhance expanded monitoring of FBI IT assets and to deploy technologies to support increased visibility into the FBI's existing IT assets and emerging technologies, such as cloud and mobility platforms.

Centralized Logging and Analytics: $24,480,000 (all non-personnel)

As the volume and speed of information increases, the FBI must make major investments to protect its networks, systems, and data sets. Adversaries persistently attempt to infiltrate the FBI's networks and systems, threatening the integrity of investigations and prosecutions and undermining the capabilities of the Intelligence Community (IC).

The FBI requests funding to continue to maintain current and build out future advanced cybersecurity capabilities, currently being developed as a part of the Enterprise Centralized Logging solution (ECLS). Initial stand-up investments in the new logging system were made through the one-time funding associated with the Information Technology Modernization Initiative (ITMI). These efforts will enable the FBI to better identify, respond to, and mitigate a wide range of sophisticated malicious cyber and insider threats.

Expanding this capability requires the technical design of transport, ingest, and storage of a wide range of FBI enterprise on-premises and off-premises machine log data (at the enterprise, machine, and application levels). This centralized data repository will be overlaid with advanced analytics which leverage the FBI's current enterprise license with a machine data analytical solution. These capabilities require additional hardware, cloud-based compute and storage, automation software and support services. Core functions include the following: Assessing existing logging practices across the FBI enterprise; evaluating network transport and storage options for the centralized logging environment; establishing standards, policy, and security requirements to implement centralized logging; and designing and deploying cybersecurity-focused data analytics and machine learning tools for various FBI programs (e.g., network security, insider threat detection, system health and performance).

The FBI requests $24,480,000 to sustain the requirements for the full scope of cybersecurity projects related to the enterprise ITMI. Specifically, funding will be allocated for sustainment of the targeted projects, listed below:

COOP for ESOC Monitoring Capabilities	$2,200,000
ECLS Hardware Expansion	$8,256,000
Trusted Internet Connection Monitoring	$2,796,000
Network Hardware Modernization	$3,870,000
Threat Analysis Platform Modernization	$4,886,000
Tech Refresh for ESOC Enclaves	$2,472,000

Modernizing cybersecurity logging will allow for the most comprehensive monitoring and protection of FBI data and will advance the FBI's cybersecurity posture. To ensure new and persistent threats can be mitigated in a timely manner, the FBI must expand the enterprise centralized logging solution as the organization grows. Further, enhancing the monitoring solutions that provide the ESOC with up-to-date threat detection systems will augment the centralized logging capabilities.

Endpoint Detection and Response (EDR) and Security Operations Center SOC Tool Modernization: $3,400,000 (all non-personnel)

The FBI requests $3,400,000 to deploy industry standard software tools and personnel resources to address the cybersecurity initiatives listed below. This initiative consists of approximately 2-3 contractors at a total annual labor cost of $400,000 and software tools for $3,000,000. Implementing this capability supports the processing of a substantially larger amount of data being generated by the growing centralized logging capability.

Cybersecurity Initiatives related to EDR and SOC Tool Modernization include:

Mobile Internet Traffic Monitoring	Provides ability to monitor network traffic to the internet from Bureau-issued phones for compromise or potential compromise.
Mobile Application Monitoring	Provides ability to monitor Bureau phones to ensure applications function in a secure fashion and to aid analysis of a compromise.
Mobile Network Traffic	Provides ability to monitor mobile network traffic from Bureau-issued phones for compromise or potential compromise.
Research on Advanced Persistent Threats	Provides ability to search repositories of data on suspicious files submitted outside the FBI to research tactics and techniques employed. Current process is performed manually on an ad-hoc basis.
Research Internet-Related Threats	Provides ability to conduct enterprise-level domain and DNS-based threat intelligence research.
Secure File Sharing	Provides ability to share files securely inside and outside the FBI. Current process is performed manually and ad-hoc.

Data Spills Mitigation	Provides ability to clean and remove data spills in an approved manner to permanently erase spilled data. Current process is performed manually on an ad-hoc basis.
Cloud Log Collections and Long-Term Storage	Allows for collection point/storage and longer-term storage for intrusion events in the cloud.
OIG-Required Mobile eDiscovery Operations	Provides ability to collect call records and text/SMS messages from Bureau-issued mobile devices. Currently being performed, but not at the pace required.

Operations and Forensic Analysis: $2,042,000 (all non-personnel)

The FBI requests $2,042,000 to enhance its incident response and digital forensics capabilities. This will allow the FBI to better respond to compromises of USG systems, process and analyze investigative data, and forensically analyze the FBI's mobile activity data and FBI data stored in the cloud. This request will provide substantial improvements to the FBI's cybersecurity posture and agility. Specifically, funding will be allocated to hire approximately 10 contractors to enhance digital forensic and incident response capabilities.

Once a major incident has been identified on an FBI network and/or system, an enterprise response team will serve two primary functions: 1) respond to and mitigate the incident, and 2) generate leads for the appropriate FBI investigative division (primarily, Cyber Division (CyD) and the Insider Threat Office (InTO)). This team will ensure major incidents are fully remediated and any evidence is retained and forwarded for investigation (as appropriate).

Cybersecurity Initiatives related Operations and Forensic Analysis include:

Forensic Analysis	Provides ability to perform forensically-sound analysis of network traffic to determine/confirm incidents and analyze potentially compromised networked devices (e.g., workstations, servers, routers).
Mobile Forensic Analysis	Provides ability to recover digital evidence or data from a mobile device under forensically sound conditions.
Malware Reverse Engineering	Provides ability to analyze source code of a suspicious file to identify a threat and its designed effect.

ESOC is required to protect FBI Information Systems (IS) by monitoring for, detecting, responding to, mitigating, and reporting on cybersecurity threats that could potentially compromise FBI IS, data, and personnel. Cybersecurity threats are continually evolving and growing in number, and tools are needed to ensure FBI systems are protected from external, internal, and foreign threats. The enhancement will allow ESOC to address mission-critical gaps to protect FBI systems and data. This request will provide substantial improvements to the FBI's cybersecurity program.

Cybersecurity Threat Assessment Program - Advanced Security Assessment Team: 3 positions (1 Special Agent) and $3,958,000 ($3,399,000 non-personnel)

Cybersecurity technical operations are designed to proactively address enterprise vulnerability and asset discovery requirements while having the flexibility to conduct advanced security assessments based on the realities of continuously evolving adversary threats, tactics, and techniques. The Cybersecurity Threat Assessment program objectives are aligned to support the FBI Director's Digital Capability and Risk Priority Initiative and focus on transforming the FBI's approach to security by ensuring systems are securely built, the enterprise is continuously monitored for insider threats and external intrusions, and FBI stakeholders are prepared to respond to cyber threats.

The FBI requests 2 Information Technology Specialist (ITS) positions, 1 Special Agent position and $3,958,000 ($3,399,000 non-personnel) to continuously assess and enhance the security posture of the FBI through threat-driven, cybersecurity technical operations based on adversarial tools, techniques, and procedures (TTP) that are realistic, relevant, and identify true risk to the FBI mission.

The primary purpose of the Advanced Security Assessment Team (Blue and Red) is to proactively assess the overall information security and cybersecurity management of an organization or system beyond vulnerability scans. The Blue Team assessments focus on a collaborative approach intended to determine the overall effectiveness of the personnel and processes used to secure information technology assets, while the Red Team operations focus on an approach based on employing potential tools, techniques, and processes used by adversaries to identify the risks to the organization's most mission-critical and mission-essential elements. This request includes $1,123,000 for advanced cybersecurity software and the associated hardware to run these tools against FBI systems. Additionally, $2,276,000 is requested for 9-11 contractors to expand the program's reach across the FBI, increasing the number of operations they can perform.

Collectively, the above team will enable the FBI to continuously assess and enhance the enterprise security posture through threat-driven cybersecurity technical operations and enterprise security services that are realistic, relevant, and identify true risk to FBI systems and information.

With this enhancement to the cybersecurity program, the FBI will gain an unvarnished view of the current state of its cybersecurity, increasing its understanding of cyber risk and allowing for the prioritization of mitigation efforts, while also validating the effectiveness of current security

controls. Investing in transformative technologies will allow the FBI to identify high-risk vulnerabilities and gaps in security which may otherwise go unidentified using less advanced methods. Further, the FBI will be able to proactively identify a compromise from insider threats or external adversaries in coordination with the ESOC and the Insider Threat Office (InTO).

Impact on Performance

With the necessary enhancements to address engineering requirements for the cybersecurity assets the FBI maintains, the FBI will improve its monitoring and analysis deployed to maintain and protect sensitive data on all FBI asset inventory. Further, for the FBI to adhere to the federally mandated FISMA security requirements for its assets, it must automate and standardize the full lifecycle development process for systems and applications. This must be accomplished by migrating towards a mature Security Development Operations (SecDevOPS) model and employing state of the art tools, such as Information Resource Management (IRM) and Mobile Application Security Vetting, to support the Security Assessment and Authorization process.

The FBI must supplement the compliance and engineering requirements with an adequate and dedicated IT workforce to address the maintenance, compliance, and developmental needs associated with the variety and uniqueness of its many assets. Through integration with programs across the FBI, the addition of government IS personnel will enhance general security awareness, increase the ability to develop a structured career path, maintain consistent hiring practices, and implement effective enterprise program management. This will substantively contribute to the FBI's ability to effectively monitor systems for adversarial exploits, strengthening security defenses, and mitigating system vulnerabilities.

Funding

1. **Base Funding**

FY 2021 Enacted				FY 2022 President's Budget				FY 2023 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
125	4	107	$63,017	144	4	108	$85,959	144	3	120	$87,137

2. **Personnel Increase Cost Summary**

Type of Position/Series	Positions Requested	Annual Costs per Position ($000)			FY 2023 Request ($000)	Annualizations ($000)	
		1st Year Adjusted Cost	2nd Year Adjusted Cost	3rd Year Full Cost (Modular)		FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Special Agent, Field	1	$328	$276	$397	$328	($52)	$122
Information Technology	4	$115	$219	$254	$460	$415	$144
Professional Support	4	$118	$158	$227	$473	$162	$280
Total Personnel	**9**	**$562**	**$653**	**$878**	**$1,262**	**$525**	**$546**

3. **Non-Personnel Increase/Reduction Cost Summary**

Non-Personnel Item	FY 2023 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
IT Services - IT Development, Modernization, and Enhancement (DME) Services	$3,399	N/A	N/A	($671)	$0
IT Software - Summary	$2,365	N/A	N/A	$0	$0
IT Software - (Non-ELAs)	$3,400	N/A	N/A	($100)	$0
IT Hardware - (Non-ELAs)	$26,522	N/A	N/A	($15,276)	$0
Total Non-Personnel	**$35,686**	**N/A**	**N/A**	**($16,047)**	**$0**

4. **Justification for Non-Personnel Annualizations**

FBI data, including national security data, is increasingly vulnerable to external cyber and insider threat attacks given the ever-changing technological landscape, including the emergence of the cloud and the increase in mobile platforms. The FBI's cybersecurity mission has historically been critically underfunded and understaffed. This enhancement allows the FBI to build some of the baseline capabilities needed to protect FBI data and systems in addition to building towards a zero-trust architecture and increased cybersecurity capabilities for

commercial cloud service providers which are federally mandated through the Executive Order on Improving the Nation's Cybersecurity. The need for these capabilities will not be reduced, and may increase, over the coming years. They, therefore, will require continued funding for software, tools, and personnel to manage this mission. Additionally, in order to run the latest tools and software, the FBI will need to continue to refresh its hardware for this mission on a regular cycle.

5. Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Current Services	144	3	120	$21,910	$65,227	$87,137	N/A	N/A
Increases	9	1	5	$1,262	$35,686	$36,948	($15,522)	$546
Grand Total	**153**	**4**	**125**	**$23,172**	**$100,913**	**$124,085**	**($15,522)**	**$546**

Item Name: **Data Analytics and Technical Tools**

Budget Decision Units: All

Organizational Programs: Office of the Chief Information Officer

Program Increase: Positions 0 Agt 0 FTE 0 Dollars $16,928,000 (all non-personnel)

Description of Item

The FBI requests $16,928,000 (all non-personnel) to enhance its technical infrastructure. The ability to process and exploit extremely large and complex data is critical for investigations. The FBI must invest in its enterprise infrastructure to effectively and efficiently access, manage, transport, protect, and evaluate information to ensure mission-essential intelligence is reaching FBI investigators and key partners with sufficient time to comprehensively and strategically address threats.

Justification

As the volume, speed, and complexity of computing technologies continue to evolve, so too must the infrastructure that supports the advanced systems and applications the FBI deploys. The need to invest in network infrastructure has never been more important to support law enforcement activities.

The FBI's investigative and intelligence systems have experienced dramatic increases in quantity and sources of data. With the advent of the Internet-of-Things (IoT) and new technologies for collection, the sources of investigative data are ubiquitous. There was a 33% increase in storage for the Data Warehouse System (DWS) alone in the three months following the Capitol Riot of January 6, 2021. The volumes of data consumed by algorithmic approaches exacerbates the impact of high resource consumption. However, this consumption is necessary to achieve investigative and intelligence results.

Investigation and analysis are increasingly conducted at the petabyte (PB) scale. To modernize investigative data analytics, the FBI requires networks that can transport bulk data and reduce reliance on stand-alone, ad hoc systems which may lack adequate security protections. In FY 2019, the FBI requested to use $225 million to create the enterprise IT Modernization Initiative (ITMI), which includes investments in network infrastructure, core data management for advanced analytics, and cybersecurity. This initiative primarily includes one-time investments that will make significant progress in reducing current IT limitations hindering operational capacity and presenting substantial security risks. While this funding will address these shortcomings and lead to tremendous advancement in IT support to operational capabilities, reduction in security risks, and improvement to the overall user experiences, further resources are required to support the operation and maintenance (O&M) of these investments.

Network Modernization – $16,928,000 (all non-personnel)

The FBI requests $16,928,000 (all non-personnel) to continue to improve reliability, security, and bandwidth across its network infrastructure, as well as provide operations and maintenance support. These needs were previously supported as part of ITMI. The FBI has been working to advance network infrastructure for several years and has made tremendous progress. However, to keep pace with the rapid evolution and distribution of innovative technologies across the world, the FBI requires the continued enhancement of enterprise technical solutions, as well as the foundational IT infrastructure supporting operational technology and mission requirements.

Outlined below are the O&M costs associated with ITMI projects.

Enterprise Networks Modernization (NERI) Continuation and Ongoing Support ($12,007,000)

The NERI ecosystem facilitates the consolidation of common classification networks, moving from a many-to-many construct to a many-to-one philosophy. Consolidating disparate networks means a smaller, more efficient infrastructure. It enables the creation of a more straightforward architecture easier to control, maintain, and secure. The consolidation also enables new features for network automation and central management of network components. NERI is an ongoing multi-year initiative, where this requested funding will be used to procure additional hardware and software licensing for the continued deployment. This will also address technology gaps between the consolidated enterprise cross domain system and other FBI cross domain systems targeted for consolidation. Overall, this request will continue the deployment of out-year operational support for the NERI eco-system.

Network Security Vulnerabilities Hardware / Software Mitigation ($2,783,000)

The FBI is working to identify critical network gear replacements to address security findings and reduce security vulnerabilities for network devices which cannot be patched and are no longer under maintenance support due to age.

The FBI still uses a multitude of network devices put into service between 2006 and 2013 which are long past vendor end of support (EoS) and can no longer receive critical security and/or software patches to fix bugs and address security vulnerability findings. These unpatched and unsecure devices represent a significant risk to the FBI's IT security posture. In addition, these legacy EoS devices are not covered by any current maintenance contracts and routinely fail, causing prolonged network outages impacting FBI personnel. This is an annually compounding issue requiring ongoing funding.

Enterprise Cross Domain Service Consolidation ($2,138,000)

Modernization investments have allowed the FBI to upgrade the existing enterprise cross domain systems and begin consolidating a number of systems into a centrally managed configuration more reliable and secure. Additional funding is needed to maintain the critical operation of data ingestion and transfer across FBI enclaves and with other government agencies and IC components.

Impact on Performance

With the information technology landscape in constant evolution, it is imperative the FBI modernize its IT infrastructure to leverage new and smarter technologies. This enhancement would better position the FBI to stay ahead of the threat by modernizing key components in the FBI's network infrastructure to increase reliability and security by remediating known vulnerabilities, improving cross domain communication, and building the foundation future network consolidation efforts will leverage.

Funding

1. Base Funding

FY 2021 Enacted				FY 2022 President's Budget				FY 2023 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
0	0	0	$23,140	0	0	0	$39,398	0	0	0	$42,018

2. Personnel Increase Cost Summary

Type of Position/Series	Positions Requested	Annual Costs per Position ($000)			FY 2023 Request ($000)	Annualizations ($000)	
		1st Year Adjusted Cost	2nd Year Adjusted Cost	3rd Year Full Cost (Modular)		FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
N/A	0	$0	$0	$0	$0	$0	$0
Total Personnel	**0**	**$0**	**$0**	**$0**	**$0**	**$0**	**$0**

3. Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	FY 2023 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
IT-Hardware	$16,928	N/A	N/A	($3,947)	$0
Total Non-Personnel	**$16,928**	**N/A**	**N/A**	**($3,947)**	**$0**

4. Justification for Non-Personnel Annualizations

IT hardware recurral costs are being requested to support ongoing maintenance of network hardware buys.

5. Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Current Services	0	0	0	$0	$42,018	$42,018	N/A	N/A
Increases	0	0	0	$0	$16,928	$16,298	($3,947)	$0
Grand Total	**0**	**0**	**0**	**$0**	**$58,946**	**$58,946**	**($3,947)**	**$0**

Item Name: **UTS**

Budget Decision Unit(s): All

Organizational Program: Critical Incident Response, Directorate of Intelligence

Program Increase: Positions 8 Agt 0 FTE 4 Dollars $8,092,000 ($6,469,000 non-personnel

Description of Item

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

Item Name: **Body Worn Cameras**

Budget Decision Unit(s): All

Organizational Programs: Criminal Investigative, Information Technology, Operational Technology

Program Increase: Positions 102 Agt 1 Atty 5 FTE 51 Dollars $27,351,000 ($9,719,000 non-personnel)

Description of Item

The FBI requests 102 positions (1 Special Agent) and $27,351,000 ($9,719,000 non-personnel) to develop and launch a Body Worn Camera (BWC) program for FBI Special Agents across all FBI field offices. Specifically, the requested resources will be used for personnel and contracting costs to develop the technical infrastructure required for the BWC program and storage of footage; personnel at Headquarters and field offices to support legal and technical efforts; and procurement of hardware, software, and other BWC-related equipment.

Justification

DOJ announced in October 2020 the Department "will permit state, local, territorial, and tribal Task Force Officers (TFO) to use BWCs on Federal task forces around the nation. DOJ's policy will permit Federally-deputized officers to activate a body worn camera while serving arrest warrants, or during other planned arrest operations, and during the execution of search warrants."

Following the implementation of DOJ's TFO policy in October 2020, DOJ launched a working group with its law enforcement agencies Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), Drug Enforcement Administration (DEA), FBI, and U.S. Marshals Service (USMS) to explore the requirements for a BWC program for Federal Special Agents. In March 2021, DOJ and the BWC Working Group determined the need for phased implementation by participating agencies; as such, the FBI anticipates launching the initial BWC program in five field offices (FOs) during FY 2022 and expanding to additional FOs during FY 2023. To expand the BWC program, the FBI requires resources to ensure successful implementation across FBI field offices.

The FBI, in conjunction with DOJ and other component agencies, thoroughly evaluated the policy, technical, and legal requirements of a BWC program for Special Agents and identified key critical requirements including technical development and support, legal support, equipment, storage of footage, and training, as detailed below.

- **HQ Technical Infrastructure Development:** The FBI requests $3,320,000 for software and contract labor support for technical infrastructure development. This request is informed by a comparative analysis conducted by the FBI which determined it would be more effective for the FBI to develop an in-house storage solution rather than contract

with a third-party. Specifically, the FBI will utilize funding for software developers, Information System Security Officers (ISSOs), system administrators, and forensic audio/visual personnel to manage development and application integration into FBI enterprise systems and redaction services. Additionally, the procured software will accommodate the tracking of service tickets, audio/video enhancing software, compliance, cybersecurity, and appropriate licenses.

- **HQ FOIA, Legal, and Technical Support:** The FBI anticipates an increase in requests for captured video via the Freedom of Information Act (FOIA) and discovery attributed to the BWC program. Additional personnel are required to manage the increased volume of requests. The FBI requests 46 positions and $6,797,000 (all personnel) to address FBI HQ personnel requirements. Specifically, the FBI requests one (1) Special Agent, 5 Attorneys (Atty), 4 Engineers, 10 Information Technology Specialists (ITS), and 26 Professional Support (PS) employees.

- **Field Office Technical and Legal Support:** The FBI anticipates an increased burden on field personnel to address the technical and legal challenges associated with the implementation of the BWC program. The FBI requests $10,835,000 to fund an additional 28 technical support positions and 28 legal support positions throughout the field. The requested positions will provide the field with the resources needed to address these challenges and ensure proper use of BWCs during operations, as determined by DOJ and FBI policy.

- **BWC Cameras:** The FBI requests $2,357,000 for the purchase of approximately 3,000 cameras and associated equipment to begin implementation at all 56 field offices.

- **Field Bandwidth Enhancement:** The FBI has identified approximately 309 sites that will be utilized for the BWC program where current bandwidth capacity is lower than the required 30 MB. The FBI requests $2,964,000 to increase bandwidth to the required 30 MB for each of these sites.

- **Video Processing/Ingest:** The FBI requests $578,000 to fund cloud storage costs associated with video ingest and processing prior to transport into FBI permanent storage. Cloud storage costs are divided into four elements to include hot storage, archive storage, computing, and bandwidth.

- **Training:** The FBI requests $500,000 to fund travel and training during the rollout efforts of the BWC program. The FBI intends to use the requested funding to facilitate the development of training material to be included in the curriculum for new Special Agents, as well as conducting on-site training to current FBI personnel.

Impact on Performance

BWCs are critical tools that enhance law enforcement transparency and accountability, and thereby assist in building and maintaining public trust. In addition, BWCs can provide protection for officers from being falsely accused of wrongdoing, thereby potentially reducing agency

liability. In the past decade, BWC use has become commonplace in large law enforcement organizations throughout the U.S. According to a study by DOJ's Office of Justice Programs (OJP), as of 2016, about 80% of non-federal law enforcement agencies with at least 500 full-time officers had acquired BWCs. Additionally, other federal entities have implemented BWC programs, including select agencies within the Department of the Interior (DOI) and Customs and Border Patrol (CBP).

The FBI has always been committed to transparency and accountability. BWC technology would enable the FBI to further this commitment to the public. With these resources, the FBI will be able to participate in the Department-wide BWC Program and launch a BWC Program for federal Special Agents across all 56 FOs. It is imperative the FBI receive the full enhancement request to successfully operate the FBI's BWC Program in accordance with existing and future policy, guidance, and legislative requirements.

Funding

1. **Base Funding**

FY 2021 Enacted				FY 2022 President's Budget				FY 2023 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
0	0	0	$0	0	0	0	$0	0	0	0	$0

2. **Personnel Increase Cost Summary**

Type of Position/Series	Positions Requested	Annual Costs per Position ($000)			FY 2023 Request ($000)	Annualizations ($000)	
		1st Year Adjusted Cost	2nd Year Adjusted Cost	3rd Year Full Cost (Modular)		FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Attorney	5	$183	$279	$288	$915	$484	$45
Electronic Technician	28	$269	$179	$246	$7,522	($2,491)	$1,904
Engineer	4	$332	$281	$305	$1,327	($200)	$96
Information Technology	10	$115	$219	$254	$1,150	$1,037	$360
Professional Support	54	$118	$158	$227	$6,390	$2,193	$3,780
Special Agent, Field	1	$328	$276	$397	$328	($52)	$122
Total Personnel	**102**	**$1,345**	**$1,391**	**$1,176**	**$17,632**	**$970**	**$6,307**

3. **Non-Personnel Increase/Reduction Cost Summary**

Non-Personnel Item	FY 2023 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
IT Hardware – Summary	$2,964	N/A	N/A	$0	$0
IT Services – IT Development, Modernization, and Enhancement (DME) Services	$6,177	N/A	N/A	$0	$0
N/AN/AIT Software Summary	$578	N/A	N/A	$0	$0
Total Non-Personnel	**$9,719**	**N/A**	**N/A**	**$0**	**$0**

4. **Justification for Non-Personnel Annualizations**

The FBI expects an annual recurring cost of $9,719,000 in FY 2024 and FY 2025. This cost will fund the annual expense of maintaining upgraded bandwidth, training, purchase of equipment, development services associated with contractor labor support, and maintenance of infrastructure for the licensed software for the BWC program.

5. **Total Request for this Item**

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Current Services	0	0	0	$0	$0	$0	N/A	N/A
Increases	102	1	51	$17,632	$9,719	$27,351	$970	$6,307
Grand Total	**102**	**1**	**51**	**$17,632**	**$9,719**	**$27,351**	**$970**	**$6,307**

Item Name: **21st Century Operations and Maintenance (O&M)**

Budget Decision Unit: All

Organizational Programs: Facilities, Human Resources, Information Technology, Security

Program Increase: Positions 47 Agt 0 FTE 24 Dollars $39,420,000 ($31,606,000 non-personnel)

Description of Item

The FBI requests $39,420,000 ($31,606,000 non-personnel) and 47 positions for the operations and maintenance (O&M) required to support the substantial personnel, technological, structural, and security requirements of the FBI's expanding presence at Redstone Arsenal (RSA) in Huntsville, Alabama.

Specifically, the FBI will utilize the requested resources to enhance the following:

- **RSA Facilities O&M and Strategic Realignment:** $39,420,000 ($31,606,000 non-personnel) and 47 positions to operate completed buildings and oversee the facilities under construction at RSA.

The FBI's 21st Century Facilities initiative is focused on ensuring the FBI workforce has access to modern facilities with the space, technical bandwidth, and power necessary to achieve the organization's current and future law enforcement and intelligence missions. Operations and maintenance resources are crucial to properly maintaining the campus and technological infrastructure critical to operations, as well as to supporting the growing staff relocating to RSA. The technical demands placed on today's special agents, IAs, and other FBI staff at RSA cannot be satisfied if the organization's space, power, and overall physical and support infrastructure on RSA is insufficient. Proper O&M must be at the forefront of the planning and must not be an afterthought.

Justification

Redstone Arsenal

The Army has permitted and/or designated over 1,000 acres of land at RSA for use by the FBI. The FBI's plan for RSA focuses on improving operational support, technology, training, and research and development capabilities and capacities. The FBI RSA plan was prepared in collaboration with the RSA Garrison Directorate of Public Works and is complementary to the Arsenal's long-range goal of becoming a key U.S. Government research and development, test and evaluation, and technology hub.

Photographs and Renderings of the FBI's North Campus (Fall 2021):

The FBI's plans for constructing new facilities and realigning functions and staff to RSA include three key opportunities:

- Creating a center of excellence for FBI explosives and counter-improvised explosive device (IED) programs and activities;
- Leveraging Huntsville-area technology, science, and engineering interests to create an FBI technology hub to support investigations and operations; and
- Providing additional advanced and specialized training capabilities to address requirements which cannot be fulfilled at the FBI Academy campus.

RSA and the Huntsville Metropolitan Area (HMA) offer a population with the skills required to meet evolving mission requirements, particularly expertise in the science and technology fields. RSA is also home to several Army and DoD tenants in addition to several civilian federal agencies with workforce requirements similar to those of the FBI. Additionally, over 400 private sector firms operating in the area are approved by the DoD to perform classified work. Many of the FBI's current private sector partners already have a local presence in Huntsville, and the area is home to several strong science, technology, engineering, and math-focused universities and colleges. The location also provides opportunities for enterprise support services, such as procurement, human resources, financial management, and security that do not need to be performed in the NCR, to be co-located and centralized in a more cost-efficient manner at RSA.

In FY 2023, two key strategic realignment buildings at RSA, Operations Building 1 (OPS 1) and Technology Building 1 (TECH 1), will be fully operational and in need of a reliable funding source to operate and maintain. The OPS 1 complex will house approximately 1,300 personnel from multiple FBI divisions and includes an approximately 307,000-square-foot office building, a vehicle parking deck, a central utility plant, and a multi-functional building. TECH 1 will house approximately 330 personnel in an approximately 87,000-square-foot tech-focused building. The resources requested here will allow the FBI to properly operate and maintain its

Redstone footprint, and support the related personnel, through the opening of these two key facilities on the North Campus.

Expected to be completed in FY 2024, the Innovation Center, an approximately 250,000 square-foot office building and central utility plant, will come online as a training center of excellence for the FBI. The Innovation Center is a state-of-the-art facility dedicated to training, cyber threat intelligence, data analytics, and combatting the rapidly changing 21st century threats. The facility will house approximately 330 permanent personnel plus an additional 300 students per week for training. The building will also have a 22,000-square-foot indoor smart city (kinetic cyber range) and a virtual and augmented reality classroom with distance learning management systems. By FY 2024, the FBI will be responsible for maintaining a footprint of over 1,000,000 square feet across its entire RSA portfolio.

The FBI will continue to expand on RSA with future technology capabilities brought to life through additional technology buildings anticipated to come online in 2026. The additional buildings, complementing each other with forward-leaning amenities and STEM personnel, will result in a new Technology District. The Technology District will house employees who will enable the movement of data via state-of-the-art networks and focus on collecting and cleaning data, all while providing technical expertise and support to the FBI and its partners. The Technology District will also be home to the FBI's state-of-the-art 30,000 square foot Network Operations Center.

Additional O&M support for facilities coming online in FY 2024 and beyond, including the Technology District and South Campus and Smart City venues, will be requested when necessary.

RSA Infrastructure O&M: 47 positions and $39,420,000 ($31,606,000 non-personnel)

- The FBI requests $3,356,000 to support ongoing O&M of the RSA campus that operates 24/7/365. Services include custodial, grounds maintenance, and predictive, corrective, and preventive maintenance service requests. An additional $1,616,000 is being requested for IT O&M to provide the commercial network circuits that connect RSA to FBI data centers and other external networks. The funding will support refresh of equipment which has been at RSA for years supporting new and transitioning personnel as the campus continues to grow. Also, the FBI requests $3,798,000 to cover energy and utilities for the FBI footprint at RSA and to maintain mission ready status.

- The FBI requests $12,884,000 to support contractor activities around the central utility plant; electronics technicians who install and maintain physical security devices such as door keypads and cameras along with wiring for computer networks; and logistics professionals who will move mail, supplies, and other goods around RSA. Further, the FBI requests $4,484,000 to provide support for armed guards at access control points onto the FBI campus. The funding will support staffing the FBI visitor center that controls access to the Redstone installation and the operations center which controls access to the FBI's North Campus. The FBI also requires $5,468,000 for contract personnel to support the complex and numerous IT systems deployed around the

campus. Highly skilled specialists will be needed to provide hands-on support of 165-plus racks of IT equipment spread across the North Campus, provide telephonic and hands-on support for desktops, printers, telecommunications, and mobility devices such as laptops and phones, provide engineering services as the FBI rolls out wired and wireless infrastructure, and to ensure the proper operation of 200-plus audio/visual (A/V) systems in training rooms, conference rooms, and auditoriums.

As additional buildings come online and FBI employees and contractors move to RSA, the FBI must have the personnel on the ground to support the new arrivals. The following are the FBI's FY 2023 personnel requirements for RSA support:

- Eight (8) Electronics Technicians will ensure all buildings meet necessary security and technical requirements. The increasing number of facilities has led to expanding security systems which must be supported. Electronics Technicians will also help maintain the IT infrastructure of the campus and support IT network needs.
- Five (5) Engineers will ensure all buildings receive adequate utility services through the central utility plant infrastructure to ensure RSA is always operating at mission ready capacity. The increasing number of buildings and associated central utility plant necessitates trained professionals to monitor and maintain the substantial investment and ensure responsible energy usage.
- Nine (9) Facilities and Logistics Professionals will handle all manner of tasks to include managing mail operations, warehousing, supply chain, and vehicle fleet operations.
- Three (3) Environmental Safety and Occupational Health Professionals will ensure compliance with Occupational Safety and Health Administration (OSHA), Environmental Protection Agency (EPA), and Alabama environmental standards along with adherence to OSHA and FBI policies of workplace safety.
- Five (5) Management and Program Analysts will perform duties such as financial analysis and capital planning, serving as contracting officer representatives with contract oversight responsibilities for contracts that provide services such as groundskeeping, custodial, cafeteria, building maintenance, and other services, provide project management support for additions, moves, and changes to workspaces and furniture, and serve as subject matter experts for their areas of responsibility.
- Seven (7) Information Technology Specialists (ITSs) and Management and Program Analysts (MAPAs) will support the 21st century hardware and technology across RSA. The ITSs will ensure network integrity is maintained as new technology is integrated as more buildings and systems are brought online. The MAPAs will staff the data center, run RSA desktop support, telecommunications management, and network engineering.
- Six (6) Physical Security Professionals will be needed as the FBI's footprint grows in both personnel and square footage. Their responsibilities will include badging, visitor access requests, clearance requests, access control, and construction security.
- Three (3) Occupational Health Nurses will perform the services and assessments and one (1) Program Analyst will perform clinic support functions such as appointment scheduling and patient check-ins. Medical Operations and Readiness supports the FBI mission through activities such as fitness for duty assessments, OSHA medical services, and foreign travel reviews.

Impact on Performance

The requested investments in the 21st Century Facilities initiative are a key part of the multi-year plan to enable the FBI to meet the demands of its unique mission at the intersection of law enforcement and national security. While the FBI has received construction appropriations to expand its RSA footprint, it requires funding to appropriately operate and maintain the growing campus. These resources will ensure that the significant investments made at RSA can be sustained and that the necessary support infrastructure and personnel exist to meet FBI mission requirements at Huntsville.

Funding

1. Base Funding

FY 2021 Enacted				FY 2022 President's Budget				FY 2023 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
67	1	63	$9,060	67	1	66	$10,001	67	1	66	$10,366

2. Personnel Increase Cost Summary

Type of Position/Series	Positions Requested	Annual Costs per Position ($000)			FY 2023 Request ($000)	Annualizations ($000)	
		1st Year Adjusted Cost	2nd Year Adjusted Cost	3rd Year Full Cost (Modular)		FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Electronic Technician	8	$269	$179	$246	$2,149	($712)	$554
Engineer	5	$332	$281	$305	$1,659	($250)	$120
Information Technology	5	$115	$219	$254	$575	$518	$180
Professional Support	29	$118	$158	$227	$3,431	$1,178	$2,030
Total Personnel	**47**	**$834**	**$836**	**$1,031**	**$7,815**	**$734**	**$2,874**

3. Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	FY 2023 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Contract-Mgmt Support	$20,038	N/A	N/A	$0	$0
Guard Services	$4,485	N/A	N/A	$0	$0
IT- Services	$6,399	N/A	N/A	$0	$0
IT - Software	$684	N/A	N/A	$0	$0
Total Non-Personnel	**$31,606**	**N/A**	**N/A**	**$0**	**$0**

4. Justification for Non-Personnel Annualizations

Annualizations are requested pursuant to the FBI's outyear mission requirements. As this enhancement request describes, this funding is needed to continue to support and maintain the expanding FBI facilities and operations at Redstone Arsenal. The O&M requirements for Redstone will only continue to grow in the out-years as additional facilities are constructed and brought online.

5. Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Current Services	67	1	66	$10,366	$0	$10,366	N/A	N/A
Increases	47	0	24	$7,815	$31,606	$39,421	$734	$2,874
Grand Total	**114**	**1**	**90**	**$18,181**	**$31,606**	**$49,787**	**$734**	**$2,874**

Item Name: **McGirt**

Budget Decision Unit(s): All

Organizational Programs: Criminal

Program Increase: Positions 76 Agt 45 FTE 38 Dollars $22,513,000 ($3,708,000 non-personnel)

Description of Item

The FBI requests $22,513,000 ($3,708,000 non-personnel) to effectively address the increased operational need in the state of Oklahoma following the Supreme Court decision in *McGirt v. Oklahoma.* This ruling significantly expanded federal jurisdiction for crimes committed on the tribal lands of six Native American reservations in Oklahoma. The requested resources will be used to enhance the FBI's capacity to address the significantly increased number of investigations which are now under FBI jurisdiction in Oklahoma.

Justification

As a result of the U.S. Supreme Court's McGirt decision, the FBI's Oklahoma City field office assumed responsibility as the investigating agency in a large number of cases within the territorial boundaries of the Muscogee (Creek) Nation. The FBI is doing so in cooperation with tribal, state, local and federal law enforcement partners. On July 9, 2020, the decision under *McGirt v. Oklahoma* ruled that land reserved for the Muscogee (Creek) Nation since the 19th century remains a Native American reservation. This resulted in the FBI becoming a responsible law enforcement agency for committed offenses, including Major and General Crimes Acts violations when a Native American is involved. This increased the FBI's role in investigating specific criminal matters within the territorial boundaries of the Muscogee (Creek) Nation.

Subsequent decisions from the Oklahoma Court of Criminal Appeals said the federal court ruling also applies to the Cherokee, Choctaw, Chickasaw, Quapaw and Seminole Nations. The Federal Government now has criminal jurisdiction over major crimes which occur on Indian reservation land involving tribal members as a subject or victim.

Since the Federal court ruling in the McGirt case, the FBI's Oklahoma City field office has managed thousands of Indian Country cases, whereas previously the field office investigated approximately 50 criminal cases a year involving Native Americans.

Under the Major and General Crimes Acts, the FBI investigates the most serious crimes in Indian Country, including murders, rapes and child sexual abuse. In eastern Oklahoma, criminal cases involving tribal members as victims or suspects that previously would have been managed by state district courts and local law enforcement are now under Federal jurisdiction. The case load includes not only new cases, but cases that were already in the criminal process, cases appealed by currently incarcerated persons, and closed cases being re-examined.

Combined, all six reservation territories encompass approximately 32,000 square miles, or 45 percent of the state of Oklahoma. The total population within the combined borders is roughly 1.9 million, of which approximately 420,000 are enrolled tribal members.

This drastic increase in FBI jurisdiction poses significant and long-term operational and public safety risks given the challenges associated with the increased number of violent criminal cases now under Federal jurisdiction within Oklahoma's Indian Country territory. Since this decision, the FBI's Oklahoma City Field Office (OC) now has the FBI's largest Indian Country investigative responsibility.

The vast majority of FBI OC Indian Country cases are death investigations and investigations of child sexual abuse, violent assaults, rape, and domestic violence. These investigations align to DOJ's strategic goal to *Keep Our Country Safe* and objectives to *Combat Violent Crime and Gun Violence* and *Protect Vulnerable Communities*, as well as meeting the goals of *Operation Lady Justice*, the Presidential Task Force on Missing and Murdered American Indians and Alaska Natives established by Executive Order 13898 in November 2019.

Currently, the FBI has been forced to send SAs, IAs, and professional staff to Oklahoma City on 90-day rotations, resulting in significant travel and lodging costs, and hampering investigations which experience frequent turnover in personnel. On average, more than 50 personnel are on temporary rotation to FBI OC at any given time. This is in addition to the over hire authority FBI OC has received for 52 positions to keep a larger number of permanent staff onboard. Without a permanent staffing level increase, these TDYs and over hire positions come at the expense of personnel and fill rates in other FBI field offices.

Based on the increased operational needs created by the *McGirt* decision, the FBI requests $18,805,000 to account for the FBI's necessary, permanent staffing increase in OC. This includes compensation and benefits for 45 Special Agents, 1 Intelligence Analyst, 1 Attorney and 29 professional staff positions assigned to work Indian Country matters within the FBI OC territory. These personnel requests are paramount to properly address the current and expected caseload generated by the adoption of the *McGirt* decision. The FBI requires these positions to directly address the many ongoing investigations and ensure facilities, equipment, technology and other administrative matters are adequately maintained and supported.

In addition to the increase in personnel, the FBI requests $3,708,000 to address requirements such as rent, training, and operational case costs. This request includes $85,000 for ongoing training for Agents, Tribal Law Enforcement, and Task Force Agents coming into Indian Country who require area-specific knowledge to carry out their duties more effectively. To accommodate the increase in staffing, the FBI requests $2,675,000 in additional funding for physical space (e.g., rent, buildout, construction). The remainder of the non-personnel request includes $948,000 to cover the costs of new operations, task force overtime, and other yearly operational and discretionary costs.

Impact on Performance

The FBI's current footprint in Oklahoma draws personnel from other field offices and from programs within FBI OC, effectively reducing resources available to investigate other illegal activity, such as domestic terrorism or cyber-crime, both within Oklahoma and across the nation. Furthermore, reducing violence and protecting American communities through vigorous investigation of violent crimes is a key DOJ priority, as is DOJ's commitment to enhance the operation of the criminal justice system to address the concerns of tribal communities. To keep Oklahoma safe, and to fully respond to effectively respond to the increased operational requirements resulting from the *McGirt* decision while maintaining operational posture against other threats, the FBI requires an additional $22,513,000 allocated to FBI OC and the Indian Country program.

Funding

1. **Base Funding**

FY 2021 Enacted				FY 2022 President's Budget				FY 2023 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
0	0	0	$0	0	0	0	0	0	0	0	$0

2. **Personnel Increase Cost Summary**

Type of Position/Series	Positions Requested	Annual Costs per Position ($000)			FY 2023 Request ($000)	Annualizations ($000)	
		1st Year Adjusted Cost	2nd Year Adjusted Cost	3rd Year Full Cost (Modular)		FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Special Agent, Field	45	$328	$276	$397	$14,779	($2,346)	$5,490
Intelligence Analyst	1	$183	$192	$258	$183	$9	$66
Attorney	1	$183	$279	$288	$183	$97	$9
CART Examiner	1	$284	$268	$302	$284	($15)	$35
Clerical	2	$84	$114	$156	$168	$59	$86
Electronic Technician	1	$269	$179	$246	$269	($89)	$68
Information Technology	2	$115	$219	$254	$230	$207	$72
Professional Support	17	$118	$158	$227	$2,012	$690	$1,190
Staff Operations Specialist	6	$116	$155	$189	$698	$232	$210
Total Personnel	**76**	**$1,680**	**$1,838**	**$2,315**	**$18,805**	**($1,156)**	**$7,226**

3. **Non-Personnel Increase/Reduction Cost Summary**

Non-Personnel Item	FY 2023 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Case Funds	$848	N/A	N/A	$0	$0
Contract – Training	$85	N/A	N/A	$0	$0
Supplies	$100	N/A	N/A	$0	$0
GSA-Rent	$2,675	N/A	N/A	$0	$0
Total Non-Personnel	**$3,708**	**N/A**	**N/A**	**$0**	**$0**

4. **Justification for Non-Personnel Annualizations**

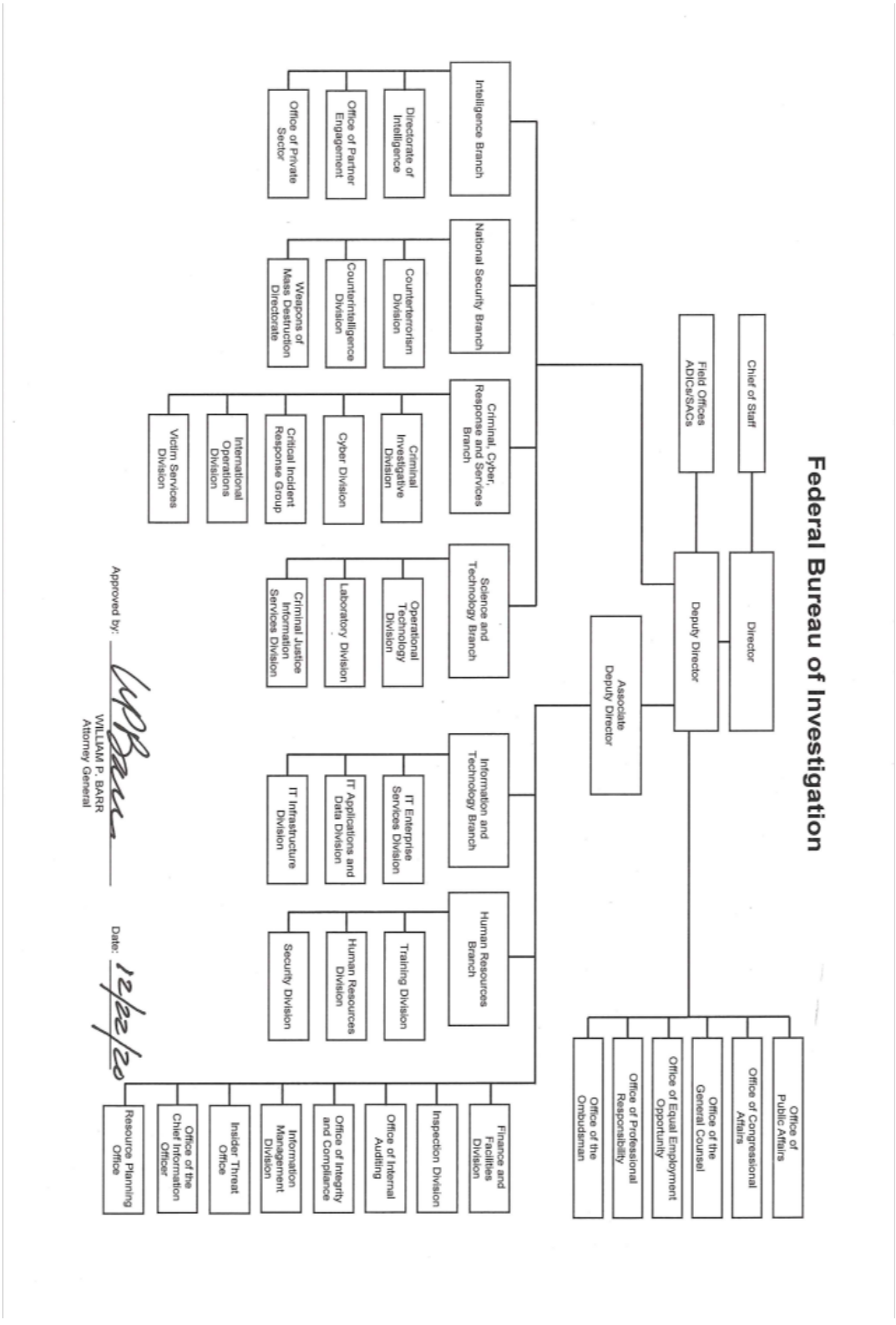
The FBI is requesting limited non-personnel funding in support of McGirt, all of which is expected to recur in the outyears based upon operational requirements. With the large increase in case volume, the FBI will continue to require increased funding to support case and source requirements. In addition, continued training will be needed to better partner and establish effective coordination with task force officers and tribal law enforcement. Finally, the Oklahoma City division will have continued space and equipment needs to support its increased mission.

5. **Total Request for this Item**

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Current Services	0	0	0	$0	$0	$0	N/A	N/A
Increases	76	45	38	$18,805	$3,708	$22,513	($1,156)	$7,226
Grand Total	**76**	**45**	**38**	**$18,805**	**$3,708**	**$22,513**	**($1,156)**	**$7,226**

VI. EXHIBITS

(U) A. Organizational Chart



VII. CONSTRUCTION

Overview: The FBI utilizes Construction funding for costs related to the planning, design, construction, modification, or acquisition of buildings and for the operation and maintenance of SWE facilities and secure networking capabilities. Construction funding supports both the national security and LE missions of the FBI.

The FBI requests $61,895,000 in the Construction account for the SWE program and safety and strategic improvements to the Quantico Campus..

SWE: SWE funds are used to apply USIC SWE standards to FBI facilities – both their physical (e.g., SCIFs) and IT infrastructure (e.g., SCINet). They are also used for SCIF construction and renovation, as well as the installation and maintenance of Top Secret networks.

FBI Redstone Arsenal: The FBI has maintained a presence at Redstone Arsenal in Huntsville, Alabama, for over 50 years, and the FBI is expanding its footprint across the base, positioned among some of the nation's top defense, LE, and technology organizations. These new facilities will drive a new era of innovation in a city deemed the "Silicon Valley of the South," where the lower cost of living and modern amenities are among the many highlights for FBI personnel whose roles are relocated to Huntsville.

By spring 2022, the FBI's presence on the North Campus will feature 300,000-square-foot operations building designed to accommodate approximately 1,350 personnel across 12 different operational and administrative FBI divisions. A nearby 87,000-square-foot technology building will house approximately 330 personnel to monitor the FBI's network 24/7/365, providing network monitoring and insider threat detection essential to the protection of sensitive intelligence and information for the entire organization.

The South Campus provides tremendous growth opportunities for the FBI and its LE partners. The recently constructed Ballistics Research Facility (BRF) is the world's only LE ammunition testing facility. The BRF evaluates weapon systems and body armor and shares this intelligence with FBI partners, including providing expert testimony in state and local LE criminal proceedings.

The current and future FBI Redstone facilities covered here reflect just a few of the innovative projects designed to ensure FBI agents and operational support personnel have state-of-the-art equipment and training to combat increasingly complex global threats.

FBI Quantico: The journey for every FBI employee starts at the FBI Academy in Quantico, Virginia. The campus hosts world-class Special Agent, Intelligence Analyst, and Professional Staff trainings, equipping these positions with the skills to investigate the nation's most critical threats. But the Academy does not only train FBI employees – it is also hosts the best and brightest LE personnel from around the world for 10 weeks at the National Academy and two 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 LE and intelligence professionals worldwide.

FBI Pocatello: Maintained for more than 30 years, the FBI's campus in Pocatello, Idaho, supports several missions and is home to a state of the art data center. The completion of this data center is a significant milestone in the organization's broader information technology transformation initiative and will provide DOJ agencies with both classified and unclassified data processing capabilities for the foreseeable future.

The facility has evolved from an FBI continuity of operations (COOP) facility with a single data center into a consolidated campus of nine buildings (more than 245,000 square feet) serving about 330 employees. As part of the DOJ-wide data center consolidation project, the facility – along with a handful of data centers, including the data center in the CJIS facility in Clarksburg, West Virginia – consolidates leased data centers across the DOJ in Northern Virginia, Texas, Maryland, and other locations.

FBI Clarksburg: The FBI Clarksburg campus encompasses nearly 1,000 acres in Clarksburg, West Virginia, and is home to the CJIS Division. CJIS serves as a high-tech hub providing state-of-the-art tools and services to LE, national security, and intelligence partners and to the public. Additionally, the campus hosts staff from other government agencies, including the ATF, DHS, and DOD. The campus, built on land acquired by the FBI, was completed in 1995. It houses over 3,700 staff and consists of two primary buildings: CJIS Main, a 528,000-square-foot office building, and the Biometric Technology Center (BTC), a 470,000-square-foot building dedicated to the analysis and advancement of biometrics and human characteristics to aid identification. The campus also includes a central utility plant, a shipping and receiving facility, a visitor's center, and related support facilities.

FBI Winchester: The FBI's new Central Records Complex (CRC) in Winchester, Virginia, will house more than two billion pages of records by 2022. The 256,000-square-foot facility uses robots to help manage the storage of truckloads of archived records now housed at each of the FBI's 56 field offices and other sites. Construction of the facility began in late 2017 and was completed in August 2020, when employees loaded the first records into custom-designed bins to be shuttled away by robots into darkened, climate-controlled confines for safe keeping and easy retrieval.

Built for nearly 500 employees, the facility also includes an office support building and visitor screening facility. The CRC houses an automated storage and retrieval system used to store and retrieve records quickly and efficiently, leveraging innovative technologies never before used in the federal government. The system manages more than 361,000 records storage bins (specifically designed for this system) using an overhead grid of frameworks, allowing robots to retrieve the desired records.

FBI Headquarters: Built in 1975 to support 2,000 personnel, the FBI HQ infrastructure, including mechanical, electrical, and life safety systems, require critical repairs or replacement to safely support the current capacity of 5,500 FBI personnel. The Administration also recognizes the critical need for a new FBI headquarters. The J. Edgar Hoover building can no longer support the long term mission of the FBI. The Administration has begun a multi-year process of constructing a modern, secure suburban facility from which the FBI can continue its mission to protect the American people. During the next year, FBI and GSA will work to identify a location to construct a Federally-owned, modern and secure facility for at least 7,500 personnel in the suburbs. Over the next year, FBI and GSA will finalize an updated program of requirements for a secure suburban campus, including the final number of personnel, to inform a 2024 Budget request for funding for the new facility. GSA will also begin initial steps to acquire, if necessary, the site for the new suburban location. Additionally, FBI and GSA will work to identify a Federally-owned location in the District of Columbia to support a presence of approximately 750–1,000 FBI personnel that would support day-to-day FBI engagement with DOJ headquarters, the White House, and Congress.

Appropriations Language and Analysis of Appropriations Language

Appropriations Language for Construction

For necessary expenses, to include the cost of equipment, furniture, and information technology requirements, related to construction or acquisition of buildings, facilities and sites by purchase, or as otherwise authorized by law; conversion, modification and extension of federally owned buildings; preliminary planning and design of projects; and operation and maintenance of secure work environment facilities and secure networking capabilities; $61,895,000 to remain available until expended.

Analysis of Appropriations Language

- No substantive change

VIII. GLOSSARY

ACTP	Accelerated Cyber Training Program
ADIC	Assistant Director in Charge
AGAAVE	Anti-Government or Anti-Authority Violent Extremism
Agt	Special Agent
AI	Artificial Intelligence
ALATs	Assistant Legal Attachés
AOR	Area of Responsibility
APB	Advisory Policy Board
ATB	Adjustments to Base
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
Atty	Attorney
A/V	Audio/ Visual
AWFC	Analytic Writing for Fusion Centers
BIDMAS	Bureau Investigative Document Management and Analysis System
BRF	Ballistics Research Facility
BTC	Biometric Technology Center
BWC	Body Worn Camera
C2	Command and Control
CBP	Customs and Border Patrol
CAR	Criminal Answer Required
CARD	Child Abduction Rapid Deployment Team
CARES	Coronavirus Aid, Relief and Economic Security Act
CART	Computer Analysis Response Team
CBP	Customs and Border Protection
CCRSB	Criminal, Cyber, Response, and Services Branch
CD	Counterintelligence Division
CDC	Centers for Disease Control
CEFC	Criminal Enterprises and Federal Crimes
CHRI	Criminal History Record Information
CHS	Confidential Human Source
CI	Counterintelligence
CIA	Central Intelligence Agency
CID	Criminal Investigative Division
CIP	Computer Intrusion Program
CIRG	Critical Incident Response Group
CISO	Chief Information Security Officer
CJ	Criminal Justice
CJIS	Criminal Justice Information Services
CJS	Criminal Justice Services
CNE	Computer Network Exploitation
CODIS	Combined DNA Index System
COL	Color of Law
CONUS	Continental United States
COOP	Continuity of Operations

CP	Counterproliferation
CPOT	Consolidated Priority Organization Target
CRC	Central Records Complex
CSO	Child Sex Offender
CSR	Customer Service Representative
CST	Child Sex Tourism
CT	Counterterrorism
CTAP	Cyber Threat Actor Program
CT/CI	Counterterrorism/Counterintelligence
CTD	Counterterrorism Division
C-TOC	Counter Transnational Organized Crime
C-UAS	Counter-Unmanned Aircraft Systems
CWS	Consolidated Watchlist System
CY	Calendar Year
CyD	Cyber Division
DCAP	Digital Collection and Analysis Platform
DEA	Drug Enforcement Agency
DHS	Department of Homeland Security
DI	Directorate of Intelligence
DIA	Defense Intelligence Agency
DNA	Deoxyribonucleic Acid
DOD	Department of Defense
DOI	Department of the Interior
DOJ	Department of Justice
DOS	Department of State
DSAC	Domestic Security Alliance Council
DT	Domestic Terrorism
DTLI	Detect, Track, Locate, and Identify
DTO	Drug-trafficking Organizations
DTOS	Domestic Terrorism Operations Section
DU	Decision Unit
DVE	Domestic Violent Extremists
EAD	Executive Assistant Director
ECLS	Enterprise Logging Solution
eDO	Electronic Departmental Order
EDR	Endpoint Detection and Response
EO	Executive Order
EPA	Environmental Protection Agency
ESOC	Enterprise Security Operations Center
ESTA	Electronic System for Travel Authorization
ET	Electronic Technician
ETI	Enterprise Theory of Investigation
E-Tips	Electronic Tips
EUROPOL	European Union Agency for Law Enforcement Cooperation
EVoIP	Enterprise Voice over Internet Protocol
FAA	Federal Aviation Administration
FACE	Freedom of Access to Clinic Entrance

FBI	Federal Bureau of Investigation
FD	Finance Division
FDDU	Federal DNA Database Unit
FFD	Facilities and Finance Division
FFL	Federal Firearms Licensee
FinCEN	Financial Crimes Enforcement Network
FLP	Foreign Language Program
FLSD	Facilities and Logistics Services Division
FO	Field Office
FOIA	Freedom of Information Act
FOSP	Field Office Strategic Plan
FTE	Full-time Equivalent
FTTTF	Foreign Terrorist Tracking Task Force
FTU	Firearms/Toolmarks Unit
FY	Fiscal Year
GCA	General Crimes Act
GPS	Global Positioning System
GRU	Russian Military Intelligence
HDS	Hazardous Devices School
HIG	High-Value Detainee Interrogation Group
HMA	Huntsville Metropolitan Area
HQ	Headquarters
HRB	Human Resources Branch
HRD	Human Resources Division
HRT	Hostage Rescue Team
HRVWCC	Human Rights Violators and War Crimes Center
HUMINT	Human Intelligence
HVE	Homegrown Violent Extremists
I2	Identities Intelligence
IA	Intelligence Analyst
IAFIS	Integrated Automated Fingerprint Identification System
IB	Intelligence Branch
IC	Indian Country
IC	Intelligence Community
IC3	Internet Crime Complaint Center
ICS	Industrial Control Systems
ICSJU	Indian Country and Special Jurisdiction Unit
IDU	Intelligence Decision Unit
IED	Improvised Explosive Device
IHR	International Human Rights
IHRU	International Human Rights Unit
III/Triple I	Interstate Identification Index
IIR	Intelligence Information Reports
IINI	Innocent Images National Initiative
ILNI	Innocence Lost National Initiative
IMD	Information Management Division
INSD	Inspection Division

IntelSup	Intelligence for Supervisors
InTO	Insider Threat Office
IntroTel	Introduction to Intelligence
IOD	International Operations Division
IPM	Integrated Program Management
IPR	Intellectual Property Right
IPS	Interstate Photo System
PII	Personally Identifiable Information
IRM	Information Resource Management
IRS-CI	Internal Revenue Service – Criminal Investigations
IS	Information System
ISIS	Islamic State of Iraq and ash-Sham
ISSE	Information Systems Security Engineering
ISSM	Information Systems Security Management
ISSO	Information Systems Security Operation
IT	Information Technology
ITS	Information Technology Specialists
ITADD	IT Applications and Data Division
ITB	Information and Technology Branch
ITCRMD	IT Customer Relationship and Management Division
ITESD	IT Enterprise Services Division
ITID	IT Infrastructure Division
ITMI	Information Technology Modernization Initiative
JCODE	Joint Criminal Opioid and Darknet Enforcement
JEH	J. Edgar Hoover Building
JTTF	Joint Terrorism Task Force
JWICS	Joint Worldwide Intelligence Communication System
KST	Known or Suspected Terrorist
LAPD	Los Angeles Police Department
LD	Laboratory Division
LE	Law Enforcement
LEO	Law Enforcement Officer
LEEP	Law Enforcement Enterprise Portal
LIE	Legal Instrument Examiner
MAPA	Management and Program Analyst
MCA	Major Crimes Act
MCAS	Malicious Cyber Actor System
MCN	Muscogee Creek Nation
MDF	Main Distribution Frame
MENACE	Mobile Encrypted Networks and Communications Exploitation
MLF	Money Laundering Facilitator
MMIP	Missing or Murdered Indigenous Persons
MPF	Multimedia Processing Framework
NAS	National Air Space
NCAVC	National Center for the Analysis of Violent Crime
NCIC	National Crime Information Center
NCIJTF	National Cyber Investigative Joint Task Force

NCIS	Naval Criminal Investigative Service
NCITF	National Counterintelligence Task Force
NCJ	Non-Criminal Justice
NCMEC	National Center for Missing and Exploited Children
NCPC	National Counterproliferation Center
NCSC	National Counterintelligence and Security Center
NCTC	National Counterterrorism Center
N3G	NCIC 3rd Generation
N-DEx	National Data Exchange
NDIS	National DNA Index System
NGI	Next Generation Identification
NIBRS	National Incident-Based Reporting System
NICS	National Instant Criminal Background Check System
NIP	National Intelligence Program
NIPF	National Intelligence Priorities Framework
NITTF	National Insider Threat Task Force
NIV	Non-Immigrant Visa
NPPS	National Palm Print System
NSB	National Security Branch
NSPM	National Security Presidential Memorandum
NSSE	National Special Security Event
NSTA	National Security Threat Actor
NSTP	National Security Threat Program
NTOC	National Threat Operations Center
NTOS	National Threat Operations Section
NTP	National Threat Priority
NVC	National Vetting Center
NVTC	National Virtual Translation Center
OC	Oklahoma City
OCE	Online Covert Employee
OCA	Office of Congressional Affairs
OCIO	Office of the Chief Information Officer
OCONUS	Outside the Continental United States
ODNI	Office of the Director of National Intelligence
OEEOA	Office of Equal Employment Opportunity Affairs
OGC	Office of the General Counsel
OIC	Office of Integrity and Compliance
OMB	Office of Management and Budget
OPA	Office of Public Affairs
OPE	Office of Partner Engagement
OPR	Office of Professional Responsibility
OPS	Office of Private Sector
OPS 1, 2, 3	Operations Building 1, 2, 3
OPU	Operational Projects Unit
OPWAN	Operational Wide Area Network
OSHA	Occupational Health Professionals
OST	Operational Support Technician

OTD	Operational Technology Division
PII	Personally Identifiable Information
POC	Point of Contact
PPP	Paycheck Protection Program
PPV	Practical Problem Venues
PS	Professional Staff
PS	Professional Support
PSC	Personal Service Contractors
PSC	Private Sector Coordinator
RA	Resident Agency
RAT	Recovery Asset Team
RBS	Rap Back Services
RCFL	Regional Computer Forensic Laboratory
RDT&E	
RF	Radio Frequency
RMD	Records Management Division
RMDT	Racially Motivated Domestic Terrorism
RMVE	Racially Motivated Violent Extremism
RPO	Resource Planning Office
RSA	Redstone Arsenal
RV	Recreational Vehicle
S&E	Salaries and Expenses
SA	Special Agent
SAC	Special Agent in Charge
SAO	Security Advisory Opinion
SAR	Suspicious Activity Reports
SCADA	Supervisory Control and Data Acquisition
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCINet	Sensitive Compartmented Information Network
SEAR	Special Event Assessment Rating
SecD	Security Division
SecDevOPS	Security Development Operations
SHOU	Shield HUMINT Operations Unit
SIA	Special Interest Alien
SID	State Identification Number
SIIG	Strategic Intelligence Issues Group
SIOC	Strategic Information Operations Center
SIP	Session Initiation Protocol
SIV	Special Interest Visa
SLTT	State, Local, Tribal, and Territorial
SME	Subject Matter Expert
SOC	Security Operations Center
SOG	Special Operations Group
SOP	Standard Operating Procedure
SOS	Staff Operations Specialists
SOS/TS	Staff Operations Specialists-Tactical Specialists

SRS	Summary Reporting System
SSA	Supervisory Special Agent
SSG	Special Surveillance Group
STB	Science and Technology Branch
STE	Sensitive Technical Equipment
SVP	Senior Vice President
SWE	Secure Work Environment
TAG	Transnational Anti-Gang Task Force
TCO	Transnational Criminal Organization
TD	Training Division
TDI	Technology and Data Innovation
TDY	Temporary Duty
TECH 1, 2, 3	Technology Building 1, 2, 3
TEDAC	Terrorist Explosive Device Analytical Center
TFO	Task Force Operator
THRU	Technical Hazards Response Unit
TIE	Threat Intake Examiner
TIPS	Threat Intake Processing System
TOC	Transnational Organized Crime
TRP	Threat Review and Prioritization
TRPS	Ten Print Rap Sheet
TS	Top Secret
TSC	Terrorist Screening Center
TSS	Threat Screening System
TSA	Transportation Security Administration
TSC	Terrorist Screening Center
TSDB	Terrorist Screening Data Base
TTK	Triage Toolkit
TTL	Threat to Life
TTP	Tools, Techniques, and Procedures
UAS	Unmanned Aircraft System
UC	Unit Chief
UCE	Undercover Employee
UCN	Universal Control Number
UCR	Uniform Crime Reporting
ULF	Unsolved Latent File
UNet	Unclassified Network
US	United States
USG	United States Government
USIC	United States Intelligence Community
USMS	U.S Marshals Service
USPIS	United States Postal Inspection Service
VAF	Voluntary Appeal File
VGSSTF	Violent Crime and Safe Streets Gang Task Forces
VPNs	Virtual Private Networks
VSD	Victim Services Division
WCC	White Collar Crime

WIDT	Wireless Identification and Direction-Finding Team
WMD	Weapons of Mass Destruction
WMDD	Weapons of Mass Destruction Directorate
5G	5th Generation