U.S. Department of Justice
Federal Bureau of Investigation

FY 2024 President's Budget Request

February 2023

Table of Contents

I. Overview

A. Introduction

Budget Request Summary: The Federal Bureau of Investigation's (FBI's) Fiscal Year (FY) 2024 budget request proposes a total of $11,386,015,000 in direct budget authority, of which $11,324,120,000 is for Salaries and Expenses (S&E) and $61,895,000 is for Construction.

The S&E request includes a total of 37,312 direct positions and 36,131 direct full-time equivalents (FTE); the positions include:

- 13,662 Special Agents (SAs)
- 3,215 Intelligence Analysts (IAs)
- 20,435 Professional Staff (PS)

The S&E program changes total $196,040,000; 306 positions (56 SAs, 7 IAs, and 243 PS), and 150 FTE, for the following:

- $63,390,000 for cyber investigative capabilities
- $12,962,000 to counterterrorism matters
- $4,466,000 for counterintelligence matters
- $27,219,000 for cybersecurity
- $14,862,000 for violent crime
- $53,117,000 for DNA lab support
- $3,100,000 for secure communications
- $14,140,000 for Zero Emission Vehicles
- $2,784,000 for Body Worn Cameras

The request includes $27,733,000 in net technical adjustments and $409,047,000 in adjustments to base (ATBs) for continued support of the FBI's current activities.

The $61,895,000 requested in the Construction account will maintain the Secure Work Environment (SWE) program and provide for ongoing activities at the FBI facilities in Quantico, Virginia.

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 2024 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 of the United States.

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 for all
- 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 cyber-criminal 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 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 2024 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 most 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 36 sub-offices in 80 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 several 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 the resources of the DI are allocated to the Intelligence Decision Unit, while all 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 2024. 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 2024 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 2021, 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), 85 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 2021, there were 1682 arrests, 1427 indictments, 162 information's, 515 judicial complaints, and 1004 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 23 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.

D. Executive Order (E.O.) and OMB Memo Concurrence

As it relates to E.O. 14058, "Transforming Federal Customer Experience and Service Delivery To Rebuild Trust in Government;" E.O. 14035, "Diversity, Equity, Inclusion, and Accessibility in the Federal Workforce;" and OMB Memo M-22-10, "Improving Access to Public Benefits Programs Through the Paperwork Reduction Act;" the FBI continues to analyze resource needs and will provide additional information after analysis is complete. In the interim:

OMB Memo M-22-10, "Improving Access to Public Benefits Programs Through the Paperwork Reduction Act"

Investing in records management workflow processes to transition to a fully digital workspace will allow the FBI to respond quickly and accurately to litigation, Freedom of Information Act (FOIA), Public Affairs, and eDiscovery requests.

The FBI is also increasing the scanning and digitization of paper records in FBI offices to meet the OMB requirement for ending the submission of paper records to the Federal Records Center (FRC).

E.O. 14035, "Diversity, Equity, Inclusion, and Accessibility in the Federal Workforce"

The FBI's will develop and execute diversity and inclusion strategies to support a high performing, diverse, and inclusive workforce, and foster a culture that integrates diversity and inclusion across the enterprise.

E.O. 14058, "Transforming Federal Customer Experience and Service Delivery To Rebuild Trust in Government"

Executive Order 14058 requires all entities of Government to continually improve their understanding of their customers, reduce administrative hurdles and paperwork burdens to minimize "time taxes," enhance transparency, create greater efficiencies across government, and redesign compliance-oriented processes to improve customer experience and more directly meet the needs of the people of the United States.

The FBI is working to fully meet these requirements through the following ongoing efforts:

- The FBI uses the FBI.gov website platform to inform and alert members of the public to mobilize them to assist investigations and to empower them to protect themselves from ongoing threats and crimes. The platform enhances the public's trust and confidence in the FBI by sharing information about the FBI's responsibilities, operations, accomplishments, policies, and values.
- The FBI accomplishes its external communications and engagement mission primarily through the management of the FBI's Media Relations and Community Outreach programs by facilitating the public release of information through liaison with media; by making direct contact with the public through the Internet, speeches, reports, digital production and community outreach activities; and by working with authors, television and film producers, and other interested parties who seek to depict the FBI in their productions.
- The FBI continues its mission to reach vulnerable communities and reinforce the FBI's dedication to investigating and bringing to justice the perpetrators of civil rights crimes.

II. Summary of Program Changes

Item Name	Description	Pos.	FTE	Dollars ($000)	Page
Salaries and Expenses Enhancements					
Cyber	This request is classified.	192	97	$63,390	64
Counterterrorism	This request is classified.	43	22	$12,962	65
Counterintelligence	This request is classified.	30	16	$4,466	66
Cybersecurity	Several highly publicized breaches of systems and data have exposed cybersecurity vulnerabilities in government networks and information systems. The speed, and complexity of computing technologies continues to evolve, and with it, so must the FBI investment in effective Cybersecurity technologies.	4	2	$27,219	67
Violent Crime	The requested resources will significantly expand efforts to deter criminal acts against children and strengthen national criminal background check resources	44	23	$14,862	72
DNA	The requested resources will allow the FBI to process the rapidly increasing number of DNA samples collected by the U.S. Department of Homeland Security, implement the Rapid DNA standards and procedures as required by the Rapid DNA Act of 2017, and re-architect the current Combined DNA Index System (CODIS) software application to a modern cloud-based application.	7	4	$53,117	81

Item Name	Description	Pos.	FTE	Dollars ($000)	Page
Salaries and Expenses Enhancements					
Secure Communications	The requested resources will allow the FBI to sustain reliable, secure access to classified information and systems in a remote environment, which improves the timely completion of investigative activities, dissemination of intelligence, and sustainment of necessary business operations.	0	0	$3,100	88
Zero Emission Vehicles	This request will allow the FBI to address requirements of Executive Order 14057 and meet standards for sustainable and resilient federal facilities and vehicle fleet electrification.	0	0	$14,140	92
Body Worn Cameras	The requested resources will support the FBI's implementation of a body worn camera program for all FBI Special Agents, enhancing law enforcement transparency and accountability.	0	0	$2,784	96
Salaries and Expenses Enhancements Total		**320**	**164**	**$196,040**	

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, $11,324,120,000 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)
2022 Enacted (including supplementals)	6,563	6,522	$1,872,638
2023 Enacted (including supplementals)	6,665	6,331	$1,971,753
Adjustments to Base and Technical Adjustments	0	50	$70,668
2024 Current Services	6,665	6,381	$2,042,421
2024 Program Increases	10	5	$22,930
2024 Program Decreases	(-1)	(-1)	$0
2024 Request	6,674	6,385	$2,065,351
Total Change 2023-2024	**9**	**54**	**$93,598**

Intelligence - Information Technology Breakout (of Decision Unit Total)	Direct Pos.	Estimate FTE	Amount ($000s)
2022 Enacted (including supplementals)			$179,975
2023 Enacted (including supplementals)			$291,696
Adjustments to Base and Technical Adjustments			$10,455
2024 Current Services			$302,151
2024 Program Increases			$3,392
2024 Request			**$305,543**

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 2023		**FY 2023**		**FY 2024**		**Current Services Adjustments and FY 2024 Program Change**		**FY 2024 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**
	6,331	$1,971,753	N/A	N/A	6,381	$2,042,421	5	$22,930	6,385	$2,065,351

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**	**Actual**	**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%	19.6%	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 (IC) 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%
FY22 Actual: 19.6%
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 enhance its successful operating posture.

B. Counterterrorism/Counterintelligence Decision Unit

Counterterrorism/Counterintelligence Decision Unit Total	Direct Pos.	Estimate FTE	Amount ($000s)
2022 Enacted (including supplementals)	13,781	13,783	$4,120,128
2023 Enacted (including supplementals)	14,055	13,231	$4,329,805
Adjustments to Base and Technical Adjustments	0	132	$148,267
2024 Current Services	14,055	13,363	$4,478,072
2024 Program Increases	161	82	$75,790
2024 Program Decreases	0	0	$0
2024 Request	14,216	13,445	$4,553,862
Total Change 2023-2024	**161**	**214**	**$224,057**

Counterterrorism/Counterintelligence - Information Technology Breakout (of Decision Unit Total)	Direct Pos.	Estimate FTE	Amount ($000s)
2022 Enacted (including supplementals)			$283,547
2023 Enacted (including supplementals)			$456,520
Adjustments to Base and Technical Adjustments			$15,633
2024 Current Services			$472,153
2024 Program Increases			$7,991
2024 Request			**$480,144**

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, 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 prevent, prepare, and mitigate chemical, biological, radiological, nuclear, and explosive WMD-related threats actively and passively. 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 continues to work cases, which aid in prevention, disruption, and attribution efforts to mitigate WMD threats across the CBRNE modalities. During FY 2022, the WMDD disrupted 52 incidents; made 86 arrests; and had 39 indictments, 79 sentencings, and 71 convictions.

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 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 2023		**FY 2023**		**FY 2024**		**Current Services Adjustments and FY 2024 Program Change**		**FY 2024 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**
	13,231	$4,329,805	N/A	N/A	13,363	$4,478,072	82	$75,790	13,445	$4,553,862

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**	**Actual**	**Target**	**Target**	**Target**	**Goal**
KPI (DOJ Objective 2.2)	Number of terrorism disruptions effected through investigations.	400	561	450	793	600	438	600	600	600	600
KPI (DOJ Objective 2.1)	Number of counterintelligence program disruptions or dismantlements.	400	365	400	447	400	402	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%	26%	5%	5%	5%	5%
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%	45%	39.4%	65%	65%	65%	65%
KPI (DOJ Objective 2.4)	Percent increase in operations conducted jointly with strategic partners.	N/A	N/A	N/A	N/A	3%	39%	3%	3%	3%	3%
KPI (DOJ Objective 2.4)	Percent increase of threat advisories disseminated to the public sector	N/A	N/A	N/A	N/A	5%	4.2%	5%	5%	5%	TBD
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	5%	15%	10%	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 initiatives. 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 evaluates 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
FY22 Actual: 438
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 exclusive 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, State, Local, Tribal, and International Counterterrorism Partnerships*. To facilitate 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, other 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 in 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
FY22 Actual: 402
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 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 and Intellectual Property*. 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 with DOJ Objective 2.1 Strategy 4: *Protect sensitive assets*.

Cyber Division (CyD)

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%
FY22 Actual: 36%
FY23 Target: 5%
FY24 Target: 5%

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: 42.7%
FY22 Target: 45%
FY22 Actual: 39.4%
FY23 Target: 65%
FY24 Target: 65%

Performance Measure: Percent increase in operations conducted jointly with strategic partners.
FY21 Target: N/A
FY21 Actual: N/A
FY22 Target: 3%
FY22 Actual: 39%
FY23 Target: 3%
FY24 Target: 3%

Performance Measure: Percent increase of threat advisories disseminated to the private sector.
FY21 Target: N/A
FY21 Actual: N/A
FY22 Target: 5%
FY22 Actual: 4.2%
FY23 Target: 5%
FY24 Target: 5%

Performance Measure: Increasing the number of ransomware matters in which seizures or forfeitures are occurring by 10%.
FY21 Target: N/A
FY21 Actual: N/A

FY22 Target: 5%
FY22 Actual: 15%
FY23 Target: 10%
FY24 Target: N/A

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, sophisticated, and 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, as documented in Guardian, 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 another potential target institutions. True for all threats the American people face, partnerships are critical to both maintaining a posture that's ahead of the threat and establishing a robust response to mitigate damage and hold malicious actors responsible – these principles are 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 they're 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)
2022 Enacted (including supplementals)	13,216	12,775	$3,613,844
2023 Enacted (including supplementals)	13,575	13,379	$3,741,029
Adjustments to Base and Technical Adjustments	6	171	$158,778
2024 Current Services	13,581	13,550	$3,899,807
2024 Program Increases	121	62	$77,927
2024 Program Decreases	(-13)	(-13)	$0
2024 Request	13,689	13,599	$3,977,734
Total Change 2023-2024	**114**	**220**	**$236,705**

Criminal Enterprises/Federal Crimes Decision Unit - Information Technology Breakout (of Decision Unit Total)	Direct Pos.	Estimate FTE	Amount ($000s)
2022 Enacted (including supplementals)			$219,124
2023 Enacted (including supplementals)			$343,273
Adjustments to Base and Technical Adjustments			$14,569
2024 Current Services			$357,842
2024 Program Increases			$7,151
2024 Request			**$364,993**

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, and
- 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. 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 2023		**FY 2023**		**FY 2024**		**Current Services Adjustments and FY 2024 Program Change**		**FY 2024 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**
	13,379	$3,741,029	N/A	N/A	13,550	$3,899,807	62	$77,927	13,599	$3,977,734

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**	**Actual**	**Target**	**Target**	**Target**	**Goal**
Measure (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%	54.1%	46%	46%	46%	52%
Measure (DOJ Objective 4.2)	Number of criminal disruptions or dismantlements in public corruption and fraud against the government	N/A	N/A	N/A	453	468	407	487	487	400	545
Measure (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%	61.7%	60%	60%	60%	60%

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 effectively 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 Communities* 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 2024 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: 42%
FY22 Target: 44%
FY22 Actual: 54.1
FY23 Target: 46%
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 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: Number of criminal disruptions or dismantlements in public corruption and fraud against the government.
FY21 Target: N/A
FY21 Actual: 453
FY22 Target: 468
FY22 Actual: 407
FY23 Target: 487
FY24 Target: 487

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%

FY22 Actual: 61.7%
FY23 Target: 60%
FY24 Target: 60%

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 2024 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.

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, several 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

[1] This list reflects the most significant international narcotic manufacturers, poly-drug traffickers, suppliers, transporters, and money laundering organizations.
[2] For Violent Criminal Threat matters, an organization is a group of three or more individuals knowingly involved in a criminal activity.

(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 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)
2022 Enacted (including supplementals)	2,460	1,745	$723,285
2023 Enacted (including supplementals)	2,705	2,649	$648,713
Adjustments to Base and Technical Adjustments	0	38	$59,067
2024 Current Services	2,705	2,687	$707,780
2024 Program Increases	28	15	$19,393
2024 Program Decreases	0	0	$0
2024 Request	2,733	2,702	$727,173
Total Change 2023-2024	**28**	**53**	**$78,460**

Criminal Justice Services -Information Technology Breakout (of Decision Unit Total)	Direct Pos.	Estimate FTE	Amount ($000s)
2022 Enacted (including supplementals)			$132,949
2023 Enacted (including supplementals)			$358,269
Adjustments to Base and Technical Adjustments			$32,621
2024 Current Services			$390,889
2024 Program Increases			$10,710
2024 Request			**$401,600**

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 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) System: 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 System 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 System 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 Department of Defense (DOD).

The NGI System's operating efficiency is an assessment of the overall availability, accuracy, and robustness. The NGI System'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 System had a 99.78 percent availability rate in 2022.

Accuracy – The accuracy of 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, 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 System:

Tenprint Fingerprint - The NGI System contains over 217 million unique fingerprint identity records, and fingerprint responses continue to exceed customer expectations. During an average day in FY 2022, Ten Print Rap Sheet (TPRS) submissions are processed within 6 seconds. Criminal Answer Required (CAR) submissions are processed within 6 minutes, and civil submissions are processed within 26 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, 69,232,790 in FY 2019, and 45,734,030 in FY 2020; 47,762,026 in FY 2021; and 62,335,282 for all FY 2022. 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 7 of 10 fingerprint solutions" to allow the NGI System 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 February 16, 2023, the ULF consisted of 1,135,146 unidentified latent prints contributed by local, state, federal, and international LE agencies, as well as LD and members of the United States Intelligence Community from evidence within both criminal and terrorism investigations.

National Palm Print System (NPPS) - Implemented as a part of the NGI System in May 2013, NPPS provides an investigative biometric service that has dramatically improved law enforcement's access to palm prints. NPPS is a central repository responsible for maintaining known palm prints derived from criminal arrests, civil applications, and national security submissions from a variety of authorized sources nationwide. As of January 2023, the collection contains more than 27 million unique subjects from more than 60 million events that are available for nationwide investigative searches. Agencies in 49 states, Washington, D.C., and the territories of Guam and Puerto Rico contribute palm prints to NPPS. Latent searches from law enforcement agencies against the NPPS produce leads within unsolved criminal investigations nationwide.

NGI Rap Back Services - In September 2014, the NGI Rap Back Services were deployed with the implementation of the "Increment 4" enhancement. There are two domains within the NGI Rap Back Services: noncriminal justice (NCJ) and criminal justice (CJ).

The NGI NCJ Rap Back Services are 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 Rap Back Services are 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).

As of January 2023, three of the largest submitting agencies include the Transportation Security Administration (TSA) Precheck – Idemia, the TSA, and the State of Texas. The TSA Precheck – Idemia and the TSA has enrolled 5,472,705 and 1,176,245 Rap Back subscriptions respectively from numerous airports and airlines throughout the United States. Texas has enrolled 4,575,098 Rap Back subscriptions, to include teachers, nurses, and EMS workers.

Repository for Individual of Special Concern (RISC) - The NGI System added RISC in FY2011, containing over 4.5 million fingerprint records of wanted persons, registered sex offenders, immigration violators, Threat Screening Center subjects, and National Security Information subjects. RISC service assists federal, state, local, and tribal law enforcement officers on the street to use a mobile identification device to perform a "lights-out" rapid search of the RISC repository. Within seconds, officers receive a response and can quickly assess the threat level of any subject encountered during their normal law enforcement activities. In FY2022, the RISC

service processed more than 614,000 rapid mobile identification searches, responding with over 76,000 highly probably candidates associated with crimes including homicides, kidnappings, and carjackings.

Altered Biometric Identification Program (ABIP) - ABIP assists law enforcement partners and civil agencies by identifying, researching, and correcting identity history records of individuals with altered fingerprints. Fingerprint alteration caused accidentally or deliberately poses a risk to providing complete and accurate identity history responses to fingerprint searches of the NGI System. The ABIP staff have identified 1,631 individuals with altered fingerprints and researched each record to ensure it is accurate and complete. In FY2022, the ABIP staff identified and researched 102 new identities with altered fingerprints. In addition, the ABIP staff monitored and researched 479 fingerprint transactions relating to subsequent activity of individuals known to have altered their fingerprints and reviewed 6,068 fingerprint transactions in which an individual known to have altered their fingerprints appears on a candidate list in the NGI System. The ABIP staff is assisting with the development of two automated detection models, which have produced an additional 156 identities with altered fingerprints that had not previously been detected during the testing phase, indicating many more altered fingerprints remain undetected.

Deceased Persons Identification (DPI) Services - In FY2020, the Biometric Services Section rebranded the NGI Cold Case/Unknown Deceased Service as the DPI Services to provide an expanded service for all deceased identification request contributors. In FY2022, the NGI System processed more than 40,000 deceased identification requests, identifying more than 60 percent of all requests. For transactions not identified by the NGI System, the DPI Services staff conducted additional research and provided 48 percent more identifications. The DPI Services also created a nationwide focus group of deceased identification stakeholders and created best practices and guidance for the submission of these requests.

NGI Iris Service - On September 29, 2020, the FBI launched the NGI Iris Service providing enrollment and search functionalities. The NGI Iris Service is the only FBI-approved contactless identification biometric. As of 01/31/2023, the NGI Iris Service consists of over 2.5 million sets of iris images representing over 1.9 million unique identities. There are 617 domestic and international contributors from over 200 agencies participating in the NGI Iris Service.

The NGI Interstate Photo System (IPS) provides enhanced photo enrollment, retrieval, search, and maintenance capabilities. These enhancements permit broader acceptance and utilization of photos by allowing more photo sets per FBI record for criminal subjects, bulk submission of photos maintained at the federal or state level repositories, submission and searching of photos other than face (e.g., scars, marks, tattoos) and investigative facial recognition (FR) search capabilities. At the end of FY2022, the NGI IPS held over 131 million criminal and civil photos contributed by federal, state, local, tribal, and select foreign and international agencies that consisted of over 27.2 million unique identities. Over 61.5 million criminal mugshots were available for an investigative FR search.

The NGI IPS' investigative FR search component allows authorized federal, state, local, territorial, and tribal law enforcement (LE) agencies to submit investigative face photos (probe photos) for an automated FR search of the NGI IPS. First, the LE agencies FR systems must be programmed to handle the FR types of transactions as specified in the *Electronic Biometric*

Transmission Specifications, version 11.0. LE agencies must have approval of their federal or state CJIS Systems Officer prior to connecting. The automated NGI IPS FR algorithm is applied to each of the submitted images to determine if the image is of sufficient quality for searching; and, if so, the FR algorithm creates a face template. Contributors receive a minimum of two, a maximum of 50, or default of 20 candidates returned in a ranked investigative candidate list. Contributors are also required to compare all available candidates against their probe photo(s). Face photos returned in the ranked gallery include the associated FBI Universal Control Number. The NGI IPS FR algorithm was upgraded on 11/17/2019 improving FR algorithm accuracy to over 99 percent. CJIS Systems Agency/State Identification Bureau must ensure all authorized LE agencies take approved training prior to conducting investigative FR searches of the NGI IPS. In addition, FBI policies and procedures emphasize that photo candidates returned are not to be considered "positive identifications." Further investigation must be performed before making an arrest. In FY 2022,16,390 investigative FR searches of the NGI IPS had been performed.

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 Query (QH) 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 2022:

Name Based Queries (QH) – 398,287,245
Quoted UCN or SID Queries - (QR) – 62,199,502
Total number of incoming III transactions –460,486,787

NGI Electronic Departmental Order (eDO) – The NGI eDO system is utilized by individuals 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 System is a database of documented criminal justice information available to law enforcement agencies 24 hours a day, 365 days a year. The NCIC System provides a timely and accurate database of criminal justice information to local, state, tribal, and federal criminal justice agencies. The information supplied by the NCIC System is critical, supporting local, state, tribal, and federal criminal justice and law enforcement (LE) agencies and is organized into 22 files including: Wanted Person File, Missing Persons File, Unidentified Person File, Foreign Fugitives File, Immigration Violator File, Protection Order File, Supervised Release File, the National Sex Offender Registry, Identity Theft File, Gang File, Threat Screening Center File, Protective Interest File, NICS Denied Transaction File, Violent Person File, Extreme Risk Protection Order File, Article File, Gun File, License Plate File, Vehicle File, Securities File, Boat File, and the Vehicle/Boat Part File. This information is used for the compilation, dissemination, and exchange of time critical criminal

justice and law enforcement information. The Federal Bureau of Investigation (FBI) is charged by Title 28, Code of Federal Regulations, Section 20, as manager of the system.

The operational availability of the NCIC System for the law enforcement and criminal justice communities is vital to the CJIS Division's customer base. The safety of law enforcement personnel and the public depends upon this availability which is supported by an average up time of 99.73% over the past 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 17.4 million active records and processes an average of 10.2 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 31 states, five U.S. territories, and the District of Columbia. The NICS provides partial service to six states. The remaining 13 states perform their own checks through the NICS system.

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.

The NICS Alert Service (NAS) provides alerts to FBI or ATF case agents whenever a subject of interest (SOI) attempts to purchase a firearm or has any other NICS check conducted. Upon legal approval, an SOI can be entered into the NAS for a period of 30, 60, 90, or 180 days. A check of the NICS Audit Log is conducted upon enrollment to determine if there are any past NICS transactions. This information, and any subsequent NICS Audit Log hits during the enrollment period, are shared with the requesting FBI or ATF office. It is important to note that NAS does not result in a denial of an attempted purchase, but instead provides alerts to the field offices with the details of the transaction. In 2009, NAS began originally providing alerts to 25 Alcohol, Tobacco, Firearms, and Explosives (ATF) field divisions. In 2014, the service expanded to incorporate NAS to the 56 FBI field offices and eventually to all federal law enforcement agencies. Both the ATF NAS and FBI NAS require an active case investigation meeting certain legal thresholds for entry.

In FY 2022, the NICS processed over 31,000,000 total transactions compared to over 41,000,000 in FY 2021, a 24 percent decrease. Since the beginning of FY 2020, the NICS Section has seen a considerable increase of incoming federal firearms background checks. Although the volume has subsided somewhat from FY 2020 and FY 2021, the transaction volume in FY 2022 is 22 percent higher than the average of pre-pandemic years.

In FY 2021, the FBI received $179.0 million and 93 positions to address both COVID-19 and NICS as part of supplemental appropriations provided in the Consolidated Appropriations Act, 2021 (P.L. 116-260). The FBI also utilized regular appropriations provided in P.L. 116-260 to fund a NICS enhancement that added 53 NICS positions. In FY 2022, the FBI received $100.0 million and 170 positions as a result of the Bipartisan Safer Communities Act (BSCA) (P.L. 117-159). The additional resources provided by these appropriations were essential to the continuance of NICS operations. The increase in personnel had a positive impact in the number of firearm background checks that are processed within three business days. Of the 316 total positions, 229 were Legal Instruments Examiners responsible for performing firearm background checks. At current productivity rates, these 229 examiners are able to process over 900,000 transactions from the NICS Delay Queue in a year. The additional personnel were directly responsible for NICS to maintain the Attorney General (AG) goal of a 90 percent immediate determinate rate. The NICS program has successfully met the AG goal for 14 consecutive months. Without the additional personnel, NICS would not be successful in processing new regulatory and legislative background checks.

Over the past two years, NICS has increased the number of IT Development teams from eight to thirteen. This increase expedited the deployment of functionality to help with the automation of transactions, which was critical due to the increasing transaction volume. Within this time period, NICS was able to accommodate technical enhancements of unanticipated Federal mandates, such as the NICS Denial Notification Act (NDNA) and the BSCA. The NDNA and

the BSCA IT enhancements would not have deployed within the deadlines associated by the new law without the additional resources.

In addition to the congressional mandates, the development team continues to support over 300 enhancements that are critical to be developed for the NICS.

Some of the highlighted efficiencies and automation are listed below:

- Enhanced identity matching that will assist the work of the examiner by removing the candidates that are not a match and performing automation on candidates that are a match to the criminal history records.
- Automation enhancements were deployed to further expand the previously established automation solution to visualize what work needs to be prioritized to be automated. This will help to assist the Examiner with completing the high volume of work.
- There has been a focus on the Quality Assurance system enhancements as well. Within this time frame, functionality has been developed to allow for the Quality Assurance examiner to perform a random blind review of the examiner's work. Additional enhancement changes will not only impact the quality of the work, but the way that examiners are selected for review.
- Enhancements to other FBI repositories were developed to make sure that NICS has utilized all the internal resources that are available to close out transactions as quickly as possible, to include development efforts to gain external information as quickly and securely as possible.
- The NICS Alert service was enhanced to improve results, expedite response, and make the ingesting of new candidates as effective as possible.

The changes and efficiencies carried in the NICS product backlog continues to grow and is prioritized to ensure that NICS continues to work towards both automation and deliver efficiencies to the examiners.

Uniform Crime Reporting (UCR): 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 collects information through 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 public releases: *Crime in the United States, Law Enforcement Officers Killed and Assaulted*, *Hate Crime Statistics, National Incident-Based Reporting System, National Use-of-Force Data Collection* and the *Law Enforcement Suicide Data Collection*. The publications provide statistical compilations of violent crime data on murder, rape, robbery, aggravated assault, and burglary; non-violent crime; hate crime statistics; and law enforcement data on officers killed and assaulted in the line of duty; use-of-force incidents; and death by suicide. These publications also fulfill the FBI's obligations under Title 28, U.S. Code, Section 534.

The FBI Crime Data Explorer (CDE) is the public facing Internet website for the UCR data. The CDE is interactive and enables LE and the public to easily access the raw data used to compose the annual reports. The CDE provides multiple visualizations and infographics to comprehend the massive amounts of UCR data currently collected. Users can view charts and agency-level data without having to mine through data tables.

The UCR program established a Hate Crime Statistics focus group, which will engage the broader stakeholder community (LE, public, academia, policy, and advocacy) through a targeted UCR Subcommittee Task Force. The task force is comprised of stakeholder members and SMEs that will develop recommendations for the collection of hate crime data and release of statistics. The goal is to improve quantity and quality of data reporting and bias identification in hate crime resulting in more functional data available for analysis.

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 665 million searchable records from over 8,300 criminal justice agencies and provides access to an additional 360 million records from DHS, the Interstate Identification Index, NCIC, and INTERPOL.

National Threat Operations Center (NTOC): NTOC serves as the FBI's central intake point for the public and other government agencies to provide tips about federal violations, threats-to-life (TTL), and threats to national security. NTOC centralizes the flow of information from the public to the FBI by handling calls from all 56 FBI field offices (FO), the Major Case Contact

Center, the Internet Crimes Complaint Center, the WMD tip line, and all FBI electronic 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.

NTOC is a key component in the FBI's initiative to provide timely and direct notification of every TTL tip received by NTOC to the appropriate FO operations center. NTOC 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 and supervisory threat intake examiners, 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 are provided to the appropriate entity.

From January 31, 2022, through January 31, 2023, NTOC processed 1,098,318 tips, resulting in 50,924 Guardian entries (referrals to a field office for further action).

In addition, NTOC holdings are made available to all FBI FOs via "read-only" access through the LEEP. This unprecedented access allows FO more opportunities to enhance ongoing investigations/assessments and provide better situational awareness of tips reported to NTOC in the FO 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.

Training Division resumed the FBI National Academy in FY22 after a hiatus in FY21 due to the ongoing pandemic. Training Division held four National Academy sessions in FY22, with a total student count of 1,088. In FY23 there will be five sessions with approximately 200 students in

each session, a small portion of each of those sessions may be international students as travel guidelines continue to decrease.

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 2023		**FY 2023**		**FY 2024**		**Current Services Adjustments and FY 2024 Program Change**		**FY 2024 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**
	2,649	$648,713	N/A	N/A	2,687	$707,780	15	$19,393	2,702	$727,173

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	Actual	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%	6.8%	38%	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.	N/A	N/A	N/A	N/A	85%	98%	95%	95%	95%	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 2024. 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 support this backend infrastructure development and program management, the FBI was provided 102 FSL in the FY 2023 Enacted appropriation, which is, in part, to build, manage, and maintain the necessary components of the BWC and digital evidence systems. The filling of these positions is well underway, on track for full utilization in FY23.

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 the Washington Field Office's (WFO) 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 launched Phase II expansion that delivered 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). To date, the BWC program has deployed 1,007 BWC camera systems and related hardware in 48 locations within the five designated field offices and the two FBIHQ components. Phase III in 2023 will expand the BWC program to the fourteen additional FBI field offices.

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%
FY22 Actual: 6.8%
FY23 Target: 38%
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. 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 initial delivery of 500 camera systems. Phase III will initiate by deploying 3,200 BWC camera systems and related hardware that was purchased with the initial $2.8 Million allotment received in FY2023. The continued success of the BWC initiative remains contingent upon the program receiving the additional requested funding for hardware procurement and installation.

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

a. Performance Plan and Report for Outcomes

In support of DOJ Strategic Objective 3.3: *Reform and Strengthen the Criminal and Juvenile Justice Systems*, specifically Strategy 1: *Promote Trust Between Communities and Law Enforcement*, 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 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: N/A
FY21 Actual: N/A
FY22 Target: 85%
FY22 Actual: 98%
FY23 Target: 95%
FY24 Target: 95%

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 DOJ's law enforcement 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**
Strategic Goal(s):	2
Strategic Objective(s):	2.4
Budget Decision Unit(s):	All
Organizational Programs:	Cyber, Criminal Investigative Division

Program Increase: Positions 192 Agt 31 FTE 97 Dollars $63,390,000 ($20,923,000 non-personnel)

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

Item Name: **Counterterrorism**

Strategic Goal(s): 2
Strategic Objective(s): 2.1, 2.2
Budget Decision Unit(s): All

Organizational Programs: Counterterrorism

Program Increase: Positions 43 Agt 20 FTE 22 Dollars $12,962,000 ($1,090,000 non-personnel)

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

Item Name: **Counterintelligence**

Strategic Goal(s): 2
Strategic Objective(s): 2.1
Budget Decision Unit(s): All

Organizational Programs: Counterintelligence

Program Increase: Positions 30 Agt 0 FTE 16 Dollars $4,466,000 ($478,000 non-personnel)

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

Item Name:	**Cybersecurity**
Strategic Goal:	2
Strategic Objective:	2.4
Budget Decision Unit(s):	All
Organizational Program:	Information Technology Infrastructure, Office of the Chief Information Officer

Program Increase: Positions 4 Agt/Atty 1 FTE 2 Dollars $27,219,000 ($26,395,000 non-personnel)

Description of Item

Over the past decade, several highly publicized breaches of systems and data, including a cyber incident involving one of the FBI's own systems as recently as February 2023, have exposed cybersecurity vulnerabilities in government networks and information systems. Threat actors, including cyber criminals and nation-state sponsored actors, have become more persistent and increasingly successful in penetrating our perimeter defenses and escalating privileges on government information systems to inflict harm to our national security.

Addressing the threats posed by cyber adversaries to the FBI is further complicated by the diverse numbers and types of networks the Bureau operates. The sensitivity of the information processed makes these networks prime targets for cyber-hackers. Over the past two years, the FBI has seen an increase in cybersecurity incidents and has discovered aging software and hardware components within critical segments of the IT infrastructure, leaving it susceptible to these types of threats. The FBI must centrally manage access to FBI resources —data, systems, devices, and networks— to protect sensitive information and national security operations from cybersecurity threats.

Cybersecurity Executive Order (EO) 14023 and National Security Memorandum-8 require the FBI to harden its networks, access controls, and system security through adoption of a Zero Trust Architecture (ZTA). Zero Trust addresses the shortcomings of past cybersecurity approaches to secure a modernized, cloud-based, and increasingly mobile information infrastructure being continuously targeted by adversaries. This will include the adoption of robust access controls, supply chain risk management program management, and cloud migration management. The resources requested will further enable the FBI to bolster its cybersecurity capabilities and address these requirements.

Justification

Zero Trust - Access management: 2 positions and $16,466,000 million ($16,200,000 non-personnel)

The FBI currently relies on a complex array of siloed manual processes and non-authoritative, duplicative, access control lists to control user accesses to individual systems and devices on its networks. With these funds, the FBI will replace the manual methods by procuring robust, standardized, access management software capabilities which utilize individual user identities to control user accesses to FBI resources, such as facilities, systems, networks, applications, and

devices. The software solution will manage the full lifecycle for each user's access to a resource. This begins with the submission of an initial request for access and the granting of access (if appropriate) through the periodic recertification, timely removal, and archival of any accounts when a user's role, organization, or need for access changes - or when the user leaves the FBI. The funds will also enable modification of FBI systems to leverage these enterprise access management services for purposes including multifactor authentication in lieu of their various system-specific access management solutions operating today. The access management capabilities will enable explicit verification of every access request at a secure, trusted level as well as improved auditing for detection of potential insider threats. Without them, the FBI will be unable to limit access to critical mission data to only those authorized to see it or to fully close the risks of large data breaches due to mistaken, perpetual maintenance of some user accounts.

The FBI requests one (1) Information Technology Specialist (ITS) to serve as a subject matter expert and one (1) professional support position to provide program management. Each time a system onboards to the enterprise service provider for access management, there is a technical conversation and project management plan to be initiated. These individuals will ensure onboarding happens in a coordinated manner and is adapted to the technical configuration of the specific system. They will also help facilitate that interaction between systems and the service provider.

Zero Trust - Privileged Access Management: $5,700,0000 ($5,700,000 non-personnel)

The FBI will obtain software capabilities to complement the access management solution to provide a more robust set of tools to monitor and control the accesses of FBI privileged users, such as network, database, and system administrators. These users can manipulate the IT security perimeter and therefore inadvertently or deliberately cause the most damage to the FBI cybersecurity posture. The solution's components will vault privileged user credentials, help prevent account takeovers, issue derived and time-limited credentials, and record and transmit privileged actions for advanced analytics. These capabilities will significantly enhance FBI abilities to identify privileged users and will enable the Bureau to track and monitor activities much more closely - a necessity to help ensure future protection against vulnerabilities contributing to cybersecurity incidents.

Zero Trust - Supply Chain Risk Management (SCRM) Program Management: 2 Positions (1 Special Agent) and $2,158,000 ($1,600,000 non-personnel)

Any time a product’s supply chain is compromised, its security can no longer be trusted. Understanding supply chain risk in a continuous way requires an investment in tools and resources to move the FBI’s supply chain risk management program from a reactive to a proactive state. Currently, the FBI reviews supply chain risk at the point of procurement but does not continue assessing risk throughout the product lifecycle. The FBI completed 11,482 procurement risk assessments from April 2020 through March 2022 and completed 2,248 product vulnerability assessments from January 2021 through March 2022. To move these assessments from a static position to a continuous monitoring posture, the FBI must procure tools which aid in the continuous monitoring of third-party risks. In the current maturity of SCRM tools, it is also necessary for the FBI to procure a tool for upstream supply chain analysis. These two (2) tools working together will allow for a holistic view of a supplier/manufacturer, as well as highlight potential areas where the FBI may be getting counterfeit or "white labeled" products. The tools will also complete vendor risk evaluations, prioritize critical assets, and verify supplier security culture. To fully utilize the requested tools and move to a more proactive

and continuous monitoring program, the SCRM team requires contract analysts in addition to the existing security architect staff. These additional positions would conduct business analysis with the aforementioned tools, and through other research, determine technical and threat analysis related to the FBI IT supply chain.

To ensure strategy and policy changes do not cause adverse effects on mission and to better incorporate FBI intelligence, one (1) Special Agent position is requested to create a more direct link for intelligence and information sharing with operational divisions. This Agent position will also represent the field operations mission set and opinion to HQ by maintaining a network with other Agents remaining in the Field Offices. SCRM information sharing within the government is also required by the both the ICD 731 and CNSS 505. The one (1) requested support IT Specialist position will allow for the direct accomplishment of these goals via intergovernmental working groups, repositories, and participation with the Federal Acquisition Security Counsel.

Zero Trust - Secure Cloud Migration: $2,895,000 ($2,895,000 non-personnel)

Effective use of cloud infrastructure is a required element of success for the FBI as it adopts a ZTA. Moreover, Section 3 of EO 14028 requires the FBI to "accelerate movement to secure cloud services," and to "update existing agency plans to prioritize resources for the adoption and use of cloud technology…". This federal government mandate recognizes cloud infrastructures can provide immediate and effective capabilities to help FBI system owners advance their ZTA posture. The FBI operates in a multi-cloud environment and requires a centralized group of experts to provide secure pathways and assess best cloud environment for any systems workload. Once assessed and moved to cloud infrastructures, systems will inherit significant and standard ZTA benefits including, but not limited to, the use of Multi Factor Authentication (Identity Pillar), managed access (Network/Environment Pillar), centralized logging (Network/Environment Pillar), data encryption at rest (Data Pillar), and data encryption in transit (Data Pillar). The FBI requests $2,895,000 to efficiently transition the highest priority systems to commercial cloud infrastructure. Establishing this fund will help enable the FBI to ensure priority systems ready for the cloud will be migrated and inherit greater ZTA effectiveness and compliance.

Impact on Performance

The global cybersecurity environment has never been more dynamic or complex. The volume, speed, and complexity of computing technologies continues to evolve, and with it, so must the FBI investment in effective Cybersecurity technologies. With these enhancements to address engineering requirements for the cybersecurity assets the FBI maintains, the monitoring and analysis deployed to maintain and protect sensitive data on all FBI asset inventory will improve.

The FBI must continue to invest in 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 2022 Enacted				FY 2023 Enacted				FY 2024 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
147	3	118	$102,951	155	5	127	$119,717	155	5	127	$122,941

2. Personnel Increase Cost Summary

Type of Position/Series	FY 2024 Request ($000)	Positions Requested	Full Year Modular Cost per Position ($000)	Annualizations ($000)			
				2nd Year	3rd Year	FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
Information Technology	$256	2	$200	$70	$57	$140	$114
Professional Support	$138	1	$195	$32	$82	$32	$82
Special Agent, Field	$430	1	$518	($82)	$113	($82)	$113
Total Personnel	**$823**	**4**	**$913**	**$20**	**$252**	**$90**	**$309**

3. Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	FY 2024 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
Information Technology (IT) Consulting	$26,395	N/A	N/A	$0	$0
Total Non-Personnel	**$26,395**	**N/A**	**N/A**	**$0**	**$0**

4. Justification for Non-Personnel Annualizations

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. This request represents project development that requires multi-year scope implementation. Once the implementation is complete, the associated contractor funding will be needed year over year to transition the expanded infrastructure into operation and maintenance support.

5. Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
Current Services	155	5	127	$27,973	$94,968	$122,941	N/A	N/A
Increases	4	1	2	$823	$26,395	$27,219	$90	$309
Grand Total	**159**	**6**	**129**	**$28,796**	**$121,363**	**$150,159**	**$90**	**$309**

6. Affected Crosscuts

- Cyber, Intelligence & Information Sharing, and National Security.

7. Current Services and Enhancement Funding Categorized by Cyber BDR 22-39

NIST Framework Function	Funding Amount ($000)
Detect	$4,785
Identify	$35,420
Protect	$82,869
Recover	$9,628
Respond	$1,972
M-22-16	$15,486
Grand Total	**$150,159**

Item Name: **Violent Crime**

Strategic Goal: 2, 3, 4
Strategic Objective: 2.3, 2.4, 2.5, 3.2
Budget Decision Unit(s): All

Organizational Program: Criminal Investigative Division, Criminal Justice Information Services, Critical Incident Response

Program Increase: Positions 44 Agt/Atty 15 FTE 23 Dollars $14,862,000 ($5,000,000 non-personnel)

Description of Item

The FBI strives to provides a critical service in ensuring the country's safety from those who choose to exercise their Second Amendment Rights and protecting the country's most vulnerable persons, children. Thus, the FBI requests the following resources to strengthen national criminal background check and significantly expand efforts to deter criminal acts against children:

- **National Instant Criminal Background Check System:** The FBI requests 27 positions and $8,433,000 ($5,000,000 non-personnel) to support the statutorily required firearm background checks.
- **Combatting Crimes Against Children and Human Trafficking:** The FBI requests 14 positions and $5,140,000 (all personnel) to develop a Crimes Against Children Unit (CACU) for the East and West regions of the United States, enhance Resiliency and Safeguarding Resources, and increase the Child Exploitation Operational Unit's (CEOU) operational Special Agent staffing. These efforts are in response to the recent Nassar investigation findings and will address operational and policy needs of the FBI field offices. Additionally, the FBI requests 3 positions and $1,289,000 (all personnel) to be devoted to the FBI's Human Trafficking Program (HTP). This will support the DOJ National Strategy to Combat Human Trafficking and further align resources to collaborate with the Department and other agencies to craft guidance for FBI field offices, while outlining best practices for victim-centered, trauma-informed, culturally responsive operations.

Justification

National Instant Criminal Background Check System: 27 positions (1 SA) and $8,433,000 ($5,000,000 non-personnel)

The National Instant Criminal Background Check System (NICS) Section serves a critical role 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. To meet this mission, the NICS Section must have sufficient resources to meet its no-fail mission.

The FBI was appropriated $100 million (no-year funds), in FY 2022, as part of the Bipartisan Safer Communities Act (BSCA) to meet additional resource needs of the FBI Criminal Justice Information Services Division's NICS Section. This funding is supporting 170 additional

positions and key Information Technology (IT) investments. Additional positions are being leveraged to support two major Federal directives (the NICS Denial Notification Act and the BSCA) while supporting a transaction volume that was 19 percent higher than pre-pandemic years.

Further, the NICS is in the early stages of implementing multiple processing changes to support the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) regulation changes and is expecting a consequential growth rate of 8 percent in FY 2023 over pre-pandemic years.

In order for NICS to continue to meet emerging critical public safety mandates, the NICS will need additional resources as requested in FY 2024, in addition to the annualization of the 170 positions funded by the BSCA. The 27 additional positions requested with this enhancement will strengthen the program's ability to complete anticipated increased transaction volume because of the new ATF Final Rule 2021R-08F. This Final Rule was not considered when additional NICS resources were requested as part of the BSCA or funded in the FY 2023 appropriations bill. These positions are also critical to support unanticipated processing challenges relating to the BSCA which were not considered when staffing estimates were provided in response to potential impacts of the BSCA.

The ATF Final Rule 2021R-08F entitled "Factoring Criteria for Firearms with Attached 'Stabilizing Braces'" seeks, to ". . . clarify when a rifle is designed and intended to be fired from the shoulder . . .." The adoption of this Rule will result in impacts to the NICS Section because it it will increase the number of NICS background checks associated with each NFA license issuance on behalf of ATF. This Rule notes ATF has estimated that nearly three million shoulder mounted braces are in circulation nationwide and conservatively estimates 1.2 million NFA checks will be added to the current volume in FY 2023. The NICS Section notes that, as a result of this clarification, items that meet this updated definition may have been previously sold by non-FFLs (including those via the Internet) and will now require an individual to be licensed under NFA prior to possessing such a device. Therefore, the FBI predicts that the amount of NFA checks received and processed annually will permanently increase. It is anticipated eight additional personnel will be needed to process these NFA checks.

In addition to the new background check volume created by the ATF regulation changes, the provisions of the BSCA continues to move forward with implementation. The full impact to processing times and personnel required to complete unprecedented transactions is still under evaluation. Since national roll-out to local agencies for U21 checks, the NICS has received only a 13% local agency response rate and 40% State response rate. NICS now recognizes that U21 background checks are more labor intensive than originally estimated. Additional personnel are needed to conduct direct outreach to local agencies who are unresponsive to NICS requests. Without the FY 2024 enhancement, NICS will need to divert resources from traditional NICS background checks to support the U21 local agency reach out. Based on the volume and processing time of the local agency follow up, the NICS anticipates an additional 18 personnel would be needed for U21 background checks that could be proceeded after the 10th day without a State or local agency response.

Based on these increases and increased correspondence with field offices, the FBI is requesting an additional Special Agent (SA) to support critical law enforcement and FBI collaboration. The SA will assist the NICS Business and Liaison Unit with field office and local law enforcement outreach in terms of NICS capabilities and gaps that are identified from the field. The SA will attend field office briefings and consult with other SAs and Supervisory Special Agents (SSA)

regarding specific case needs and overarching division goals. The SA will provide support to the NICS Alert Service (NAS) team in streamlining their process and creating products that are more accessible to the field offices. The NAS allows FBI field offices and the ATF to submit qualified biographic information to the NICS Section to request enrollment. Once approved, the biographic information in the NICS audit log is reviewed to determine if the subject of interest (SOI) had any previous NICS background checks, and then monitored day one forward for a specific period (30, 60, 90, or 180 days) to determine if the SOI is the subject of a new NICS-related background check. The SA will also serve as a consultant on various projects including the U21 outreach program.

In addition to the personnel requests in this enhancement, NICS is requesting a non-personnel enhancement of $5,000,000 to sustain system development. The NICS reprioritized the list of system enhancements to ensure successful implementation of BSCA requirements. The reprioritization delayed other system enhancements relating to automation efforts. The NICS development effort utilizes an agile development methodology prioritizing requirements to resolve known or discovered operational system defects. The prioritization is reevaluated upon identification of new system requirements during program increment planning sessions. Priority changes are driven by newly identified system vulnerabilities or defects and changes in the operational environment such as changes in gun laws, new congressional mandates, and new executive orders. The continued success of the NICS is dependent on system enhancements and future development which will provide increased system availability and automate the NICS transaction life-cycle process. Efficiencies will be gained by reducing system/software redeliveries and having complete interoperability with NICS partners and agencies. Of the total NICS request, $5,000,000 will support a team of developers with the capacity to do a set amount of work at a steady velocity.

Combatting Crimes Against Children: 17 positions (14 SAs) and $6,429,000 (all personnel)

Crimes Against Children 14 positions (11 SAs) $5,140,000 (all personnel)

In response to the recent Larry Nassar investigation findings, the FBI plans to develop a Crimes Against Children Unit (CACU) for East (E) and West (W) regions of the United States to be housed at FBI headquarters, enhance Resiliency and Safeguarding Resources, and increase the Child Exploitation Operational Unit's (CEOU) Special Agent staffing.

Specific to the Office of the Inspector General's (OIG's) recommendations, developing the program management and training structure will better enable the FBI to follow those recommendations. To effectively respond to FBI and OIG findings from the Nassar Investigation, the headquarters regional program management units CACU-E and CACU-W will be created to address the operational and policy needs of FBI field offices outlining best practices for victim-centered, trauma-informed, culturally responsive operations and to support national operational investigations. The creation of the headquarters regional program management units will afford the FBI the ability to provide more resources to the field and have more visibility and control of active investigations. New Resiliency and Safeguarding Resources will be created to address the loss of safeguarding for all non-undercover employee (UCE) and non-online covert employee (OCE) Crimes Against Children and Human Trafficking employees, which will promote resiliency and longevity in the violation.

Lastly, positions will be assigned to enhance CEOU and strengthen its ability to coordinate large-scale national and international investigations spanning multiple FBI offices commonly too resource intensive to be managed at the field level. CEOU often coordinates and assists with the execution of large-scale national and international investigations. For example, an ongoing initiative resulted in CEOU identifying, creating, and distributing hundreds of targeting packages and leads for subjects all over the world who are using enhanced sophisticated techniques to hide their identity. This large operation has already resulted in the disruption of numerous Crimes Against Children (CAC) offenders. An impactful investigation of this size and complexity would not be feasible for a single field office to coordinate and execute, with its already limited CAC resources.

The FBI's Combatting Crimes Against Children program will primarily address the following five major crimes with the additional 11 Special Agents, 2 Management and Program Analysts (MAPA), and 1 Psychologist:

1. Child Abductions
    a. A child abduction or the mysterious disappearance of a minor, especially a child of tender years (12 years of age or younger), under circumstances that suggest involuntariness, abduction, and the like, requires an immediate response by the FBI, regardless of how the case comes to the attention of FBI personnel (e.g., media reports, police requests for assistance, family notifications, or otherwise). Of the children who are abducted and killed each year in the United States, the majority are murdered within a few hours of being abducted. Because of this, the FBI considers all mysterious disappearances of children of tender years as stranger abductions until investigations into those disappearances determine otherwise. For this reason, rapid deployment of investigative resources upon notification of a mysterious disappearance may enhance the odds of recovering the victim alive and may facilitate the identification and arrest of the offender, thereby preventing others from becoming victims. When a child abduction occurs, the FBI must support local authorities with various resources and be actively involved, should federal kidnapping jurisdiction be established.
    The Child Abduction Rapid Deployment (CARD) Team often responds to child abductions and is an effective force multiplier utilized to safely recover child victims. The CARD Team is designed to deploy FBIHQ and FBI field office investigative and intelligence personnel with proven experience in child-abduction matters as a rapid, on-site response. This team provides investigative, technical, and resource assistance during the most critical period following a child abduction.
2. Contact Offenses Against Children
    a. Three of the most resource-intensive contact offenses against children investigated by the CAC Program are the Production of Child Sexual Abuse Material (CSAM), Sextortion, and Traveler/Enticement offenses. CSAM Production investigations typically involve child sexual exploitation through high-technology services and often involve ongoing victimization which place victims in imminent and continuous danger. Sextortion occurs when an adult, through threat or manipulation, coerces a minor into producing a sexually explicit visual depiction and sending it over the Internet. Traveler/Enticement investigations involve offenders who attempt to meet minors for the purpose of sexual exploitation or who entice minors to travel for sexual purposes represent serious threats to children.
3. Sexual Exploitation of Children Enterprises

a. Investigations conducted into Sexual Exploitation of Children Enterprises involve the disruption and dismantlement of online groups, organizations, and for-profit enterprises whose focus is the sexual exploitation of children. Subjects of these investigations use the internet to share CSAM and/or to profit from it, to communicate with other sex offenders, and to further the sexual exploitation of children. These complex, multijurisdictional, multisubject investigations represent crimes the FBI must address domestically and internationally. The requested FY 2024 resources will enable our Child Exploitation Operational Unit (CEOU) to obtain the newest technological resources and additional personnel to investigate the most complex enterprises domestically and internationally. As technology rapidly advances, it continues to get more difficult to investigate these matters because the FBI does not have the most updated technology.

4. Transportation of CSAM
    a. Investigations conducted into the transportation of CSAM involve combatting the trading and distribution of images and videos depicting the sexual abuse of children. Case analysis, research, and experience have shown some of the most prolific abusers of children are first investigated solely based upon a complaint or a lead regarding possession and/or distribution of CSAM.
5. International Parental Kidnapping (IPK)
    a. IPK, whether because of an individual taking or wrongfully retaining a child(ren) with the intent to obstruct the lawful exercise of parental rights, merits the full and timely attention of law enforcement. The child should be considered in danger, especially when the person taking or retaining the child has previously threatened to abduct or harm the child, has threatened to harm himself or herself, or is otherwise unstable.

The graphic nature of the CAC violation can sometimes have a severely negative impact on the mental health and psychological well-being of the personnel assigned to investigate these matters. Repeated exposure to CSAM can affect an employee's life at work and home. The addition of Resiliency and Safeguarding Resources will protect the safety, security, and psychological well-being of FBI personnel investigating child exploitation matters as well as non-FBI child exploitation task force members working on task force related matters in furtherance of the investigative programs and priorities of the CAC Program.

CEOU is an essential part in the mitigation of the CAC threat. This highly sophisticated, technologically advanced unit employs a comprehensive approach to address prioritized child exploitation threat vectors. By conducting proactive, intelligence-led initiatives, including platform undercover operations, CEOU disrupts and dismantles criminal enterprises and the criminal activities of the most egregious individual offenders involved in the exploitation of children. The requested enhancement to CEOU will strengthen its ability to develop tools and technical expertise to provide substantial assistance in CAC investigations and coordinate large-scale international investigations through the Violent Crimes Against Children International Task Force (VCACITF) and international law enforcement partners to identify and promulgate best practices and effective and efficient investigative strategies. Investigations of this magnitude are often too overwhelming and resource intensive to be managed in the field.

Human Trafficking 3 positions (3 SAs) $1,289,000 (all personnel):

The additional 3 SAs will be devoted to the FBI's Human Trafficking Program (HTP) in support of DOJ's Human Trafficking Strategy and to collaborate with the DOJ and other agencies to

craft guidance for FBI field offices outlining best practices for victim-centered, trauma-informed, culturally responsive operations and to support national investigations. Through operational and program management support, these (3) SA positions will allow the FBI to meet its commitment to the National Action Plan to Combat Human Trafficking and DOJ Human Trafficking Strategy recommendations, which seek to enhance the department's capacity to prevent human trafficking, prosecute human trafficking cases, and support and protect human trafficking victims and survivors.

The Human Trafficking (HT) subprogram of the Crime Against Children / Human Trafficking Program covers two categories: (1) sex trafficking and (2) labor trafficking. The HT subprogram includes investigating crimes with a domestic or foreign nexus, as well as both adult and minor victims. Sex trafficking is the recruitment, harboring, transportation, provision, or obtaining of an individual who, under force, fraud, or coercion, is induced to perform a commercial sex act. Sex trafficking investigations can involve a U.S. Person (USPER) or non-USPER victim or both. The FBI must investigate allegations of sex trafficking regardless of victims' nationalities. Labor trafficking occurs when persons, both USPERs and non-USPERs, are compelled to perform labor or services using force, threats of force, physical restraint, or threats of physical restraint; serious harm or threats of serious harm; abuse or threatened abuse of law or legal process; or coercion.

The sex trafficking of minors (STM) is one of the most complex forms of child sexual exploitation. Offender's target and lure vulnerable children to engage in sex trafficking activities and other forms of sexual exploitation by using manipulation, drugs, and violence. Once a trafficker gains control over a child, he or she often uses acts of violence, intimidation, or psychological manipulation to keep the child in a life of sex trafficking. STM investigations fall under the Innocence Lost National Initiative (ILNI), which is supported by the Department of Justice and the National Center for Missing & Exploited Children (NCMEC). ILNI was implemented in 2003 to address the problem of children being recruited and/or forced into commercial sex.

Both domestic and international adult and minor HT investigations are largely resource-intensive and require a substantial amount of financial and personnel resources from both FBIHQ and the field to adequately mitigate the threat. One of the biggest challenges to overcome concerning HT is technology. Advances in technology have made it easier for traffickers to target, recruit, and exploit trafficking victims throughout the world without detection. Human traffickers conduct business operations easily due to an increase in online monetary exchanges and anonymizing software.

On January 31, 2022, Attorney General Garland announced the DOJ multi-year National Strategy pursuant to the Justice for Victims of Trafficking Act, 34 USC 20711(a). The DOJ National Strategy is rooted in the interagency National Action Plan to Combat Human Trafficking, which President Biden released on December 2, 2021. The DOJ National Strategy seeks to enhance the Department's capacity to prevent human trafficking, prosecute human trafficking cases, and support and protect human trafficking victims and survivors. The DOJ National Strategy will be implemented under the direction of the National Human Trafficking Coordinator designated by the Attorney General.

As a result of the DOJ National Strategy, the FBI is responsible, either alone or in coordination with other agencies, for numerous tasks, which include:

- Developing and delivering human trafficking training modules

- Providing human trafficking training to Federal Agents and Prosecutors
- Developing DOJ Human Trafficking Victim Screening Protocol
- Establishing District-Level Forced Labor Trafficking Team and participating in the district selection process to increase forced labor investigations
- Developing and adopting a protocol to consistently refer cases to state, local, tribal partners

The positions and resources requested for CAC and HT will enable the FBI to be compliant with the OIG's recommendations and ensure the necessary training and case management are provided for these critical investigative programs.

Impact on Performance

The additional resources for NICS will assist in reducing the amount of firearm background checks that are not processed until the third business day and help to minimize the number of firearm sales to prohibited persons.

Individuals who prey on children continue to exploit them through both hands-on offenses and the production and distribution of CSAM with other like-minded offenders. Child exploitation continues to proliferate, threatening public health, safety, and the future of our children. Every year, thousands of children become victims of crimes—whether it's through kidnappings, violent attacks, sexual abuse, or online predators. This funding will provide resource allocation to the highest priority units to show the unwavering commitment to ensuring that all children in America are able to reach their potential in a nation that protects them from violence and abuse. With these resources, the FBI will advance its efforts to identify and mitigate the human trafficking threat posed by criminal actors and organizations who obfuscate their illicit activities through technology.

Funding

1. Base Funding

FY 2022 Enacted				FY 2023 Enacted				FY 2024 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
953	22	905	$124,206	1,001	27	1,130	$152,978	1,169	29	1,167	$200,726

2. Personnel Increase Cost Summary

Type of Position/Series	FY 2024 Request ($000)	Positions Requested	Full Year Modular Cost per Position ($000)	Annualizations ($000)			
				2nd Year	3rd Year	FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
Clerical	$205	2	$146	$25	$55	$49	$110
Information Technology	$256	2	$200	$70	$57	$140	$114
Professional Support	$689	5	$195	$32	$82	$161	$410
Special Agent, Field	$6,445	15	$518	($82)	113	($1,230)	$1,695
NICS/NTOC	$2,267	20	$158	$15	$50	$299	$1,000
Total Personnel	**$9,862**	**44**	**$1,217**	**$60**	**$357**	**($581)**	**$3,329**

3. Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	FY 2024 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
Advisory and Assistance Services	$5,000	N/A	N/A	$0	$0
Total Non-Personnel	**$5,000**			**$0**	**$0**

4. Justification for Non-Personnel Annualizations

The FBI requests these annualizations to pursue the out-year costs for the Violent Crime mission. This enhancement allows the FBI to increase the capabilities needed to deter, discover, and dismantle violent crime actors and threats. The FBI requests that the non-personnel costs fully recur.

5. Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
Current Services	1,169	29	1,167	$138,231	$62,495	$200,726	N/A	N/A
Increases	44	15	23	$9,862	$5,000	$14,862	($581)	$3,329
Grand Total	**1,213**	**44**	**1,190**	**$148,093**	**$67,495**	**$215,588**	**($581)**	**$3,329**

6. Affected Crosscuts

- Violent Crimes, Crimes Against Children, Mass Violence, Gun Safety, and Human Trafficking.

Item Name: **DNA**

Strategic Goal: 1, 2, 3, 4
Strategic Objective: 1.2, 2.1, 2.2, 2.3, 2.4., 2.5, 2.6, 3.1, 3.2, 4.2
Budget Decision Unit(s): All

Organizational Program: Finance and Facilities, Laboratory

Program Increase: Positions 7 Agt/Atty 0 FTE 4 Dollars $53,117,000 ($51,869,000 non-personnel)

Description of Item

The FBI requests seven (7) positions and $53,117,000 ($51,869,000 non-personnel) to effectively address the increase in DNA collections resulting from the amended rule within U.S. Code (in 34 U.S.C. § 40702(a)(1)(A) and (B)), to appropriately allow the FBI to implement the Rapid DNA standards and procedures as required by the Rapid DNA Act of 2017, and to re-architect the current Combined DNA Index System (CODIS) software application to a modern, cloud-based application.

Justification

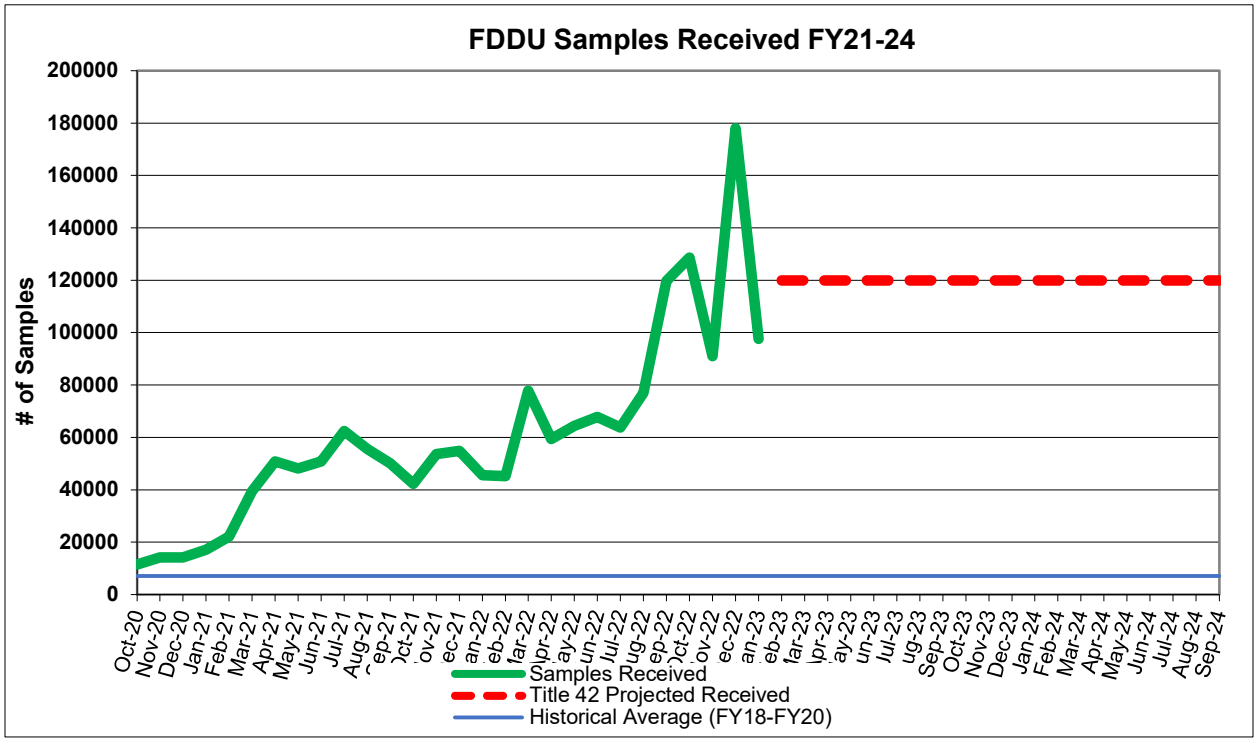
The FBI plays a critical role in protecting the U.S. from threats to public safety. Fulfilling this role requires the FBI to process DNA samples in a timely manner and to further develop advanced methods and technologies to detect and prevent threats to public safety. Investment in additional DNA expansion capabilities and technology is critical to maintaining and enhancing the FBI's ability to address emerging threats and help mission critical information reach partners and investigators in an expeditious manner.

Legislatively Mandated DNA Expansions: 7 positions and $37,817,000 ($36,569,000 non-personnel)

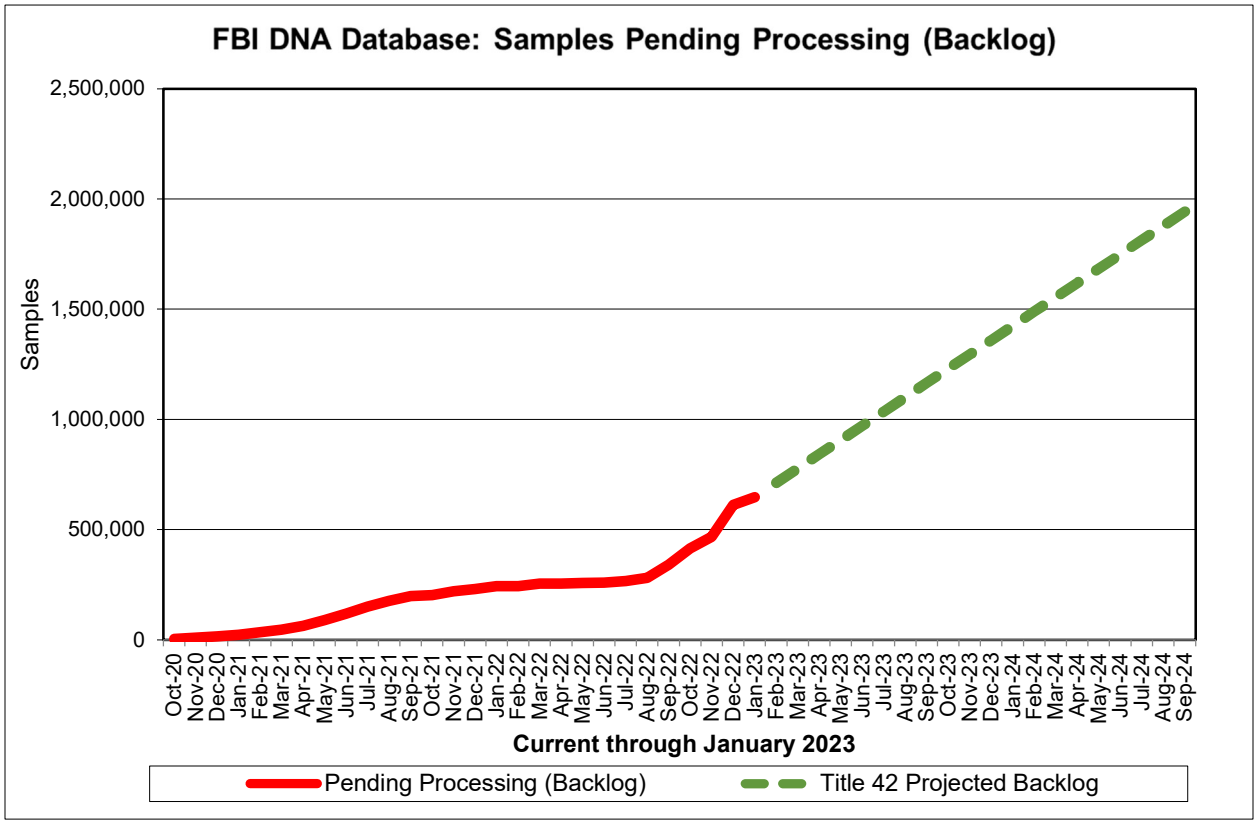
DHS Related DNA Collections: 3 positions and $28,716,000 ($28,019,000 non-personnel)

The FBI requests additional funding to process and enter the increased number of genetic profiles into CODIS per its mandate in the DNA Identification Act of 2005. Due to the Department of Homeland Security (DHS) DNA collection expansion in April 2020, the FBI began receiving between approximately 50,000 to 60,000 DNA samples per month (7x historical sample volume) which continued in FY 2022. The substantial increase has created massive budget and personnel shortfalls for the FBI. Prior to the DHS DNA expansion, the FBI dedicated approximately $7M annually to DNA databasing efforts, but this initial expansion created a budgetary shortfall of $22.5M in FY 2021. The volume of samples is dependent on the future of Title 42 or similar policies which change how DHS may detain or remove non-US persons. When Title 42 ends, the FBI anticipates an additional 50,000 samples per month due to increased DHS detentions. This will eventually bring the total monthly samples received to approximately 120,000 (~1,440,000 samples per year). The FY 2023 budget of approximately $15M, which includes the FY 2023 enhancement of $8M for DNA databasing, only allows for approximately 423,000 samples to be processed ($35.44 per sample cost in FY 2022). The FBI anticipates receiving between 1.2M and 1.5M samples per year in future fiscal years; $27,539,000 of the

non-personnel request aids the FBI in covering costs associated with processing an additional 777,000 samples as well as provides enhancements to the processing infrastructure.



Note: The spike in received samples in December 2022 was a result of a computer outage at the end of November 2022, which delayed input of received samples.



The FY 2023 funding is inadequate to meet the incoming sample volume that will be received in FY 2024 and future years. The FBI will need to maintain the additional contract personnel, supplies, and DNA collection kits to effectively support the anticipated 100,000 samples per month. The FBI also requests $480,000 in non-personnel funding to continually add high-density storage solutions year over year to accommodate the increased submission level. To maintain efficiency and avoid critical failures in processing, the FBI will need to regularly replace DNA databasing instrumentation that is nearing end-of-life. The $700,000 in personnel funding will fund two (2) Professional Support positions and one (1) Forensic Examiner.

The FBI estimates thousands of unsolved crimes could be resolved by DHS DNA collections and has coordinated with DOJ to plan for the impact of fully implemented DNA collections. The FBI has been working with DHS component agencies, building automated and streamlined workflows to minimize costs and administrative efforts for both agencies. Despite efforts to efficiently process the increased volume of samples, a backlog of approximately 650,000 samples has developed. Without additional funding, the backlog will continue to grow and the entry of DNA profiles into CODIS will be severely delayed, increasing the likelihood of arrestees and non-U.S. detainees being released before identification through investigative leads. Additionally, the inability to enter profiles into CODIS degrades the trust and partnerships established with the FBI's law enforcement customers. Without the ability to provide DNA collection kits or process collected DNA samples, submitting Federal Agencies will not continue to support these critical biometric collections. This would mean fewer CODIS leads produced, less intelligence generated, and a reduction in overall public safety.

The FBI is requesting additional funding to effectively support the demand of laboratory processing due to the increased sample intake, to begin eliminating the backlog, and to successfully deliver on legislative requirements. By doing so, the FBI can continue to provide 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 of processing DNA samples across the USG.

Shipping Contract: $4,500,000 (all non-personnel)

The large increase in DNA samples collected has also resulted in substantial shipping costs which are borne by the FBI. The additional 60,000 samples-per month, or additional 720,000 per year, have a current per unit shipping cost of $6.25. This results in $375,000 monthly funding requirement or $4,500,000 required annually.

Rapid DNA: 4 positions and $4,601,000 ($4,050,000 non-personnel)

The FBI is also required to act on the implementation of 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 instrument/device, query that profile immediately against unsolved crimes of special concern in the national DNA database within CODIS, and return the results within minutes, allowing for the immediate detention of these individuals. As stated in Sec. 2(b) of the Rapid DNA Act, the FBI is required to provide oversight of Rapid DNA technologies and capabilities. As the lead agency for Rapid DNA, it is essential that the FBI fund the implementation of Rapid DNA in FBI field office locations as well as the staffing needed to provide mandated oversight of the program. This request is for staffing and funds to implement and sustain the FBI's Rapid DNA program.

The ability to successfully implement Rapid DNA in booking stations requires considerable planning and training. The FBI Laboratory receives approximately 6,500 arrestee samples per year from 300 plus FBI booking locations. There are currently 24 FBI booking locations that submit between 75 and 250 arrestee samples per year, totaling approximately 50% of all FBI arrestee submissions. These 24 locations are ideal candidates to implement Rapid DNA due to their high volume of arrestee submissions. This enhancement will enable the FBI to implement its Rapid program in a scaled manner to at least six FBI Field Office booking stations per year until it reaches a maximum of 24 field office booking locations. As more booking locations are added, funding will be shifted to service agreements and supplies to support the deployed instrumentation. Once the maximum is reached, all funds will be used for supplies, instrument service agreements, and instrument replacement. To ensure the accuracy of systems, processes, and data, this request also includes travel costs for audit services. The FY 2024 enhancement request outlined here will expand on the FBI's Rapid DNA implementation capabilities.

As the lead agency for Rapid DNA implementation referenced above, the FBI has oversight responsibilities for agencies implementing the Rapid DNA technology both inside and outside the FBI's purview. The personnel enhancement request is for three (3) auditors and one (1) Rapid booking station program manager. The auditors would be responsible for oversight outside the FBI by auditing the State CODIS agencies involved in implementing Rapid DNA for their respective state and ensures the Rapid DNA program is being operated in an authorized manner. These auditors would also assist the Rapid booking station program manager with implementation, training, and annual audits of FBI booking facilities as required by the Standards for the Operation of Rapid DNA Booking Systems by Law Enforcement Booking Agencies. State CODIS Agencies are responsible for auditing local and municipal sites within their state. Audits of select local or municipal sites may be needed to ensure the state is correctly enforcing the policy requirements. These auditors will need to visit each state within the first year of implementation and operation and a minimum of every three years thereafter, to ensure compliance with the FBI's Standards for the Operation of Rapid DNA Booking Systems by Law Enforcement Booking Agencies and National Rapid DNA Booking Operational Procedures Manual. The Rapid booking station program manager would be responsible for oversight of Rapid DNA within the FBI by managing the FBI's implementation of Rapid DNA at FBI booking facilities, to include training booking personnel, managing annual auditing of FBI booking facilities, instrument installation, as well as reagent and supply management.

Combined DNA Index System (CODIS) Cloud Development: $15,300,000 (all non-personnel)

The FBI requests $15,300,000 (all non-personnel) for the re-architecture of the current CODIS software application to a modernized, cloud-based application. Modernizing the application is critical to increasing its efficiency, improving the maintainability of the application, reducing downtime, and hardening its security posture in accordance with Executive Order 14028 (issued May 21, 2021). The cloud version would serve as a single application accessible to all federal, state, and local law enforcement agencies participating in the National DNA Index System (NDIS). Under Section 3 of EO 14028, Modernizing Federal Government Cybersecurity, "The Federal Government must… accelerate movement to secure cloud services, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS)…"

The CODIS software has been in service for approximately 30 years. In that time, there have been two distinct generations of the software. The first was in use for approximately 20 years

while the second and current generation, is approximately 10 years old. This enhancement would allow the FBI to retire the current generation of CODIS after approximately 20 years of use and move to a more stable, reliable, efficient, and secured platform.

Transitioning CODIS to the cloud is necessary to ensure the application continues to meet the ever-evolving needs of its stakeholders well into the future. The current client-server architecture lacks the flexibility to evolve at a rapid rate, requires substantial deployment periods to upgrade each agency, and is comprised of an aging code base that is complex to maintain and enhance. Transitioning to a cloud-based version will allow the software to comply with EO 14028 and meet the ever-changing cybersecurity requirements of the White House, DOJ, and the FBI's Office of the Chief Information Officer (OCIO).

Impact on Performance

Statutory requirements and recent regulatory changes have significantly expanded the DNA processing requirements of the FBI. Expanded collection by DHS has a substantial impact on the FBI's ability to process and add these samples to CODIS in a timely manner, resulting in a sizable backlog of ~650,000 samples from all federal law enforcement agencies. With additional funding, the FBI will be able to process the increased sample volume, leading to significant improvements in investigative leads and public safety.

The FBI is also required to provide oversight of Rapid DNA technologies and capabilities. As the lead agency for Rapid DNA, it is critical that the FBI fund the implementation of Rapid DNA in FBI field office locations as well as provide mandated oversight of the program. With additional funding and staffing for Rapid DNA, the FBI can complete the implementation and oversight responsibilities of the Rapid DNA Act. This requirement is integral to national security and to support the overall mission of the FBI.

Transitioning CODIS to a cloud-native architecture is critical to meet several strategic goals for the FBI and federal government. Cloud migration is a primary objective across the enterprise. While other approaches, such as a "lift and shift" approach, were considered, a full modernization is the most cost effective and strategically valuable approach. The proposed approach will allow the FBI to fully implement a zero-trust architecture and employ the latest Identity and Access Management controls.

The operational benefits to modernization are numerous. A cloud-native version of CODIS will allow the FBI to leverage modern computing advantages to improve communications among participating laboratories and dramatically decrease database searching times. Currently, DNA profiles are transmitted to the National DNA Index System via a time-consuming bulk transmission. As a result, searches of the database and the subsequent detection of matches can only occur once per day during the overnight hours. A cloud native application will handle these types of transactions in real time. This will allow law enforcement to immediately enroll DNA profiles and generate investigative leads on demand, further improving public safety and security.

Funding

1. Base Funding

FY 2022 Enacted				FY 2023 Enacted				FY 2024 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
166	0	162	$45,446	168	0	162	$53,625	168	0	165	$56,703

2. Personnel Increase Cost Summary

Type of Position/Series	FY 2024 Request ($000)	Positions Requested	Full Year Modular Cost per Position ($000)	Annualizations ($000)			
				2nd Year	3rd Year	FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
Professional Support	$827	6	$195	$32	$82	$193	$492
Forensic Examiner - Scientist	$421	1	$488	($103)	$93	($103)	$93
Total Personnel	**$1,248**	**7**	**$683**	**($71)**	**$175**	**$90**	**$585**

3. Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	FY 2024 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
Information Technology Operation and Maintenance	$1,300	N/A	N/A	$0	$0
Laboratory Equipment – Non-Capitalized	$3,500	N/A	N/A	($958)	$0
Laboratory Supplies	$26,042	N/A	N/A	$0	$0
Local Travel	$25	N/A	N/A	$0	$0
Management and Professional Support Services	$16,002	N/A	N/A	$0	$0
Other Services	$5,000	N/A	N/A	$0	$0
Total Non-Personnel	**$51,869**	**N/A**	**N/A**	**($958)**	**$0**

4. Justification for Non-Personnel Annualizations

DHS Related DNA Collections:
The FBI requests this enhancement to handle a substantial increase in sample submissions from DHS and other federal law enforcement partners due to policy changes (e.g., ending of Title 42 authority). This volume of samples is expected to remain consistent going forward and requires increased funding to meet the legally mandated DNA databasing work. DNA collection kits are required to provide a standardized collection mechanism and subsequent processes require chemical reagents and supplies to obtain CODIS DNA profiles. The samples processed by the FBI require permanent storage to maintain the integrity of the samples for possible re-analysis. This storage will continue to be needed as more samples are submitted for processing.

Rapid DNA:
This enhancement enables the FBI to implement its Rapid program in a scaled manner to at least six FBI Field Office booking stations per year until it reaches a maximum of 24 field office booking locations. As more booking locations are added, funding will be shifted to service maintenance agreements and supplies to support the deployed instrumentation. Once the maximum is reached, all funding will be used for supplies, instrument service agreements and instrument replacement.

5. Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
Current Services	168	0	165	$32,713	$23,990	$56,703	N/A	N/A
Increases	7	0	4	$1,248	$51,869	$53,117	($868)	$585
Grand Total	**175**	**0**	**169**	**$33,961**	**$75,859**	**$109,820**	**($868)**	**$585**

6. Affected Crosscuts

- Intelligence & Information Sharing and National Security.

Item Name: **Secure Communications**

Strategic Goal: 1, 2, 3 & 4
Strategic Objective: 1.2, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 3.1, 3.2 & 4.2
Budget Decision Unit(s): All

Organizational Program: Information Technology Application and Data, Information Technology Infrastructure

Program Increase: Positions 0 Agt/Atty 0 FTE 0 Dollars $3,100,000 (all non-personnel)

Description of Item

The FBI is requesting resources to maintain secure, remote access devices that were deployed throughout the enterprise in 2021. The investment and funding will be used to support the Enterprise Remote Access System (ERAS) program, allowing the FBI the ability to access the FBI's Secret Enclave securely and remotely to quickly adapt to rapidly changing mission requirements.

Justification

Secure Communications: $3,100,000 ($3,100,000 non-personnel)

The FBI requires reliable, secure access to classified information and systems in a remote environment to support necessary operations and functions. The FBI's ERAS program provides FBI users the ability to access the FBI's Secret Enclave securely and remotely. This is particularly important in field offices where Special Agents may be several hours from the nearest FBI Field Office (FO) or Resident Agency (RA). This remote access significantly improves the timely completion of investigative activities, dissemination of intelligence, and sustainment of necessary business operations.

This provides several benefits to use:

- Access to the secured enclave from anywhere and anytime
- Reduced office space needs
- Increased network and communication circuit performance at small sites
- Improved user experience

The FBI is requesting operational and maintenance funding to support the ERAS secured communication devices. The investments and funding used to support the ERAS program and new deployments do not have a permanent, sustained funding source. During the COVID-19 pandemic, ERAS devices were acquired and deployed using coronavirus supplemental funding provided in P.L. 116-260, allowing the FBI to quickly adapt to rapidly changing health and safety protocols. The devices have helped to accelerate capabilities not initially seen during pre-COVID. The FBI needs to be able to sustain the infrastructure for this capability.

The operation and maintenance costs include servers, network equipment located in the CJIS (East) and Pocatello (West) data centers, license costs, and contractor support. Without this funding, the FBI will not be able to support the ERAS program long-term, hampering the ability of FBI users to have timely access to required information and tools to support the FBI mission. With increasingly remote work demands on the FBI workforce and mission, sustainment of this program is crucial.

Impact on Performance

The ERAS provides remote access to FBI Information Systems outside FBI-controlled spaces in accordance with the National Security Agency Commercial Solutions for Classified (CSfC) Mobile Access (MA) Capabilities Package (CP) 2.5.1. This capability was severely constrained pre-COVID due to a limited number of devices and an aging, unsupported infrastructure only capable of supporting a small number of concurrent users. With a larger ERAS footprint and the continued demand for ERAS due to technical capabilities required for mission-critical operations during and post-COVID, the continued Operations and Maintenance (OM) funding is vital to sustain devices that have been fully integrated into the day-to-day business of the FBI. Maintaining the supporting infrastructure and devices at their expanded capacity is necessary to operations across the enterprise. With the additional funding the FBI will be able to sustain active ERAS devices, improving operational capabilities across the organization.

Funding

1. Base Funding[3]

FY 2022 Enacted				FY 2023 Enacted				FY 2024 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
0	0	0	$39,439	0	0	0	$50,140	0	0	0	$49,658

2. Personnel Increase Cost Summary

Type of Position/Series	FY 2024 Request ($000)	Positions Requested	Full Year Modular Cost per Position ($000)	Annualizations ($000)			
				1st Year	2nd Year	FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
None	$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 2024 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
Equipment	$2,500	N/A	N/A	$0	$0
Advisory and Assistance Services	$600	N/A	N/A	$0	$0
Total Non-Personnel	**$3,100**	**N/A**	**N/A**	**$0**	**$0**

4. Justification for Non-Personnel Annualizations

The FBI must continuously improve its investigative capabilities through advanced technology to keep pace with its adversaries. The equipment investment will fully recur to maintain long-term sustainability of secured communication tools. Advisory and assistance costs must fully recur to support the multi-year efforts to develop and

[3] Reflects IT O&M Enterprise Support funding. ERAS has no dedicated base funding for O&M.

administer the program capabilities and infrastructure. Without these recurrals, the FBI is at risk of losing momentum in sustaining advanced technologies.

5. Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
Current Services	0	0	0	$2,367	$47,291	$49,658	N/A	N/A
Increases	0	0	0	$0	$3,100	$3,100	$0	$0
Grand Total	**0**	**0**	**0**	**$2,367**	**$50,391**	**$52,758**	**$0**	**$0**

6. Affected Crosscuts

- Cyber, Intelligence & Information Sharing, and National Security.

Item Name: **Zero Emission Vehicles**

Strategic Goal: 1, 2, 3, 4
Strategic Objective: 1.2, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 3.1, 3.2, 4.2
Budget Decision Unit(s): All

Organizational Program: Facilities

Program Increase: Positions 0 Agt/Atty 0 FTE 0 Dollars $14,140,000 (all non-personnel)

Description of Item

- **Zero Emission Vehicles:** The FBI requests $14,140,000 (all non-personnel) to begin to address executive order requirements and meet standards for sustainable, resilient vehicle fleet electrification.

Justification

In support of the President's goal of transitioning to a fully Zero Emission Vehicle (ZEV) federal fleet, the FBI requests $14.1 million for ZEV (battery electric, plug-in electric hybrid, and hydrogen fuel cell vehicles) acquisitions and the deployment of vehicle charging and refueling infrastructure. These acquisitions are a significant step toward eliminating tailpipe emissions of greenhouse gases (GHG) from the FBI's fleet and aligning the FBI's fleet operations with the goal of achieving a fully ZEV federal fleet. This request supports the FBI's comprehensive plan pursuant to E.O. 14057.

The FBI's ZEV acquisition strategy includes vehicles for both its agency-owned and General Services Administration (GSA)-leased segments of its vehicle fleet. To ensure effective and efficient deployment of ZEVs, the FBI will undertake preparation and planning for deploying ZEVs at its facilities, properly prioritizing transition to ZEVs where it is simplest, and allowing time for additional planning where mission demands pose a challenge to transitioning based on current technologies. Integral to this preparation is growth in the number of agency-accessible vehicle charging stations. In installing this infrastructure on-site to support ZEVs, the FBI will take the long-term view to ensure efficiencies and strategic infrastructure decisions that aims to limit total expenditures.

Zero Emission Vehicles: $6,250,000 (all non-personnel)

The FBI requests $6,250,000 to acquire and deploy 125 ZEVs, including battery electric and plug-in hybrid electric vehicles (PHEV), to expand its ZEV pilot program and support compliance with E.O. 14057's requirement that all new light-duty vehicle acquisitions be ZEVs beginning in 2027. In addition to E.O. 14057 goals, the automotive industry is moving toward electrification and the FBI must plan to advance alongside industry to keep its fleet operational. The FBI has observed that new ZEV prices are approximately 40% more than internal combustible engine vehicles and expects ZEVs to cost approximately $50,000 each, on average, across multiple vehicle classes in FY 2024.

The FBI will continue to deploy these ZEVs to its owned/operated campuses and select Field Offices where sufficient Electric Vehicle Supply Equipment (EVSE), also called "charging

stations," currently exists on-site or where public charging infrastructure is sufficient to support FBI missions. In addition, the FBI will prioritize transitioning to ZEV where it is simplest and may explore the use of PHEV where missions require driving long distances and/or where public charging infrastructure is limited.

Charging Station Infrastructure to Support Integration of Zero Emission Vehicles into FBI Fleet: $7,890,000 (all non-personnel)

To support the deployment of ZEV across the fleet, the FBI requests funding to acquire and install EVSE, including approximately 210 Level II dual-port stations, 20 Direct Current Fast Chargers (DCFC), and 15 Level II solar-powered charging stations at FBI facilities to support new ZEVs in the fleet. The FBI has a fleet of more than 20,000 vehicles, and estimates that it will need between 5,000 and 10,000 stations on FBI property to adequately support an electrified fleet. The requested amount of EVSE would support the deployment of at least 1,000 ZEV in future years. In addition to acquisitions and installation costs, the FBI requires funds for continued maintenance of the EVSE, electrical utilities, and potential electrical grid upgrades. While further funding will be required to fully install the required infrastructure, this request is an important first step that will support the FBI's fleet as it begins to procure more electric vehicles.

The FBI will acquire and install EVSE at FBI owned/operated campuses and select Field Offices that are conducive to early ZEV fleet transition based on vehicle use cases, climate and geography, supporting public charging infrastructure, and existing electrical capacities. The Level II dual-port charging stations plus installation cost approximately $14,000 each. The DCFC cost approximately $70,000 each, including installation, and will be necessary to support the law enforcement mission of the FBI. The solar-powered stations cost approximately $75,000 each and include 4 charging ports. The solar-powered stations do not require construction, would be well-suited for typically sunny environments, and would reduce reliance on the electrical grid, providing an operational safety-net. The FBI requires $1,475,000 for site planning support, electricity utilities, and potential electrical upgrade costs. Approximately $900,000 is requested for five-year EVSE operations and maintenance costs of the planned EVSE and the training of FBI automotive technicians in the new technology.

Impact on Performance

The requested $14,140,000 is necessary to assist the FBI in beginning to meet key federal executive order requirements as they relate to ZEVs and mitigating the risks climate change poses to mission readiness and operational continuity. With the requested funding, the FBI will have the resources necessary to gradually transition the current fleet to meet the specific E.O. 14057 mandate for agencies to achieve 100 percent ZEV acquisitions by 2035, including 100 percent zero-emission light-duty vehicle acquisitions by 2027 (Sec. 102). This funding will help ensure the long-term viability of the FBI's transition to ZEV and support its continued operational readiness in face of a changing automotive market environment.

Funding

1. Base Funding

FY 2022 Enacted				FY 2023 Enacted				FY 2024 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
0	0	0	$2,197	0	0	0	$1,135	0	0	0	$1,385

2. Personnel Increase Cost Summary

Type of Position/Series	FY 2024 Request ($000)	Positions Requested	Full Year Modular Cost per Position ($000)	Annualizations ($000)			
				1st Year	2nd Year	FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Total Personnel	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**

3. Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	FY 2024 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
Equipment	$14,140	N/A	N/A	$0	$0
Total Non-Personnel	**$14,140**	**N/A**	**N/A**	**$0**	**$0**

4. Justification for Non-Personnel Annualizations

In support of the President's goal of transitioning to a fully ZEV federal fleet, the FBI's budget includes $14.1 million for zero emission vehicles (battery electric, plug-in electric hybrid, and hydrogen fuel cell vehicles) acquisitions and deploying vehicle charging and refueling infrastructure. These acquisitions are a significant step towards eliminating tailpipe emissions of GHG from FBI's fleet and aligning the FBI's fleet operations with the goal of achieving a fully ZEV Federal fleet.

5. Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
Current Services	0	0	0	$0	$1,385	$1,385	N/A	N/A
Increases	0	0	0	$0	$14,140	$14,140	$0	$0
Grand Total	**0**	**0**	**0**	**$0**	**$15,525**	**$15,525**	**$0**	**$0**

6. Affected Crosscuts

- Intelligence & Information Sharing and National Security.

Item Name: **Body Worn Cameras**

Strategic Goal: 1, 2, 3, 4
Strategic Objective: 1.2, 2.1, 2.2, 2.3, 2.4., 2.5, 2.6, 3.1, 3.2, 4.2
Budget Decision Unit(s): All

Organizational Program: Operational Technology

Program Increase: Positions 0 Agt 0 Atty 0 FTE 0 Dollars $2,784,000 (all non-personnel)

Description of Item

The FBI requests $2,784,000 in non-personnel funding for the continued development and launch of a Body Worn Camera (BWC) program for FBI Special Agents across all FBI field offices. The requested resources will be used for contracting costs to develop the technical infrastructure required for the BWC program and storage of footage 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 launched 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 additional funding 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 $1,800,000 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 to support 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.

- **BWC Cameras:** The FBI requests $724,000 for the purchase of cameras and associated equipment to continue implementation at all 56 field offices.
- **Training/Travel:** The FBI requests $260,000 to fund travel and training during the continued 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 George Floyd Justice in Policing Act of 2021, if signed into law, would require federal law enforcement officers (LEOs) to utilize BWCs during certain operations.

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 successfully develop and launch the BWC program for 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 2022 Enacted				FY 2023 Enacted				FY 2024 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
0	0	0	$6,208	102	1	52	$32,170	102	1	102	$40,856

2. Personnel Increase Cost Summary

Type of Position/Series	Positions Requested	Annual Costs per Position ($000)			FY 2024 Request ($000)	Annualizations ($000)	
		1st Year Adjusted Cost	2nd Year Adjusted Cost	3rd Year Full Cost (Modular)		FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Total Personnel	**0**	**$0**	**$0**	**$0**	**$0**	**$0**	**$0**

3. Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	FY 2024 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
Equipment	$724	N/A	N/A	$0	$0
Advisory and Assistance Services	$1,411	N/A	N/A	$0	$0
Travel and Transportation of Persons	$260	N/A	N/A	$0	$0
Other Services	$389	N/A	N/A	$0	$0
Total Non-Personnel	**$2,784**	**N/A**	**N/A**	**$0**	**$0**

4. Justification for Non-Personnel Annualizations

The FBI expects to fully recur cost in FY 2024 and FY 2025. This cost will help fund the development of technical infrastructure, storage of footage and procurement of hardware, software and BWC related equipment.

5. Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
Current Services	102	1	102	$22,891	$17,965	$40,856	$0	$0
Increases	0	0	0	$0	$2,784	$2,784	$0	$0
Grand Total	**102**	**0**	**102**	**$22,891**	**$20,749**	**$43,640**	**$0**	**$0**

6. Affected Crosscuts

- Civil Rights and Federal Criminal Justice Reform.

VI. Program Decreases by Item

Item Name: **Ukraine Supplemental – Russian Kleptocracy Team**

Strategic Goal: N/A
Strategic Objective: N/A
Budget Decision Unit(s): Intelligence, Criminal Enterprises/Federal Crimes

Organizational Program: Criminal Investigative Division

Program Decrease: Positions (14) Agt/Atty (11) FTE (14) Dollars $0

Description of Item

Supplemental appropriations provided in the Consolidated Appropriations Act, 2022 (P.L. 117-103) provided the FBI with $43.6 million, to remain available until September 30, 2023, to respond to the situation in Ukraine and for related expenses. A portion of the funding was utilized to support a team of 14 personnel (11 agents) to investigate Russian Kleptocracy matters.

Because these funds will no longer be available in FY 2024, the FBI does not have sufficient funding to sustain the 14 positions.

Justification

The positions supported with Ukraine supplemental funding are not annualized in the FY 2024 budget request. Without annualized funding, the FBI is unable to sustain the costs of these positions.

Impact on Performance

This is a technical budget adjustment that will ensure that the FBI budget does not display position amounts for which there is no longer available funding.

Funding

1. Base Funding *(includes one-time supplemental funding)*

FY 2022 Enacted				FY 2023 Enacted				FY 2024 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
14	11	0	$43,600	14	11	14	$0	14	11	14	$0

2. Personnel Decrease Cost Summary

Type of Position/Series	FY 2024 Request ($000)	Positions Requested	Full Year Modular Cost per Position ($000)	Annualizations ($000)			
				2nd Year	3rd Year	FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
Total Personnel	**N/A**	**(14)**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**

3. Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	FY 2024 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
Total Non-Personnel	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**

4. Justification for Non-Personnel Annualizations

Not applicable.

5. Total Request for this Item

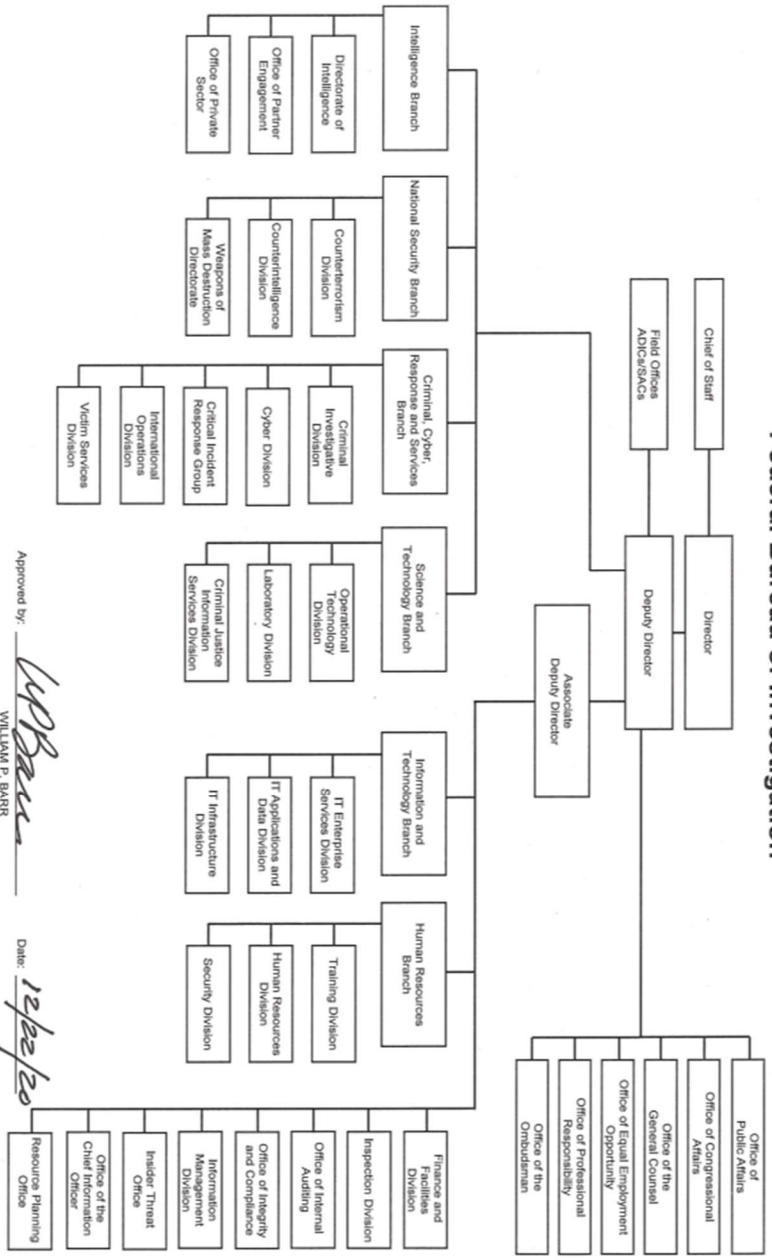
Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
Current Services	14	11	14	$0	$0	$0	N/A	N/A
Decreases	(14)	(11)	(14)	$0	$0	$0	$0	$0
Grand Total	**0**	**0**	**0**	**$0**	**$0**	**$0**	**$0**	**$0**

6. Affected Crosscuts

- N/A

VII. EXHIBITS

A. Organizational Chart



VIII. 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.

Richard Shelby Center for Innovation and Advanced Training at 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.

The FBI's presence on the North Campus features a 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 houses 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, houses more than two billion pages of records. 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 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. Major building systems are near end-of-life and structural issues continue to mount, making the current building unsustainable. The Administration proposes continuation of a multi-year effort to construct a modern, secure suburban facility from which the FBI can continue its mission to protect the American people.

The General Services Administration (GSA) and FBI are currently working to select one of the three sites previously included in the 2016 procurement, on which GSA will construct a Federally-owned, modern and secure headquarters facility for at least 7,500 personnel in the D.C. suburbs. Pending the site selection and full funding, GSA and FBI will proceed with procurement and construction activities.

The 2024 Budget supports the funding necessary for execution of this complex project via the Federal Capital Revolving Fund (FCRF). The Administration's FCRF proposal provides a new budgetary mechanism to fully fund the costs of very large civilian real property capital projects that are difficult to accommodate in the annual appropriations process. This is accomplished by providing mandatory resources for the total project cost upfront and repaying those resources with annual discretionary appropriations over 15 years. For the FBI suburban headquarters campus, the Budget proposes a $3.5 billion allocation from the FCRF, to be repaid by the Federal Buildings Fund in 15 annual amounts of $233 million. The FCRF funding would be paired with $645 million in GSA prior year appropriations to support the acquisition and construction of the FBI's new suburban headquarters campus.

Additionally, GSA and FBI continue efforts 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, Congress and other partners. The Administration plans to use existing balances in the FBI's account previously appropriated for the new headquarters effort to build out a downtown D.C. location to support the FBI's mission.

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

IX. GLOSSARY

ADIC	Assistant Director in Charge
Agt	Special Agent
ALATs	Assistant Legal Attachés
AOR	Area of Responsibility
AS	Administrative Specialist
ATB	Adjustments to Base
ATF	Alcohol, Tobacco, Firearms, and Explosives
Atty	Attorney
BAS	Building Automation System
BWC	Body Worn Camera
C2	Command and Control
CAC	Combatting Crimes Against Children
CACU	Crimes Against Children Unit
CAR	Criminal Answer Required ----
CARD	Child Abduction Rapid Deployment
CCRSB	Criminal, Cyber, Response, and Services Branch
CD	Counterintelligence Division
CDE	Crime Data Explorer
CE	Criminal Enterprises
CEFC	Criminal Enterprises and Federal Crimes
CEOU	Child Exploitation Operations Unit
CHRI	Criminal History Record Information
CI	Counterintelligence
CIA	Central Intelligence Agency
CID	Criminal Investigative Division
CIP	Computer Intrusion Program
CIRG	Critical Incident Response Group
CJ	Criminal Justice

CJIS	Criminal Justice Information Services
CJISD	Criminal Justice Information Services Division
CJS	Criminal Justice Services
CODIS	Combined DNA Index System
COL	Color of Law
COOP	Continuity of Operations
CP	Counterproliferation
CPOT	Consolidated Priority Organization Target
CSAM	Child Sexual Abuse Material
CST	Child Sex Tourism
CT	Counterterrorism
CT/CI	Counterterrorism/Counterintelligence
CTD	Counterterrorism Division
C-UAS	Counter-Unmanned Aircraft Systems
CY	Calendar Year
CyD	Cyber Division
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
DU	Decision Unit
EAD	Executive Assistant Director

EAMS	Enterprise Access Management System
ECU	Evaluation and Certification Unit
EDO	Electronic Departmental Order
EGIS	Expert Government Information Specialist
EJI	Elder Justice Initiative
EO	Executive Order
ERAS	Enterprise Remote Access Solution
EVSE	Electric Vehicle Supply Equipment
FACE	Freedom of Access to Clinic Entrance
FBI	Federal Bureau of Investigation
FFA	Federal Firearms Act
FFD	Facilities and Finance Division
FFL	Federal Firearms Licensee
FISA	Foreign Intelligence Surveillance Act
FLP	Foreign Language Program
FO	Field Office
FTE	Full-time Equivalent
FTTTF	Foreign Terrorist Tracking Task Force
FY	Fiscal Year
GCA	General Crimes Act
GIS	Government Information Specialists
GRU	Russian Military Intelligence
GSF	Gross Square Feet
HDS	Hazardous Devices School
HIG	High-Value Detainee Interrogation Group
HQ	Headquarters
HRB	Human Resources Branch
HRD	Human Resources Division
HRT	Hostage Rescue Team

HT	Human Trafficking
HUMINT	Human Intelligence
HVE	Homegrown Violent Extremists
IA	Intelligence Analyst
IaaS	Infrastructure as a Service
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
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
InTO	Insider Threat Office
IOD	International Operations Division
IPM	Integrated Program Management
IPS	Interstate Photo System
IPK	International Parental Kidnapping
IS	Information System
ISIS	Islamic State of Iraq and ash-Sham
ISSE	Information Systems Security Engineering
ISSO	Information Systems Security Operation
IT	Information Technology

ITADD	Information Technology Applications and Data Division
ITB	Information and Technology Branch
ITESD	Information Technology Enterprise Services Division
ITID	Information Technology Infrastructure Division
JWICS	Joint Worldwide Intelligence Communication System
KPI	Key Performance Indicator
LD	Laboratory Division
LE	Law Enforcement
LEEP	Law Enforcement Enterprise Portal
LEO	Law Enforcement Officer
MAPA	Management and Program Analyst
NAS	NICS Alert Service
NCAVC	National Center for the Analysis of Violent Crime
NCIC	National Crime Information Center
NCIJTF	National Cyber Investigative Joint Task Force
NCITF	National Counterintelligence Task Force
NCJ	Non-Criminal Justice
NCMEC	National Center for Missing and Exploited Children
NCPC	National Counterproliferation Center
NCTC	National Counterterrorism Center
N3G	NCIC 3rd Generation
N-DEx	National Data Exchange
NDIS	National DNA Index System
NIBRS	National Incident-Based Reporting System
NICS	National Instant Criminal Background Check System
NIP	National Intelligence Program
NOC	Network Operations Center
NPPS	National Palm Print System
NSA	National Security Agency

NSB	National Security Branch
NTOC	National Threat Operations Center
NTP	National Threat Priority
OCA	Office of Congressional Affairs
OCE	Online Covert Employee
OCIO	Office of the Chief Information Officer
ODNI	Office of the Director of National Intelligence
OEEOA	Office of Equal Employment Opportunity Affairs
OGC	Office of the General Counsel
OIA	Office of Internal Auditing
OIC	Office of Integrity and Compliance
OIG	Office of the Inspector General
OM	Operations and Maintenance
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
OTD	Operational Technology Division
PaaS	Platform as a Service
PIN	Private Industry Notices
PMF	Privately Made Firearm
POC	Point of Contact
PS	Professional Staff
PS	Professional Support
PSC	Private Sector Coordinator
RA	Resident Agency
RBS	Rap Back Services
RPO	Resource Planning Office

S&E	Salaries and Expenses
SA	Special Agent
SaaS	Software as a Service
SAC	Special Agent in Charge
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCINet	Sensitive Compartmented Information Network
SCRM	Supply Chain Risk Management
SEAR	Special Event Assessment Rating
SecD	Security Division
SID	State Identification Number
SIIG	Strategic Intelligence Issues Group
SIOC	Strategic Information Operations Center
SLTT	State, Local, Tribal, and Territorial
SME	Subject Matter Expert
SOI	Subject of Interest
SOG	Special Operations Group
SOP	Standard Operating Procedure
SSA	Supervisory Special Agent
SSG	Special Surveillance Group
STB	Science and Technology Branch
STM	Sex Trafficking of Minors
SWE	Secure Work Environment
TAG	Transnational Anti-Gang Task Force
TCO	Transnational Criminal Organization
TD	Training Division
TFO	Task Force Officer
TIE	Threat Intake Examiner
TIPS	Threat Intake Processing System

TOC	Transnational Organized Crime
TRP	Threat Review and Prioritization
TS	Top Secret
TSC	Terrorist Screening Center
TSA	Transportation Security Administration
TTL	Threat to Life
UAS	Unmanned Aircraft System
UCE	Undercover Employee
UCN	Universal Control Number
UCR	Uniform Crime Reporting
UNet	Unclassified Network
US	United States
USC	United States Code
USIC	United States Intelligence Community
USPER	U.S Person
VCACITF	Violent Crimes Against Children International Task Force
VG	Violent Gangs
VGSSTF	Violent Crime and Safe Streets Gang Task Forces
VSD	Victim Services Division
WCC	White Collar Crime
WMD	Weapons of Mass Destruction
WMDD	Weapons of Mass Destruction Directorate
ZTA	Zero Trust Architecture