FY 2025 President's Budget Request

March 2024

Table of Contents

I. Overview

A. Introduction

Budget Request Summary: The Federal Bureau of Investigation's (FBI's) Fiscal Year (FY) 2025 Budget request proposes a total of $11,334,839,000 in direct budget authority, of which $11,272,944,000 is for Salaries and Expenses (S&E) and $61,895,000 is for Construction. The Budget also proposes a cancellation of $50,000,000 in prior-year S&E balances.

The S&E request includes a total of 37,083 direct positions and 35,632 direct full-time equivalents (FTE). The positions include:

- 13,623 Special Agents (SAs)
- 3,337 Intelligence Analysts (IAs)
- 20,123 Professional Staff (PS)

The S&E program increases total $118,588,000; 353 positions (77 SAs, 58 IAs, and 218 PS); and 312 FTE for the following:

- $7,000,000 for cyber investigative capabilities
- $17,792,000 for counterintelligence matters
- $8,433,000 for the National Instant Criminal Background Check System (NICS)
- $85,363,000 for restoration of 2023 national security & law enforcement personnel

The request includes $192,033,000 in technical adjustments and $286,323,000 in adjustments to base (ATBs) for continued support of the FBI's base operations.

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 2025 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 Mission: Protect the American people and uphold the Constitution of the United States.

The FBI Vision: Ahead of the threat.

Department of Justice (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 of the United States, 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

Guiding Principles and Enterprise Objectives:

1. People
    - § Promote a culture of development and resilience
    - § Assemble diverse teams
    - § Cultivate leadership and mentorship
    - § Recruit for the future
2. Partnerships
    - § Integrate meaningful partnerships
    - § Improve information sharing
    - § Increase community engagement
3. Process
    - § Strengthen confidence and trust
    - § Enhance rigor and accountability
    - § Align resources to priorities
4. 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 (FOs), and legal attaché offices (Legats) 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 FOs and 62 Legats use this national guidance to formulate an FO and Legat threat prioritization and complete their own specific strategies. These threat and program strategies undergo mid-year and end-of-year evaluations, and each individual FO and Legat is held accountable to their performance targets. FBI executives and program managers hold regular meetings to review and evaluate FO and Legat 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 and maintenance funding. Moreover, a multi-year planning approach allows FBI management to better understand the implications of proposed initiatives. This FY 2025 budget request is designed to promote capabilities and strategies that are sufficiently agile to meet ongoing, emerging, and unknown national security, cyber, and criminal threats.

Organization of the FBI: The FBI operates FOs 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 FOs and enable the FBI to maintain a presence in and serve a greater number of communities. FBI employees assigned to FOs 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 FOs report directly to the Director and Deputy Director.

The FBI also operates 62 Legats and 34 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 (HQ) 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 Victim 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 (DUs) 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 2025. 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 2025 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 whom 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 FOs across all 50 states.

Foreign Intelligence: 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. The foreign intelligence threat targets far more than U.S. government secrets: it is one arm by which nation-state competitors aim to challenge U.S. economic as well as military and diplomatic power across the globe, as well as challenge the U.S. commitment to human rights and democratic values within U.S. borders. The FBI is adapting its foreign intelligence focus to take a comprehensive approach that draws on the full extent of available tools and legal authorities, including in partnerships with other U.S. government agencies and friendly foreign partners with shared security concerns, to address the alarming spectrum of illegal activity from hostile nations.

The FBI remains vigilant against core national security threats such as traditional espionage activities and efforts to evade export control and sanctions laws. It is essential that the U.S. thwarts attempts to unlawfully obtain classified information relating to national defense, weapons systems and sensitive technologies and research. In addition, the FBI and the DOJ bring all tools to bear to protect U.S. economic security and prosperity, including key technology innovations, private information about Americans, and supply chains and industry. Threats to American technology, critical infrastructure, information systems, and the information itself come both in person and through cyber means, and the FBI meets adversaries on both fronts. The newest challenge is preventing malign foreign influence and protecting the freedom of expression and democracy for all residents of the U.S. against nations seeking to export their repression of speech through threats and violence. The FBI is committed to confronting any nation that threatens U.S. national security, economic security, or democratic institutions and freedoms.

Cyber: Nation-state and cyber criminals pose a growing 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 2023, cyberattacks caused significant financial damage and extensive harm to governments, critical infrastructure, and industries worldwide. The effects of cyberattacks are also felt by individuals, in the form of identity theft, account hacking, email compromise schemes, and cyberstalking. The rise of cryptocurrencies also enables cybercriminals, terrorists, and nation states to acquire tools, collaborate, and launder their criminal proceeds in new and challenging ways.

The U.S.'s adversaries are investing significant resources to plan and conceal their malicious operations. Nation-state actors also collaborate 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 leverages a strategy to impose risk and consequences on cyber adversaries through unique authorities, world-class capabilities, and enduring partnerships. The strategy provides the needed human and technical resources to enable the FBI and 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, in February 2024 the FBI, in coordination with foreign and domestic partners, conducted a joint-sequenced operation that led to the disruption of the LockBit ransomware group. LockBit emerged in 2020 and has grown to become a prolific ransomware group that has targeted over 2,000 victims, made ransom demands totaling hundreds of millions of dollars, and received over $120 million in ransom payments. As a result of the successful operation to dismantle LockBit, the FBI and other partners seized numerous public-facing websites used by LockBit to connect to the organization's infrastructure and seized control of serves used by LockBit administrators. This prevented LockBit actors from attacking and encrypting networks to extort victims both domestically and abroad. During the operation, the FBI was able to obtain keys from seized LockBit infrastructure, which will be used to help victims decrypt their systems and regain their stolen data.

These actions, and victim-focused efforts, are especially impactful when coupled with the Justice Department's indictment against two Russian nationals associated with the LockBit ransomware group. This is a continuation of efforts from 2022 and 2023 where three other Russian nationals were charged and indicted for their participation and role in the LockBit organization. The FBI will continue to help and protect victims and bring justice to those who commit cyberattacks, whether they are part of a coordinated ransomware group or nation-state.

White Collar Crime (WCC): The WCC program addresses public corruption, border corruption, corporate fraud, securities/commodities fraud, mortgage 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 democratic institutions and threaten public safety and national security. U.S. public officials and employees are vulnerable to exploitation from individuals, 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 sea, air, and land ports of entry, 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 FOs 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 criminal 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. In addition, the FBI investigates those involved in the fraudulent diversion of controlled substances, from their legal purpose into illicit drug trafficking. 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 deceptive 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 sector 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 investigate 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 reach. 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 2023, the FBI led over 100 organized crime and major theft task forces targeting TCO networks based in both 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 into the country's illicit drug market, including fentanyl and fentanyl analogues.

To address the evolving threat of Darknet drug trafficking, the FBI manages the Joint Criminal and Opioid Darknet Enforcement (JCODE) Initiative. JCODE is a collaboration involving 11 Federal law enforcement agencies, bringing together agents, analysts, and other staff – with expertise in drugs, gangs, health care fraud, and more – with state and local law enforcement partners from across the U.S. JCODE further unifies its investigative reach by partnering with Europol and other foreign law enforcement agencies. JCODE developed a comprehensive, multi-pronged criminal enterprise strategy to target fentanyl and opioid trafficking on Darknet and Clearnet. This strategy focuses on a headquarters-based team dedicated to developing sophisticated systems and applications to provide comprehensive data analysis for direct targeting, as well as the development and support of task forces in the field. Task forces focus on initiating robust criminal enterprise investigations through the execution of proactive undercover operations, the identification and infiltration of marketplace administrative teams, technical infrastructure and through the exploitation of virtual currency and seized data sets.

The FBI recently created the Mobile Encrypted Networks and Communications Exploitation (MENACE) team to address the growing threat of encrypted messaging applications and technical data sharing mechanisms. MENACE supports enterprise investigations targeting the companies who promote the use of these applications for criminal organizations to subvert law enforcement. The goal of MENACE is to pioneer new technology to infiltrate the communications of these organizations and stay ahead of them as technology evolves. MENACE develops applications to exploit vulnerabilities within a criminal organization's communication plan, which is in direct collaboration with U.S. and foreign law enforcement partners.

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 throughout 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 2023, the FBI led 178 VGSSTFs and 57 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, 85 Child Exploitation and Human Trafficking Task Forces, and 76 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 children, as well as arresting numerous offenders.

In 2019, the FBI created the Child Exploitation Operation Unit (CEOU) to develop complex global investigations, utilize innovative technologies, to identify and rescue children and apprehend the world's most egregious offenders. The CEOU is not constrained by geographic boundaries and maintains squads of specialized investigators who work collaboratively with domestic and international partners to address the crimes against children threat on a global scale.

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 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 the Department of Justice 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 (BIA) 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 2023, there were 1,275 arrests, 880 indictments, 118 informations, 159 judicial complaints, and 981 convictions in Indian Country.

The Indian Country and International Violent Crime Unit (ICIVCU) 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. ICIVCU supports joint investigative efforts with the BIA and Tribal law enforcement agencies and manages and conducts essential investigative training for 24 Safe Trails Task Forces, as well as approximately 150 full-time FBI agents and 510 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 the Inspector 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 COL 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; the USIC; and the private sector. 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, 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 via two primary activities:

- The FBI uses a standardized model for field intelligence that can adapt to the size and complexity of small, medium, and large FOs. There are 56 intelligence programs, with one in each FBI FO.
- 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.

Executive Order (E.O.) Adherence and Congressional Budget Justifications

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 the cost people experience in their interactions with government, 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.

While continuing to analyze resource needs, in the interim, the FBI is working to fully meet these requirements through the following 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 FBI 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 engagements 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 communities and reinforce the FBI's dedication to investigating and bringing to justice the perpetrators of civil rights crimes.

Current Services Budget Authority Categorized by Cybersecurity[1]

NIST Framework Function	**Funding Amount ($000)**
Detect	$5,543
Identify	$24,713
Protect	$85,572
Recover	$10,174
Respond	$12,737
Grand Total	**$138,739**

Personnel Vetting

The FBI does not have Non-Sensitive Public Trust (NSPT) personnel, as all FBI personnel fall into the National Security Sensitive Public Trust population. The FBI will continue to collect and report performance metrics as mandated in the Performance Management Implementation Guidance jointly issued by the Director of National Intelligence and the Director of the Office of Personnel Management in October 2023. However, due to the current rollout and transition to a new case management platform for Background Investigations, some reporting may be delayed during FY 2024.

[1] Provided in alignment with Budget Data Request (BDR) 22-39.

Whereas the FBI continues to reach the milestones associated with the implementation framework required under the Trusted Workforce (TW) 2.0 mandate, the lack of personnel enhancements will exacerbate the current backlog of Continuous Vetting (CV) alerts as well as negatively impact the timeliness of all personnel vetting scenarios as outlined in the ODNI and OPM's Performance Management Implementation Guidance. Regarding non-personnel funding, the FBI utilizes an integrated CV Tool as the IT system designed to ingest, manage, and store all CV alerts. The FBI also developed a new case management platform to process Background Investigations. These systems require continued software development and maintenance to support the TW 2.0 requirements.

II. Summary of Program Changes

Item Name	Description	Pos.	FTE	Dollars ($000)	Page
Salaries and Expenses Enhancements					
Cyber	The requested resources will increase the FBI's capacity for unilateral, joint, and enabled operations with other Federal, State, local, and international partners. The request focuses on the development of Victim Engagement and Incident Response.	12	6	$7,000	70
Counterintelligence	The requested resources will enhance the FBI's ability to combat foreign adversary intelligence collection and subversion tactics against the U.S.	44	22	$17,792	71
National Instant Criminal Background Check System	The requested resources will strengthen the National Instant Criminal Background Check System, ensuring the safety and security of the American people among those who choose to exercise their Second Amendment rights.	27	14	$8,433	72
Restoration of 2023 National Security & Law Enforcement Personnel	The requested resources will restore positions and funding for critical national security and law enforcement cases and programs originally reduced due to budget allocations. Recent limitations and restrictions placed on FBI resources have put the organization's ability to protect the American people and uphold the Constitution at risk, and this request aims to alleviate a significant portion of those concerns.	270	270	$85,363	77
Salaries and Expenses Enhancements Total		**353**	**312**	**$118,588**	

III. Appropriations Language and Analysis of Appropriations Languages

For necessary expenses of the Federal Bureau of Investigation for detection, investigation, and prosecution of crimes against the United States, $11,272,944,000, 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.

(CANCELLATION)

Of the unobligated balances available under this heading, $50,000,000 is hereby permanently cancelled: Provided, That no amounts may be cancelled from amounts that were designated by the Congress as an emergency requirement pursuant to a concurrent resolution on the budget or the Balanced Budget and Emergency Deficit Control Act of 1985.

Analysis of Appropriations Language

- The FY 2025 request proposes a balance rescission, which cancels $50,000,000. The FBI will execute this rescission using prior-year balances.

IV. Program Activity Justification

A. Intelligence Decision Unit

Intelligence Decision Unit Total	Direct Pos.	Estimate FTE	Amount ($000s)
2023 Enacted	6,666	6,185	$1,914,971
2024 Continuing Resolution[2]	6,285	6,150	$1,971,836
Adjustments to Base and Technical Adjustments	193	193	$65,129
2025 Current Services	6,478	6,343	$2,036,965
2025 Program Increases	89	80	$23,748
2025 Request	6,567	6,423	$2,060,713
Total Change 2024-2025	**282**	**273**	**$88,877**

Intelligence - Information Technology Breakout (of Decision Unit Total)	Direct Pos.	Estimate FTE	Amount ($000s)
2023 Enacted			$291,696
2024 Continuing Resolution			$176,829
Adjustments to Base and Technical Adjustments			$0
2025 Current Services			$176,829
2025 Program Increases			$0
2025 Request			$176,829
Total Change 2024-2025			**$0**

1. Program Description

The FBI's IDU is composed 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; FO 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, STB, IOD, IMD, SecD, and VSD, 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, STB, 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, law enforcement, and private sector communities.

[2] Amounts included herein referring to the FY 2024 Continuing Resolution reflect an Annualized Continuing Resolution level.

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 IC and USG. Led by a Deputy Assistant Director, the SIIG includes a Bureau Intelligence Council, made up of Senior National Intelligence Officers and their Deputies with subject-matter expertise on geographic and functional programs who help integrate the FBI's understanding of priority threat issues. The SIIG houses the Bureau Control Office, which manages the FBI's sensitive compartmented information program. The SIIG also oversees the Domestic Director of National Intelligence (DNI) Representative Program, which fosters a strategic-level environment for unifying the intelligence community domestically. Finally, a representative of the SIIG is detailed to the President's Intelligence Advisory Board, a component of the Executive Office of the President that advises the President on intelligence matters.

Directorate of Intelligence

The DI program manages all FBI intelligence functions and has a dedicated national intelligence workforce. The DI's mission is to enable the FBI to identify threats and opportunities, inform decision-making, and avoid surprise. The DI carries out these functions through embedded intelligence elements at HQ and in each FO. The DI also internally houses intelligence professionals who prepare all-source cross-programmatic strategic analysis, conduct whole-of-FBI collection analysis, and provide enterprise-wide raw intelligence surge capacity.

Intelligence Analysts

The work performed by Intelligence Analysts (IAs) is essential to the FBI's ability to understand national security and criminal threats, and to develop a deeper understanding of 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 Foreign Language Program (FLP) provides exemplary foreign language solutions, analysis, and cultural expertise to advance the FBI's intelligence and law enforcement mission. 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 translated foreign intelligence. 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 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 National Virtual Translation Center (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 an IC Service of Common Concern in 2014, and executively managed by the FBI. Since its inception, NVTC has complemented IC elements' foreign language translation capabilities by supporting tasks ranging from high-volume surges to immediate translation requirements in over 140 languages and dialects. NVTC operates within a virtual model that connects NVTC program staff, translators, FOs, and customers globally via a common web-based workflow management system.

HUMINT Operations

The DI oversees all aspects of the FBI's HUMINT and Confidential Human Source (CHS) programs. Through its policies and evaluative methods, the DI ensures all FOs, Legats, and FBI HQ divisions manage their respective CHSs in compliance with FBI and Intelligence Community directives. The DI ensures those CHSs with the highest risk potential are rigorously and objectively screened for reliability and productivity through established validation and assessment procedures. The DI develops and coordinates messages and provides intermediate

and advanced HUMINT operations training to FBI personnel, taskforce officers, and other IC/law enforcement agencies. Additionally, the DI is the primary stakeholder in the FBI's Positive Foreign Intelligence collection effort, conducts internal and external liaison with FBI operational divisions and other governmental agencies regarding HUMINT matters, and coordinates cross-programmatic intelligence opportunities for CHS activities.

Ubiquitous Technical Surveillance

The DI leads the FBI's efforts to build an enterprise-wide Ubiquitous Technical Surveillance (UTS) strategy that will increase awareness of UTS risks across all programs, while creating a culture that considers the risk posed by UTS in everything the FBI does. The DI works to enhance the FBI workforce's understanding of UTS and the development of UTS mitigation measures through promoting UTS awareness and education, the development of tools and tradecraft to safeguard operations, engagement with internal and external partners with technical expertise, and integration of UTS concerns into FBI policy.

Intelligence Training

The DI ensures the FBI's intelligence workforce is prepared with the necessary specialized skills and expertise to successfully fulfill its mission. The FBI's extensive intelligence training program leverages expertise within the organization and its partners in the IC, academia, 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.

Intelligence Technology

Intelligence Technology provides the services and applications necessary to support the FBI's intelligence mission across the enterprise to protect the nation and its interests. Intelligence Technology provides a broad spectrum of tools to facilitate open-source intelligence gathering, social media analysis, big data exploitation, human and technical source management, tactical and geospatial analysis, and the timely dissemination of intelligence to the enterprise and the Intelligence Community. Intelligence Technology's comprehensive suite of services and applications ensures the workforce and FBI leaders have the actionable intelligence necessary to support ongoing investigations, make informed decisions, facilitate opportunities, counter threats, identify risks and vulnerabilities, and avoid surprise.

Office of Partner Engagement

Office of Partner Engagement (OPE) supports the FBI mission by building and improving relationships and information sharing with law enforcement partners. To carry out this mission, OPE serves as FBI HQ's primary liaison to executive law enforcement partners and integrates meaningful partnerships; improves information sharing; increases community engagement; strengthens confidence and trust; and promotes a culture of development and resilience between the FBI and its law enforcement partners. This unique role allows OPE to be a voice for law

enforcement partners within the Bureau, bringing policy recommendations and executive updates to FBI leadership. Likewise, OPE fields messages from the FBI to outside law enforcement partners, as appropriate. This is most often accomplished by leveraging relationships with major national and international law enforcement associations which represents Federal, State, local, Tribal, territorial, and campus law enforcement.

In addition to its liaison role, OPE provides active shooter training, both internally to FBI personnel and externally to law enforcement partners; leads an intelligence training program for law enforcement partners; manages the FBI's fusion center engagement program; and is part of the Joint Counterterrorism Assessment Team. Each partner's contribution is instrumental to information and intelligence sharing in support of the FBI's mission.

Office of Private Sector

The primary mission of the Office of Private Sector (OPS) is to protect the nation's economic and national security by strengthening the FBI's relationships with U.S. private sector partners. OPS builds, supports, facilitates, and enhances strategic relationships between the FBI and private industry. 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 private sector partners' understanding of the threat and facilitates engagements between private industry and FBI leadership to build and increase collaboration and information-sharing to mitigate risk and remain ahead of the threat. OPS achieves its objectives by working to facilitate one "FBI voice;" providing a consistent contact for the private sector; focusing on meaningful dialogue with private sector partners to build trust; and messaging companies creating innovative and emerging technologies that may be targeted. OPS also focuses on engaging the private sector on threat priorities including cybersecurity, insider threat, and emerging technologies. In addition to its main office at FBI HQ, OPS manages the Private Sector Coordinator (PSC) Program, which provides training and resources for PSCs working in each of the FBI's 56 FOs, who develop and maintain private sector partnerships in their Areas of Responsibility. OPS manages two private sector information-sharing programs, the Domestic Security Alliance Council (DSAC) and InfraGard, which promote effective information exchanges through public-private partnerships.

Enterprise Vetting Center

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

Terrorist Screening Center

The TSC consolidates and coordinates the USG's approach to national security screening and facilitates the sharing of information to protect the nation and its foreign partners. This effort provides direct support for the FBI, the DOJ, Department of Homeland Security (DHS), Department of State, the ODNI, the IC, and other major Federal law enforcement, screening, and regulatory agencies. The TSC accomplishes this mission through a unique, interagency business model that incorporates 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 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

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	**Actual**		**Target**		**Changes**		**Requested (Total)**	
	FY 2023		**FY 2024**		**Current Services Adjustments and FY 2025 Program Change**		**FY 2025 Request**	
Total Costs and FTE (reimbursable FTE are included, but reimbursable costs are bracketed and not included in the total)	**FTE**	**$000s**	**FTE**	**$000s**	**FTE**	**$000s**	**FTE**	**$000s**
	6,278	$1,949,544	6,151	$1,971,836	274	$88,876	6,425	$2,060,712

Strategic Objective	**PERFORMANCE MEASURE TABLE**							
	Decision Unit: Intelligence							
	Performance Report and Performance Plan Targets	**FY 2022**		**FY 2023**		**FY 2024**	**FY 2025**
		Target	**Actual**	**Target**	**Actual**	**Target**	**Target**
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%	19.6%	15%	19%	15%	15%

3. Resources and Strategies

Directorate of Intelligence (DI)

a. Performance Plan and Report for Outcomes

The FBI Intelligence Program provides insightful, timely, and actionable intelligence to protect the American people and uphold the Constitution. The FBI's DI leads efforts for the FBI to drive integration of intelligence and operations throughout the organization, enabling the FBI and its partners, including those in the Intelligence Community, to identify and mitigate current and emerging threats. A measure of progress towards this goal is reflected by the inclusion of FBI-originated reporting in IC intelligence products.

Performance Measure: Percentage of FBI IIRs used in the development of USIC intelligence products.

FY22 Target: 15 percent
FY22 Actual: 19.6 percent
FY23 Target: 15 percent
FY23 Actual: 19 percent
FY24 Target: 15 percent
FY25 Target: 15 percent

Discussion

Percentage of FBI 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 for 2024-2028 outlines the growth and evolution of FBI intelligence to meet the demands of an increasingly interconnected, mobile, and ever-changing environment. The DI is leading a team of experts and practitioners from across the enterprise to develop actions and milestones to propel the FBI's Intelligence Program into its desired future. Successful execution of this strategy will result in an integrated, agile, and innovative Intelligence Program that will bolster the FBI's ability to stay ahead of the threat, inform decision-making, and avoid surprise.

B. Counterterrorism/Counterintelligence Decision Unit

Counterterrorism/Counterintelligence Decision Unit Total	Direct Pos.	Estimate FTE	Amount ($000s)
2023 Enacted	14,054	12,882	$4,176,600
2024 Continuing Resolution	13,867	13,002	$4,348,357
Adjustments to Base and Technical Adjustments	223	223	$168,952
2025 Current Services	14,090	13,225	$4,517,309
2025 Program Increases	119	103	$47,689
2025 Request	14,209	13,328	$4,564,998
Total Change 2024-2025	**342**	**326**	**$216,641**

Counterterrorism/Counterintelligence - Information Technology Breakout (of Decision Unit Total)	Direct Pos.	Estimate FTE	Amount ($000s)
2023 Enacted			$456,520
2024 Continuing Resolution			$343,967
Adjustments to Base and Technical Adjustments			$0
2025 Current Services			$293,359
2025 Program Increases			$6,589
2025 Request			$350,549
Total Change 2024-2025			**$6,589**

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, 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 law enforcement 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 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 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 law enforcement and domestic intelligence efforts to prevent and neutralize weapons of mass destruction (WMD) threats against the homeland and support interests abroad. The WMDD unifies law enforcement authorities, intelligence analysis capabilities, and technical subject matter expertise into an effective national approach to preventing and responding to WMD threats.

Preparing, assessing, and responding to WMD threats and incidents is challenging because WMD 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, law enforcement, foreign, and private sector partners – to identify, understand, and mitigate priority current and emerging WMD threats and vulnerabilities.

The FBI combined the operational activities of the 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 2023, the WMDD disrupted 42 incidents; made 62 arrests; and had 43 indictments, 56 sentencings, and 56 convictions.

Counterintelligence Program

Executive Order (EO) 12333 assigns 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 investigates and disrupts threats to America's national and economic security, both from hostile foreign nations and from insider threats. These threats include not just traditional espionage efforts, but also foreign influence operations, transnational repression, economic espionage, and critical infrastructure attacks. In response to these wide-ranging threats, the FBI, together with counterintelligence partners and other Federal law enforcement, seeks to identify the potential assets or persons targeted, engage with the appropriate stakeholders, and protect them from nefarious foreign intelligence activity. 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. Foreign governments now employ 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, especially in the growing risks of foreign malign influence operations and transnational repression activity that target U.S. democratic values and national sovereignty.

Computer Intrusion Program (Cyber)

As a law enforcement agency and a member of the Intelligence Community, the FBI has a unique lens into cyber adversary's motivations and the tactics they use to conduct their illicit activity. By combining investigative information with intelligence, the FBI can identify who is conducting the nefarious cyber activities. The level of attribution provided by the FBI not only furthers investigations but also serves as a platform for the FBI, other government agencies, international partners, and the private industry to collaborate on threat mitigation strategies and operations.

In 2020, the FBI updated its cyber strategy by reaffirming its mission to impose risk and consequences on cyber adversaries using its unique authorities, world class capabilities, and enduring partnerships to ensure the United States' safety, security, and confidence in a digitally connected world. The FBI's new strategy seeks to enhance both the capability and capacity of its workforce to conduct joint, enabled operations with its partners. Specifically, the focus of the strategy includes:

- Standardizing investigative squads across the FBI's 56 FOs consisting of agents, analysts, and technical-trained personnel.
- Developing tools to further internal investigations, joint operations, and information sharing with domestic and international partners and private industry.
- Leveraging the National Cyber Investigative Joint Task Force (NCIJTF) to address significant ransomware threats and illicit activity surrounding virtual currency.
- Recruiting, hiring, retaining, and training a highly-skilled cadre of personnel who can conduct cyber investigations, collect technical evidence, and support operations which address and combat cyber threats.
- Increasing the FBI's ability to intake, analyze, enrich, and share cyber threat intelligence and information.
- Cultivating and maintaining enduring partnerships with domestic/international partners and private industry.

The new cyber strategy has proven effective since its implementation and its success is best illustrated in the July 2022 take down of the Hive ransomware group. Through its unique authorities, the FBI penetrated Hive's networks and captured its decryption keys. Leveraging its partnerships both domestically and abroad, the FBI notified over a thousand potential targets and victims from key critical infrastructure sectors worldwide and spared them from nearly $130 million in ransom demands. This operation highlights the FBI's comprehensive, whole-of-society approach to combatting cyber threats and intrusions, leveraging the FBI's unique authorities, technical capabilities, and global partnerships to disrupt ransomware attacks and provide tangible support to victims. Notwithstanding operational success stories such as the disruption of the Hive ransomware group, without sufficient personnel, technical, and development resources, the FBI will not be able to scale its success or remedy the long list of unattributed cyber cases.

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 law enforcement 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 law enforcement 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 FOs. 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 program, performing both detect, track, locate, and identify 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. CIRG encompasses all of these elements.

Legal Attaché Program

Legats are the forward element of the FBI's international law enforcement effort and often provide the first response to crimes against the U.S. and its citizens that have an international nexus. The counterterrorism component of the Legat program is comprised of 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	**Actual**		**Target**		**Changes**		**Requested (Total)**	
	FY 2023		**FY 2024**		**Current Services Adjustments and FY 2025 Program Change**		**FY 2025 Request**	
Total Costs and FTE (reimbursable FTE are included, but reimbursable costs are bracketed and not included in the total)	**FTE**	**$000s**	**FTE**	**$000s**	**FTE**	**$000s**	**FTE**	**$000s**
	13,228	$4,289,582	13,002	$4,348,357	327	$216,640	13,328	$4,564,997

Strategic Objective	**PERFORMANCE MEASURE TABLE**							
	Decision Unit: Counterterrorism/Counterintelligence							
	Performance Report and Performance Plan Targets	**FY 2022**		**FY 2023**		**FY 2024**	**FY 2025**	
		Target	**Actual**	**Target**	**Actuals**	**Target**	**Target**	
KPI (DOJ Objective 2.2)	Number of terrorism disruptions effected through investigations.	600	438	600	405	600	600	
KPI (DOJ Objective 2.1)	Number of counterintelligence program disruptions or dismantlements.	400	402	400	494	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.	5%	25.7%	5%	14%	5%	5%	
KPI/FYs 22-23 (DOJ Objective 2.4)	Percent of reported ransomware incidents from which cases are opened, added to existing cases, or resolved within 72 hours.	45%	39.4%	65%	47%	65%	65%	

Strategic Objective	PERFORMANCE MEASURE TABLE						
	Decision Unit: Counterterrorism/Counterintelligence						
	Performance Report and Performance Plan Targets	FY 2022		FY 2023		FY 2024	FY 2025
		Target	Actual	Target	Actuals	Target	Target
KPI (DOJ Objective 2.4)	Percent increase in operations conducted jointly with strategic partners.	3%	16%	3%	-38%	3%	3%
KPI (DOJ Objective 2.4)	Percent increase in threat advisories disseminated to the private sector.	5%	4.2%	5%	-5%	5%	5%
FYs 22-23 (DOJ Objective 2.4)	Increasing the number of ransomware matters in which seizures or forfeitures are occurring by 10%.	5%	15%	10%	0%	N/A	N/A
*N/A is listed above when the measure was not readily tracked by the FBI prior to the new DOJ Strategic Plan for FY 2022 – FY 2026.							

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 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.

FY22 Target: 600
FY22 Actual: 438
FY23 Target: 600
FY23 Actual: 405
FY24 Target: 600
FY25 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 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, Tribal, State, local, 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 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.

Counterintelligence Division (CD)

a. Performance Plan and Report for Outcomes

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

The expanded scope of sensitive American assets of interest to strategic competitor states coupled with a continually evolving technological environment opens new security vulnerabilities, particularly around foreign malign influence and transnational repression operations. 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 the 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.

FY22 Target: 400
FY22 Actual: 402
FY23 Target: 400
FY23 Actual: 494
FY24 Target: 400
FY25 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 four 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 increased whole-of-government coordination through the National Counterintelligence Task Force (NCITF), providing nationwide coordination with Federal law enforcement and IC partners on the model of successful drug and counterterrorism joint task forces. The NCITF supports counterintelligence task forces in all 56 FOs, 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 Strategy 4: Protect Sensitive Assets. 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 the protection of critical infrastructure.

Cyber Division (CyD)

a. Performance Plan and Report for Outcomes

CyD's strategy to combat cyber-based threats and attacks focuses on deterring, disrupting, and prosecuting cyber adversaries by leveraging the FBI's unique authorities, world-class capabilities, and enduring partnerships. As such, CyD aims to impose risk and consequences on cyber adversaries by increasing: (1) disruptions of malicious cyber actors' use of online infrastructure through proactive FBI cyber operations and judicial means; (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 and, (3) operations conducted jointly with strategic partners – including public, private, and international stakeholders – 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 work with the private sector and other government agencies to share vital information they can use to strengthen their cyber defenses and resilience, specifically by increasing the number of threat advisories disseminated to the private sector.

CyD also 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.

FY22 Target: 5 percent
FY22 Actual: 26 percent
FY23 Target: 5 percent
FY23 Actual: 14 percent
FY24 Target: 5 percent
FY25 Target: 5 percent

Performance Measure: Percent of reported ransomware incidents from which cases are opened, added to existing cases, or resolved within 72 hours.

FY22 Target: 45 percent
FY22 Actual: 39 percent
FY23 Target: 65 percent
FY23 Actual: 47 percent
FY24 Target: 65 percent
FY25 Target: 65 percent

Performance Measure: Percent increase in operations conducted jointly with strategic partners.

FY22 Target: 3 percent
FY22 Actual: 16 percent
FY23 Target: 3 percent
FY23 Actual: -38 percent
FY24 Target: 3 percent
FY25 Target: 3 percent

Note: *Joint, sequenced operations with other government agencies, foreign partners, and the private sector have achieved tremendous impact in degrading those cyber actors who wish to do the U.S. harm – and remain a priority for the FBI moving forward. Quarterly and annual tallies of these operations depend on a variety of factors, including the accumulation of sufficient intelligence, timing, coordination with other agencies, and the actions of targeted actors. This KPI metric considers joint intelligence products, which often inform and lead directly to joint operations. The volume of joint intelligence production can ebb and flow throughout the year based on staffing/personnel changes, the needs and interests of our partners, the number and frequency of significant cyber incidents, the rates of collection and processing of complex and voluminous data, and the FBI's collaboration with other agencies to glean actionable intelligence. The NCIJTF remains the FBI's key liaison in coordinating complex, joint operational efforts among the USG to combat malicious cyber activity. To further the cyber mission, the FBI continues to make great strides in forging deep and cooperative relationships*

with both foreign and domestic partners as well as with the private sector, including academia and critical infrastructure entities. The FBI is renewing guidance to Field Offices for tracking and claiming appropriate accomplishments for this important measure. FY 2023 Q4 is a percent decrease from FY 2022 Q4.

Performance Measure: Percent increase in threat advisories disseminated to the private sector.

FY22 Target: 5 percent
FY22 Actual: 4.2 percent
FY23 Target: 5 percent
FY23 Actual: -5 percent
FY24 Target: 5 percent
FY25 Target: 5 percent

Note: *This KPI measures the dissemination of four types of advisories from FBI's Cyber Division: Private Industry Notifications (PINs), FBI Liaison Alert System (FLASH) reports, Joint Cybersecurity Advisories (CSAs), and Public Service Announcements (PSAs). The combined figure can oscillate widely on a quarterly and annual basis based on a myriad of factors, including but not limited to professional staffing levels; contract cycles and associated personnel; the unpredictable rhythm of cyber incidents, operations, and intelligence gathering that can prompt, necessitate, and inform threat advisories; and whether threat information has already been disseminated by partner agencies or private companies. Additionally, this metric does not reflect the FBI's delivery of crucial cyber-threat information through other means, such as but not limited to intelligence sharing and collaboration with other government agencies; ongoing dialogues with foreign law enforcement and intelligence agencies; briefings, speeches, and panel participation at private-sector conferences and other gatherings; the distribution of slicksheets to the private sector by field offices; the FBI's social media presence; and media engagement by FBI staff (or the media's force-multiplying coverage of our threat advisories). The Bureau's focus with threat advisories is always on quality over quantity, and we emphasize the dissemination of threat information whenever – and as soon as – warranted. FY 2023 Q4 is a percent increase from FY 2022 Q4*

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-based threats the country faces are more diverse, more sophisticated, and more dangerous. These threats come from every corner, 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. Nation-state, surrogate, and criminal hackers operate around 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.

CyD continues to focus on enhancing strategic partnerships and technical innovation to maximize the FBI's impact and ability to disrupt, dismantle, and deter cybercriminal organizations and nation-state actors alike. To advance the mission of imposing risk and consequences on those cyber actors who wish to do America harm, the FBI relies on a unique blend of technical equipment and specially trained personnel. To this end, CyD strives to cultivate a standardized team of technically trained personnel in each of the FBI's 56 FOs. This initiative will ensure each FO 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, the broader US government, private industry (including critical infrastructure organizations), and international partners, with equal focus on network defense, intelligence, investigation, and offensive action to combat these threats. CyD is uniquely situated at the nexus of these efforts, as the FBI is both a leading intelligence and law enforcement agency. As such, CyD aims to develop and maintain 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 cyber investigations, increasing efficiency and collaboration across not only the FBI but also with the USIC, the US government as a whole and the private sector as well as intelligence and law enforcement partners around the globe.

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

C. Criminal Enterprises/Federal Crimes Decision Unit

Criminal Enterprises/Federal Crimes Decision Unit Total	Direct Pos.	Estimate FTE	Amount ($000s)
2023 Enacted	13,577	13,175	$3,716,318
2024 Continuing Resolution	13,346	13,003	$3,712,800
Adjustments to Base and Technical Adjustments	156	156	$199,576
2025 Current Services	13,502	13,159	$3,912,376
2025 Program Increases	65	61	$26,585
2025 Request	13,567	13,220	$3,938,961
Total Change 2024-2025	**221**	**217**	**$226,161**

Criminal Enterprises/Federal Crimes Decision Unit - Information Technology Breakout (of Decision Unit Total)	Direct Pos.	Estimate FTE	Amount ($000s)
2023 Enacted			$343,273
2024 Continuing Resolution			$250,476
Adjustments to Base and Technical Adjustments			$0
2025 Current Services			$250,476
2025 Program Increases			$439
2025 Request			$250,914
Total Change 2024-2025			**$438**

1. Program Description

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

- Public corruption, civil rights, international human rights, and international corruption programs.
- Financial crimes program.
- Transnational organized crime program.
- Violent crime, Indian country crime, crimes against children, human trafficking, and gang/criminal enterprise programs.
- Criminal intelligence programs and the criminal investigative components of Cyber Division's (CyD) programs, including criminal computer intrusions, the Internet Crime Complaint Center (IC3), and a share of the FBI's Legal Attaché 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.

Public Corruption, Civil Rights Crimes, and Financial Crimes

The FBI's public corruption program investigates violations of Federal law by public officials, threats to election workers and other election crimes, border corruption, law enforcement corruption, fraud against the government, and environmental crime.

The FBI's civil rights crime program works to prevent and address threats including hate crimes, color of law violations, and Freedom of Access to Clinic Entrances (FACE) Act violations.

The FBI's international human rights program works to detect and address violations of human rights including war crimes, genocide, torture, recruitment of child soldiers, providing material support to serious human rights violators, and female genital mutilation.

The FBI's international corruption program investigates criminal threats including violations of the Foreign Corrupt Practices Act (FCPA), kleptocracy, international money laundering enterprises, and antitrust violations.

The FBI's financial crimes program investigates complex financial crimes including corporate fraud, securities and commodities fraud, mortgage fraud, financial institution fraud, health care fraud, money laundering, and illicit use of virtual assets. Additionally, the program leads the FBI's assets forfeiture program.

Transnational Organized Crime, Violent Crime, and Crimes Against Children

The FBI's transnational organized crime program works to disrupt and dismantle transnational criminal organizations posing the greatest threat to the economic and national security of the United States. Transnational organized crime is a global threat that encompasses a number of criminal activities including drug trafficking, money laundering, human trafficking, alien smuggling, public corruption, weapons trafficking, extortion, kidnapping, exploitation, fraud schemes, and large-scale organized theft.

The FBI's violent crime program is dedicated to combating violent criminal threats including violent crimes occurring domestically, violent crimes committed against U.S. citizens overseas, violent gangs, major crimes within the FBI's jurisdiction on Tribal lands, crimes against children, and human trafficking.

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 law enforcement 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 law enforcement, and U.S. and foreign intelligence and security services.

The IOD and Legat program also includes a major training component, which includes efforts such as supporting international law enforcement academies and teaching law enforcement 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	**Actual**		**Target**		**Changes**		**Requested (Total)**	
	FY 2023		**FY 2024**		**Current Services Adjustments and FY 2025 Program Change**		**FY 2025 Request**	
Total Costs and FTE (reimbursable FTE are included, but reimbursable costs are bracketed and not included in the total)	**FTE**	**$000s**	**FTE**	**$000s**	**FTE**	**$000s**	**FTE**	**$000s**
	13,434	$3,780,889	13,003	$3,712,800	217	$226,159	13,613	$3,938,960

Strategic Objective	PERFORMANCE MEASURE TABLE							
	Decision Unit: Criminal Enterprises/Federal Crimes							
	Performance Report and Performance Plan Targets	**FY 2022**		**FY 2023**		**FY 2024**	**FY 2025**
		Target	**Actual**	**Target**	**Actual**	**Target**	**Target**
KPI (DOJ Objective 2.6)	Percent of crimes-against-children FBI cases which address abductions, hands-on offenders, sextortion, or enticement.	44%	54.1%	46%	65%	46%	46%
KPI (DOJ Objective 4.2)	Percent of new contacts by the FBI with foreign anti-corruption agencies that progress to mutual sharing of information or assistance or result in a new international corruption case.	60%	61.7%	60%	47%	60%	60%
KPI (DOJ Objective 4.2)	Number of criminal disruptions or dismantlements in public corruption and fraud against the government	468	407	487	320	487	

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 the DOJ and the 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

Pursuant to DOJ Strategic Objective 2.6: *Protect Vulnerable Populations*, CID will measure investigations involving abductions, hands-on offenders, sextortion, and enticement as a part of the 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 FOs 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.

FY22 Target: 44 percent
FY22 Actual: 54 percent
FY23 Target: 46 percent
FY23 Actual: 65 percent
FY24 Target: 46 percent
FY25 Target: 46 percent

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 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, non-government organizations, 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.

Financial Crimes Section

a. Performance Plan and Report for Outcomes

The prioritization of CID's strategy into elder financial exploitation investigations, outreach, training events, awareness briefings, and using 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 other FBI operational sections; conduct outreach on a national level; issue Public Service Announcements; and, provide training, guidance, and coordination to FOs, including training and tools related to the illicit use of virtual assets in investigations, in furtherance of the EJI on a state and local level.

In FY 2022, the FBI launched the Virtual Assets Unit (VAU) as 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. VAU continues to focus on strategic case support for illicit use of virtual assets across all FBI programs, including developing and improving training, providing access to equipment and blockchain analytical tools, and virtual asset seizure support. FBI CID anticipates this cross-divisional approach will further EJI focused investigations, along with other investigative matters connected to virtual assets.

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

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

Public Corruption and Civil Rights Section

Performance Measure: Percent of new contacts by the FBI with foreign anti-corruption agencies that progress to mutual sharing of information or assistance or result in a new international corruption case.

FY22 Target: 60 percent
FY22 Actual: 62 percent
FY23 Target: 60 percent
FY23 Actual: 47 percent
FY24 Target: 60 percent
FY25 Target: 60 percent

Performance Measure: Number of criminal disruptions or dismantlements in public corruption and fraud against the government.

FY22 Target: 400
FY22 Actual: 407
FY23 Target: 487
FY23 Actual: 320
FY24 Target: 487
FY25 Target: 400

Transnational Organized Crime (TOC) Global Section

a. Performance Plan and Report for Outcomes

The 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.[3] 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 and developing advanced analytical capabilities to identify criminal activity, thereby targeting the most egregious criminal actors to disrupt and dismantle transnational criminal organizations. The advantage of this strategy is by neither working nor viewing the threat in isolation, investigative personnel can both gain from and contribute to the larger law enforcement community's collective understanding and mitigation of the threat.

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 efforts, the FBI strives to ensure increased public safety.

Discussion

A **dismantlement** occurs when the targeted organization's[4] 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.

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

Each of these cells or subgroups maintains and provides a distinct function supporting the entire organization. The point in which a dismantlement will be claimed is only at the time of the conviction of the last subject in the organization and/or the conviction of the primary target of the organization/identifiable cell or subgroups.

A **disruption** is interrupting or inhibiting a threat actor from engaging in criminal or national security related activity. A disruption is the result of direct actions and may include but is not limited to the arrest; seizure of assets; or impairing the operational capabilities of key threat actors. A disruption should be claimed in conjunction with an affirmative law enforcement action (e.g., Arrest, Indictment, Conviction, Seizures) and/or regulatory action that impedes the normal and effective operation of the targeted criminal enterprise as indicated by changes in the organizational leadership or methods of operation (e.g., including but not limited to financing, trafficking patterns, communications, or drug production). An affirmative law enforcement action resulting in multiple arrests, seizures, indictments, or convictions of an organization's members should be reported as one disruption of that organization.

b. Strategies to Accomplish Outcomes

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

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

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.

D. Criminal Justice Services Decision Unit

Criminal Justice Services Decision Unit Total	Direct Pos.	Estimate FTE	Amount ($000s)
2023 Enacted	2,703	2,384	$625,016
2024 Continuing Resolution	2,602	2,535	$643,007
Adjustments to Base and Technical Adjustments	59	59	$44,699
2025 Current Services	2,660	2,593	$687,706
2025 Program Increases	80	68	$20,566
2025 Request	2,740	2,661	$708,272
Total Change 2024-2025	**138**	**126**	**$65,265**

Criminal Justice Services -Information Technology Breakout (of Decision Unit Total)	Direct Pos.	Estimate FTE	Amount ($000s)
2023 Enacted			$358,269
2024 Continuing Resolution			$110,713
Adjustments to Base and Technical Adjustments			$10,207
2025 Current Services			$120,920
2025 Program Increases			$4,928
2025 Request			$125,848
Total Change 2024-2025			**$15,135**

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 law enforcement 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 law enforcement, 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 law enforcement 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.

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 the 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 of 99.78 percent and exceeds all availability and accuracy performance goals.

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 99.99 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 99.10 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. On average, Tenprint Rap Sheet (TPRS) submissions are processed within six seconds. Criminal Answer Required (CAR) submissions are processed within six 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; 45,734,030 in FY 2020; 47,762,026 in FY 2021; 62,335,282 in FY 2022; and 74,091,712 for all of FY 2023. 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 law enforcement 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 December 21, 2023, the ULF consisted of 1,213,152 unidentified latent prints contributed by Federal, State, local, and international law enforcement agencies, as well as LD and members of the United States Intelligence Community from evidence within both criminal and terrorism investigations. An enhanced latent search algorithm was deployed on February 26, 2023, to further refine latent search accuracy.

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 November 30, 2023, the collection contains more than 28 million unique subjects from more than 63 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.

The NGI CJ Rap Back Services are designed to provide immediate notifications to law enforcement on an NGI Identity of subscribed individuals currently under an active criminal investigation, active probation, or parole (custody and supervision).

As of November 2023, four of the largest submitting agencies include the Transportation Security Administration (TSA) Precheck, TSA Transportation Worker Identification Credential (TWIC), the TSA, and the State of Texas. The TSA Precheck, TSA TWIC, and the TSA have enrolled 11,621,112; 1,184,330; and 1,415,035 Rap Back subscriptions respectively from

numerous airports and airlines throughout the United States. Texas enrolled 5,038,263 Rap Back subscriptions including teachers, nurses, and EMS workers.

Repository for Individual of Special Concern (RISC) – The NGI System added RISC in FY 2011, containing over 4.8 million fingerprint records of wanted persons, registered sex offenders, immigration violators, Terrorist Screening Center subjects, and Foreign Subjects of Interest as of November 30, 2023. The 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 FY 2023, the RISC service processed more than 732,000 rapid mobile identification searches, responding with over 88,000 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 1,892 individuals with altered fingerprints and researched each record to ensure accuracy. In FY 2023, the ABIP staff identified and researched 407 new identities with altered fingerprints. In addition, the ABIP staff monitored and researched 501 fingerprint transactions relating to subsequent activity of individuals known to have altered their fingerprints and reviewed 10,583 fingerprint transactions in which an individual known to have altered their fingerprints appears on a candidate list in the NGI System. The ABIP staff are anticipating the implementation of an automated altered fingerprint detection within the NGI System, which will enhance the ability to detect, research, and correct records associated with altered fingerprints.

Deceased Persons Identification (DPI) Services – In FY 2020, 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 FY 2023, the NGI System processed 46,353 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 more identifications, bringing the overall deceased identification rate up to 70 percent. 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 November 30, 2023, the NGI Iris Service consists of over 3.3 million sets of iris images representing more than 2.6 million unique identities. There are 722 domestic and international contributors from over 300 agencies participating in the NGI Iris Service. In FY 2023, there were 2,842 Iris Identification Searches conducted with 2,547 identifications returned.

The NGI Interstate Photo System (IPS) provides enhanced photo enrollment, retrieval, search, and maintenance capabilities. These enhancements permit broader acceptance and use 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 FY 2023, the NGI IPS held over 146.7 million criminal and civil photos contributed by Federal, State, local, Tribal, and select foreign and international agencies that consisted of over 30 million unique identities. Over 67.4 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 agencies to submit investigative face photos (probe photos) for an automated FR search of the NGI IPS. First, the law enforcement agencies FR systems must be programmed to handle the FR types of transactions as specified in the *Electronic Biometric Transmission Specifications, version 11.0*. law enforcement 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. 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 November 17, 2019, improving FR algorithm accuracy to over 99 percent. CJIS Systems Agency/State Identification Bureau must ensure all authorized law enforcement agencies take approved training prior to conducting investigative FR searches of the NGI IPS. In addition, FBI policies and procedures emphasize photo candidates returned are not to be considered "positive identifications." Further investigation must be performed before making an arrest. In FY 2023, 34,014 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) query (QR) can be made with an 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 2023:

- Name Based Queries (QH) – 473,153,236
- Quoted UCN or SID Queries (QR) – 53,814,060
- Total number of incoming III transactions – 526,967,296

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, 4) challenge/appeal the reason for their firearm-related denial, and 5)

submit a Voluntary Appeal File for firearm-related requests. 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 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, Terrorist 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 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 percent over the past 12 months. Providing essential information to law enforcement officers, investigators, judges, prosecutors, correction officers, court administrators, and other law enforcement and criminal justice agency officials in the execution of their day-to-day operations, the NCIC contains over 18.4 million active records and processes an average of 10.8 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 law enforcement 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.

The Bipartisan Safer Communities Act (BSCA) expanded background checks for persons under the age of 21 (U21) to include juvenile criminal and mental health records. This requires three additional record checks of the following entities where the prospective U21 firearm transferee resides:

1. State criminal history or juvenile justice system information,
2. State custodian of mental health adjudications; and
3. Contact with the local law enforcement agency.

The BSCA requires the NICS Section to perform a three business day background check to determine if a potential prohibiting juvenile criminal or mental health adjudication exists under 18 U.S.C. 922 § (d), (g), or (n), or State, local, or Tribal law for all persons under the age of 21. The Act also requires the system to notify the licensee if cause exists to further investigate potential disqualifying juvenile record within that three-business-day time frame.

In addition, 18 U.S.C. § 922(a)(1)(C)(iii) requires the NICS Section, when cause exists, to continue research for a ten-business-day time period if receipt of a firearm would violate 18 U.S.C. § 922 (d) or subsections (g) or (n), or State, local, or Tribal law.

Since the implementation of the U21 background checks in October of 2022, the NICS has denied 502 transactions of persons under the age of 21 with information that would not have been available without the passage of the BSCA.

Firearm background checks may be conducted by either the CJIS NICS Section or a State or local law enforcement agency serving as an intermediary between an FFL and the NICS Section. These intermediaries are referred to as points of contact (POCs). The NICS Section provides full service to the FFLs in 31 states, five U.S. territories, and the District of Columbia. NICS provides partial service to five states. The remaining 14 states perform their own checks using the FBI provided NICS interface.

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 Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) 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.

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. In FY 2023, NICS processed 30,551,065 total transactions compared to 31,670,108 in FY 2022, a four percent decrease.

NICS Alert Service – 28 CFR § 25.9 allows for NICS to share NICS Audit Log information that indicates a violation or potential violation of law or regulation with the appropriate investigating law enforcement agency. Information available on the NICS Audit Log, not yet destroyed, could contain delayed or open transactions up to 88 days, proceeded transactions within the last 24 hours, and any previously denied transactions. This service recently rebranded as the NICS Alert Service (NAS), formally known as the NICS Monitoring Service (NMS), has been used by the ATF since 2009, the FBI since 2014, and other Federal agencies on a case by case basis. Approved subjects of investigative interest are enrolled for up 180 days of monitoring and are eligible for renewal through the life of the investigation. Both the ATF NAS and FBI NAS require an active case investigation meeting certain legal thresholds for entry. While subjects of interest are enrolled in NAS, law enforcement agencies are alerted near real time to past NICS Audit Log activity and when a subject of interest attempts to purchase a firearm. While a subject of interest in enrolled in NAS, research is conducted to identify Federal firearms prohibitions for these threat actors.

Threat Triage Team – The mission of the NICS Threat Triage Team (TTT) is to leverage the FBI CJIS Division to detect and disrupt acts of targeted violence by persons of concern. The purpose of the NICS TTT is to provide situational awareness to an FBI FO (FO) of a person(s) with violent tendencies who may pose a threat to themselves or the community. The TTT will accomplish this by:

- Detecting reliable indicators of impending violence, particularly when driven or enhanced by mental distress
- Researching CJIS systems and other relevant data sources for information that may provide clues as to the likelihood and imminence of violence, including criminal history, adjudicated mental defective (AMD) status, and other information that may shed light on the individual's level of escalation to violence
- Disseminating the findings in a clear, succinct package to appropriate FBI field personnel to enable rapid assessment, intervention, and ultimately, disruption; and
- Logging the information to enable investigators to research previously disseminated information about an individual if s/he is subsequently encountered, enabling more effective escalation detection over time

Bioterrorism Risk Assessment Group – The Bioterrorism Risk Assessment Group (BRAG) completes bioterrorism security risk assessments by conducting research of various databases including the Next Generation Identification System, Department of Homeland Security Automated Biometric Identification System, National Crime Information Center, Department of Defense, Veteran's Affairs, FBI Indices, the Royal Canadian Mounted Police's Real Time Identification System, and the U.S. Immigration and Customs Enforcement databases. The BRAG analyzes data to determine if a subject meets the Federal categories as established by Congress of persons restricted from accessing biological select agents and/or toxins. The BRAG serves as a resource for weapons of mass destruction coordinators in the field since it houses personally identifiable information, fingerprints, and photos on approximately 10,000 individuals who possess, use, or transfer biological select agents and/or toxins.

Criminal History Analysis Team – The Criminal History Analysis Team's (CHAT) mission is to provide exceptional customer service to appellants by responding to all initial firearm background check denial challenges within the mandated five business day deadline as well as perform in-depth reviews of available criminal history records, requesting record modifications, and detailing case specifics when positive identification has been determined through fingerprint comparison on individuals requesting the reasons, they were denied the purchase of a firearm. In addition, the passage of the Fix NICS Act modified the Brady Handgun Violence Prevention Act, of 1993 to require a 60-day determination on firearm denial challenges once the NICS Section receives information to correct, clarify, or supplement the record. The CHAT also performs analysis and evaluations on an individual's eligibility to be entered into the Voluntary Appeal File (VAF) to prevent erroneous denials or extended delays on future firearm transactions.

On October 19, 2023, an agreement between the ATF and FBI NICS was finalized, allowing individuals to use administrative appeals processes of FBI NICS to attempt to resolve record related issues that are revealed during a NICS background check, initiated as part of the individual's National Firearms Act (NFA) application. In addition, the agreement recognizes an NFA applicant may use the VAF when NICS responds with a "delayed" recommendation to the NFA applicant's background check. The "delayed" or "denied" NFA applicant will receive a letter from NFA Division advising how to take advantage of each respective process and the associated NICS Transaction Number (NTN) for "denied" NFA applications. As part of this process, applicants may be requested to submit an additional set of fingerprints.

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 from the 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. The additional personnel were directly responsible for NICS maintaining the Attorney General (AG) goal of a 90 percent immediate determinate rate. The NICS program has successfully met the AG goal for 23 consecutive months. Without the additional personnel provided in the supplemental appropriations noted above, NICS would not have been successful in processing new regulatory and legislative background checks.

The NICS Section continues to operate with thirteen IT Development teams. The highest priority continues to be automation of specific functions of the firearm background check process to reduce volume hitting the workforce. However, the need for continuous maintenance to ensure the system is operating at maximum capacity during "busy season" has recently taken precedence. Further, a massive effort to redesign portions of the NICS application identified as cumbersome by those processing NICS transactions has injected an influx of work into an already large backlog. This is taking place in conjunction with requirements for the interface to be Section 508 compliant.

In addition, the development teams continue to support more than 400 enhancements that are critical for the continued development of the NICS. Some of the highlighted efficiencies and automation efforts are listed below:

- Expansion of the NICS Alert Service is being considered to provide valuable notifications to State and local law enforcement agencies on their subjects of interest when they are attempting to purchase a firearm.
- The creation of a response portal wherein external agencies receiving requests for information from the NICS can log in to a secure location within the NICS application and provide responses at their discretion.
- The filtering/removal of non-prohibitive information from data sources being reviewed to make firearm determinations.
- The creation of a service and subsequent messaging that provides an option to POC and non-POC states (especially in instances for disaster recovery) that allows them to conduct their own background checks directly within the NICS application and therefore eliminate the need to maintain their own State systems.
- Regularly, individuals that purchase firearms are repeat buyers. Further, in the event an individual is "delayed" at a Federal firearms licensee, they attempt to purchase elsewhere in the same timeframe. There has been a major effort to automatically link transactions for the same individual so that duplicative work for the same purchaser does not take place. The automation of this "chaining" will greatly reduce volume once complete.

The changes and efficiencies carried in the NICS product backlog continues to grow and are prioritized to ensure 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 law enforcement since 1930. The FBI collects, analyzes, reviews, and publishes the data collected from participating Federal State, local, Tribal, and territorial partners. The UCR program collects information through the National Incident-Based Reporting System (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 law enforcement 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.

Law Enforcement Enterprise Portal (LEEP) – The FBI's LEEP is a gateway for thousands of users in the criminal justice, intelligence, and military communities to gain access to critical data protected at 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 (N-DEx) – The 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 compliments 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 900 million searchable records from over 8,500 criminal justice agencies and provides access to an additional 380 million records from the 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 FBI FOs, 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 determine the threat level associated with the information provided, determine if the information needs immediate action, and refer the information to the appropriate FBI entity or other appropriate law enforcement agency for action. NTOC works 24 hours a day, 365 days a year, 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.

NTOC received and processed over 1.2 million calls and electronic tips in FY 2023, including 7,000 plus TTL tips to FOs and fusion centers. 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. FO users can listen to audio recordings of NTOC's telephonic complaints and request certified copies for official use. FO users can set customized search subscriptions for persons or topics of interest and receive email notifications when a new record at NTOC matches their query. NTOC provides TIPS demonstrations and feedback sessions with users throughout the Bureau to increase awareness of TIPS and gather requirements for future system enhancements. NTOC provides TIPS submitter training to Bureau employees, allowing them to send tips to NTOC for triage in place of forwarding emails and phone calls. 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 law enforcement and intelligence agencies, and some foreign law enforcement 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 law enforcement partners, both at the FBI Academy and throughout the U.S. at State, regional, and local training facilities. The principal course for State and local law enforcement officers is the 10-week multi-disciplinary course at the FBI National Academy. These training sessions cover the full range of law enforcement training topics, such as hostage negotiation, computer-related crimes, and arson.

Training Division held four National Academy sessions in FY 2022, with a total student count of 1,088. In FY 2023, Training Division graduated four National Academy sessions with a total student count of 921 students, which included 99 international students for 11 percent of the student body. In FY 2024, Training Division anticipates graduating four sessions with 200 students per session for a total of 800 students with 100 of those from foreign countries, or 12.5 percent of the student population.

International Operations Division

Due to the increasingly global nature of many of the FBI's investigative initiatives, the FBI has in recent years emphasized the need to train its foreign law enforcement partners through the international training and assistance program.

2. Performance and Resource Tables

PERFORMANCE AND RESOURCES TABLE								
Decision Unit: Criminal Justice Services								
RESOURCES	**Actual**		**Target**		**Changes**		**Requested (Total)**	
	FY 2023		**FY 2024**		**Current Services Adjustments and FY 2025 Program Change**		**FY 2025 Request**	
Total Costs and FTE (reimbursable FTE are included, but reimbursable costs are bracketed and not included in the total)	**FTE**	**$000s**	**FTE**	**$000s**	**FTE**	**$000s**	**FTE**	**$000s**
	2,650	$655,985	2,534	$643,006	126	$65,266	2,660	$708,272

E. All Decision Units

1. Performance Table

Strategic Objective		PERFORMANCE MEASURE TABLE					
		Decision Unit: All Decision Units					
	Performance Report and Performance Plan Targets	FY 2022		FY 2023		FY 2024	FY 2025
		Target	Actual	Target	Actual	Target	Target
KPI/FYs 22 – 23 Agency Priority Goal (3.3)	Percent of Federal law enforcement officers equipped with Body Worn Cameras (BWCs) and associated training.	5%	6.8%	38%	33%	75%	100%
KPI/FYs 22 – 23 Agency Priority Goal (3.3)	Percent of Special Agents who receive Use of Force Sustained Training within a 3-year period.	85%	98%	95%	96.8%	95%	95%

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 (DAG) to devise, construct and implement a Body Worn Camera (BWC) capability within the FBI, the BWC Program was initiated to develop and spearhead a multi-phase roll-out strategy designed to deliver a fully operational, enterprise-wide BWC capability in FY 2023. This aligns with the FBI enterprise objective to Strengthen Confidence and Trust by allowing for more transparency n 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 OTD, ITADD, CIRG, CID, Training Division, RPO, OGC, and FFD, as well as multiple FOs. 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. Phase I of BWC implementation pilot program involved training and equipping agents in the Washington FO. Beginning in April 2022, the BWC program launched Phase II, delivering BWC capability to four additional FOs (Miami, Milwaukee, Atlanta, and New York) and two FBI HQ components (CIRG/SWAT/HRT and the FBI Academy New Agent Training Program). Phase III is underway, equipping 15 additional FOs in calendar year 2023, bringing the total number of offices with BWCs to 20.

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 and associated training.

FY22 Target: 5 percent
FY22 Actual: 7 percent
FY23 Target: 38 percent
FY23 Actual: 33 percent
FY24 Target: 75 percent
FY25 Target*:* 100 percent

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 FOs. 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 scheduled initial delivery of 500 camera systems by late February 2022. Phase 3 of BWC implementation is now complete, with 24 FOs being equipped with BWCs, surpassing the original Phase 3 goal of 20. Phase 4 began in January 2024, with a goal of onboarding the remaining 31 FOs by September 2024. In January 2024, five FOs were onboarded: Sacramento, San Francisco, Las Vegas, San Diego, and Los Angeles. Two offices will onboard in February and four additional offices in March. The onboarding process continues to run smoothly and BWC implementation has been well received across FOs. The backend infrastructure is fully operational (with additional feature development ongoing) and has been performing extremely well. The decision to utilize FBI infrastructure has proven to be cost effective. In summary, 29 of the FBI's FOs have deployed BWCs with nearly 5,000 agents trained and equipped. Approximately 1,500 pre-planned search and/or arrest operations have successfully utilized the BWC with over 10,000 evidence items created.

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

a. Performance Plan and Report for Outcomes

In support of DOJ Strategic Objective 3: *Reform and Strengthen the Criminal and Juvenile Justice Systems to Ensure Fair and Just Treatment*, specifically the APG: *Promoting Trust in Law Enforcement through Transparency*, TD provides Use of Force training to all new agents at the FBI Academy, which teaches proper use of force for escalation and de-escalation. To ensure continued adherence to use of force protocols, and in support of FBI's fifth mission priority, *Protect Civil Rights*, the FBI provides mandatory annual training on use of force to all onboard FBI Special Agents and Police Officers. The 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.

FY22 Target: 85 percent
FY22 Actual: 98 percent
FY23 Target: 95 percent
FY23 Actual: 96 percent
FY24 Target: 95 percent
FY25 Target: 95 percent

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 all onboard FBI Special Agents and Police Officers.

b. Strategies to Accomplish Outcomes

On September 13, 2021, the DAG issued a memorandum to the FBI and components related to the use of force, emphasizing a shared obligation to lead by example in a way that engenders the trust and confidence of the communities that it serves. The FBI's existing and continued training to both new and onboard FBI Special Agents and FBI Police Officers 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 to include de-escalation to all new FBI special agents at the FBI Academy and at a minimum, in collaboration with OGC, provide Use of Force training annually for onboard FBI Special Agents and FBI Police Officers.

V. Program Increases by Item

Item Name: **Cyber**

Strategic Goal(s): 1, 2, 3, 4
Strategic Objective(s): 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: Cyber

Program Increase: Positions 12 Agt/Atty 4 FTE 6 Dollars $7,000,000 ($3,231,000 non-personnel)

Description of Item

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

Item Name: **Counterintelligence**

Strategic Goal(s): 1, 2, 3, 4
Strategic Objective(s): 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: Counterintelligence

Program Increase: Positions 44 Agt/Atty 14 FTE 22 Dollars $17,792,000 ($6,150,000 non-personnel)

Description of Item

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

Item Name: **National Instant Criminal Background Check System**

Strategic Goal(s): 2
Strategic Objective(s): 2.3
Budget Decision Unit(s): Criminal Justice Services (CJS)

Organizational Program: Criminal Justice Information Services

Program Increase: Positions 27 Agt/Atty 1 FTE 14 Dollars $8,433,000 ($4,928,000 non-personnel)

Description of Item

National Instant Criminal Background Check System (NICS): 27 positions (1 SA) and $8,433,000 ($4,928,000 non-personnel)

The FBI requests 27 positions (one agent) and $8,433,000 ($4,928,000 non-personnel) to support statutorily required firearm background checks. The FBI strives to provide a critical service to U.S. citizens in ensuring their safety amidst those who choose to exercise their Second Amendment rights and requests these resources to strengthen national criminal background check processes.

Justification

The NICS program serves a critical role in enhancing 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 no-fail mission, the NICS program requires sufficient personnel and technical resources.

In FY 2022, the FBI was appropriated $100.0 million in supplemental funding as part of the Bipartisan Safer Communities Act (BSCA) to meet resource requirements for the NICS program. This funding is supporting 170 additional positions (two agents) and key Information Technology (IT) investments to address two major Federal directives (the NICS Denial Notification Act and the BSCA) as well as a transaction volume 25 percent higher than pre-pandemic years. While one major requirement of the BSCA has yet to be fully implemented, the FBI anticipates additional near-term growth in the overall volume of background checks.

The BSCA amended section 103(b) of the Brady Handgun Violence Prevention Act (34 U.S.C. 40901(b)) by adding subsection (2) voluntary background checks. This revision will allow licensees to use NICS for the purposes of voluntary employment background checks relating to a current or prospective employee (i.e., Firearm Handler Checks). As this unprecedented NICS background check has yet to be implemented, metrics are not currently available. However, as NICS serves approximately 50,000 Federal firearms licensees, the FBI conservatively estimates an impact of approximately 750,000 additional checks per year.

For the FBI to meet emerging critical public safety mandates, the Bureau requires further NICS resources in FY 2025, beyond the annualization of the 170 positions funded by the BSCA. The 27 new positions included in this request will strengthen the program's ability to complete Firearm Handler Checks.

Based on the estimated number of transactions expected for under the age of 21 (U21) and Firearm Handler Check (FHC) background checks, the FBI estimated it would need 51 NICS examiners to process U21 and FHC background checks. However, due to processing challenges experienced with U21 background checks, the FBI is utilizing 61 NICS examiners to perform only U21 background checks. The FBI has drafted recommended Federal regulation changes required for the implementation of FHCs. The FBI is working toward the publication of regulations on the remaining provisions to include NICS checks for FFL employment. The implementation of the FHCs is dependent on the public comment period and the responses needed. The Notice of Proposed Rule Making for Firearm Handler Checks is currently with the DOJ, who will submit it to the Office of Information and Regulatory Affairs for notice and comment in the Federal Register. . As previously stated, the number of transactions and the number of employees needed to process may increase or decrease based on the outcome of the FHC regulation. Once the FHCs are implemented, further evaluation of processes will be needed to determine sufficient staffing levels.

In addition to the Firearm Handler Checks, the FBI continues to move forward with the implementation of enhanced background checks before any sale or transfer of a firearm to a person under the age of 21. U21 background checks have three prongs for outreach – criminal history contacts, mental health contacts, and local law enforcement contacts. Under BSCA, NICS is required to conduct three additional record checks for potential transferees whose ages are 18-20 years old. These expanded checks are to determine whether the potential transferee has a possible disqualifying juvenile record. In addition to the FBI's routine outreach for information pertaining to criminal history, mental health, and law enforcement, a follow up call is made to non-responsive agencies. On average, the FBI makes approximately 2,000 calls per week. As of January 16, 2024, the response rate for receiving documents relevant to expanded backgrounds from these agencies is as follows:

- Criminal history contacts – 66.3 percent
- Mental health contacts – 69.2 percent
- Local law enforcement contacts – 60.2 percent

These background checks are labor intensive and additional personnel are required to conduct direct outreach to local agencies who are unresponsive to NICS requests. Without this enhancement, the FBI would need to divert NICS resources from traditional background checks to support U21 local agency outreach.

During the implementation of the BSCA, it was identified that additional outreach, marketing, and training would be necessary to have a successful response rate from agencies that are contacted for dispositions, police reports, and mental health information. The U21 background check process now utilizes 61 positions solely for this effort. Between U21 transactions and FHCs, it was estimated that 51 NICS examiners would be able to process these expanded checks. However, based on the number of FHCs anticipated, along with the employees processing U21 checks currently, the FBI estimates 99 employees would be needed to process these expanded checks. Considering the 27 positions requested, and maintaining the current U21 staffing level of 61 positions, the FBI currently estimates a deficit of 11 positions and will continue to evaluate and refine estimates for personnel requirements.

Since the U21 background check process was implemented, the response rate for all three prongs of research (criminal history, mental health, and law enforcement) has increased by approximately thirty percent due to additional outreach and follow up requests being conducted by NICS employees.

The FBI is also requesting one Special Agent position to support critical external law enforcement and internal FBI collaboration. The SA will work closely with NICS business and liaison personnel on outreach to FBI FOs as well as State and local law enforcement partners regarding NICS capabilities and gaps. The SA will attend FO briefings and consult with other SAs and Supervisory Special Agents regarding specific case needs and overarching division goals. The SA will provide support to the NICS Alert Service (NAS) team in streamlining their processes and creating products more accessible to FO personnel. The NAS allows FBI FOs and the ATF to submit qualified biographic information to NICS and request enrollment. Once approved, the biographic information in the NICS audit log is both reviewed to determine if the subject of interest (SOI) had any previous NICS background checks, and monitored 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 personnel resources, the FBI is requesting $4,928,000 in non-personnel funding to sustain system development via a team of contracted resources. NICS reprioritized system improvements to ensure successful implementation of the BSCA requirements, which subsequently delayed those relating to automation efforts. One example of a delayed system improvement is NICS transaction number (NTN) chaining, which would provide systematic recognition when multiple transactions exist for the same individual and automatically link the subsequent transactions to the original. An additional improvement delayed during the implementation of BSCA requirements was the Predictable Learning Automation of the NICS (PLAN) functionality, which would greatly improve the efficiency of NICS processing by eliminating a significant volume of data requiring manual processing by NICS staff. There are improvements for the PLAN included in the FY 2025 Program Increment schedule.

This enhanced funding in FY 2025 will assist NICS developers in expanding the NICS Alert Service, wherein FBI FOs and the ATF enroll subjects of interest. This service sends the FO or the ATF a notification if/when their SOI attempts to purchase a firearm. There are plans to expand this capability to State and local law enforcement agencies as well as other Federal agencies. This will require the creation of a new user interface to allow for entries and several other technical enhancements.

The NICS development effort utilizes an agile 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 NICS is dependent on system improvements 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. Maintenance and system upgrades will reduce the number of "bug fixes" necessary. Reducing required

system fixes will allow the FBI to proceed with new system improvements rather than performing rework to correct issues. Furthermore, completion of the migration to an XML communication platform is critical to gaining efficiencies. The FBI will be able to put forth system enhancements that allow for complete automation once the NICS and the State systems are able to communicate, thus reducing the need for manual review of agency responses.

Impact on Performance

The NICS program is anticipating continued growth in firearm background checks with unprecedented checks involving U21 purchasers and Firearm Handler Checks resulting from the BSCA. As firearm background checks continue to grow and evolve, additional personnel and system enhancements are integral to maintaining the NICS Immediate Determination Rates and providing accurate and timely determinations on firearm purchasers to ensure public safety. The BSCA also requires the NICS program to make system modifications to the firearm background check process. The technological demands and enhancements require the NICS program to prioritize these modifications to meet implementation deadlines as required by the BSCA.

Funding

1. **Base Funding**

FY 2023 Enacted				FY 2024 Continuing Resolution				FY 2025 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
1129	0	1,094	$132,691	1,129	2	1,094	$117,015	1,129	2	1,094	$165,952

2. **Personnel Increase Cost Summary**

Type of Position/Series	FY 2025 Request ($000)	Positions Requested	Full Year Modular Cost per Position ($000)	Annualizations ($000)			
				2nd Year	3rd Year	FY 2026 (net change from 2025)	FY 2027 (net change from 2026)
Information Technology	$274	2	$217	$86	$61	$172	$122
Professional Support	$282	2	$201	$35	$103	$70	$206
Special Agent, Field	$438	1	$534	($66)	$153	($66)	$153
NICS / NTOC	$2,295	20	$162	$18	$57	$370	$1,140
Clerical	$215	2	$157	$32	$56	$64	$112
Total	$3,505	27	$1,271	$105	$430	$610	$1,733

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

Non-Personnel Item	FY 2025 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2026 (net change from 2025)	FY 2027 (net change from 2026)
IT System Development	$4,928	N/A	N/A	$0	$0
Total Non-Personnel	**$4,928**	**N/A**	**N/A**	**$0**	**$0**

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

The NICS program costs for non-personnel funding is driven by multiple system modifications created by the BSCA and the continued development of the system. To sustain system development for the future of the NICS, non-personnel funds are required to identify system vulnerabilities, correct operational defects, and continue enhancement of NICS for a faster and more accurate firearm background check determination. Due to the expected increase in firearm background checks, it is essential for the NICS program to continue upgrading the system to ensure public safety and support those individuals exercising their Second Amendment rights. The NICS program requests the annualization of non-personnel funds to continue critical technological advancements.

5. **Total Request for this Item**

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2026 (net change from 2025)	FY 2027 (net change from 2026)
Current Services	1,129	2	1,094	$125,123	$40,829	$165,952	N/A	N/A
Increases	27	1	14	$3,505	$4,928	$8,433	$610	$1,733
Grand Total	**1,156**	**3**	**1,108**	**$128,628**	**$45,757**	**$174,385**	**$610**	**$1,733**

6. **Affected Crosscuts**

Gun Safety, Mass Violence

Item Name:	**Restoration of 2023 National Security and Law Enforcement Personnel**
Strategic Goal(s):	1, 2, 3, 4
Strategic Objective(s):	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:	All

Program Increase: Positions 270 Agt/Atty 65 FTE 270 Dollars $85,363,000 ($20,000,000 non-personnel)

Description of Item

Restoration of 2023 National Security and Law Enforcement Personnel: 270 positions (60 SA) and $85,363,000 ($20,000,000 non-personnel)

As of formulation of the FY 2025 request to Congress, an FY 2024 Appropriation had not yet been passed. Therefore, the starting point for the FY 2025 President's Budget for Salaries and Expenses is the annualized FY 2024 continuing resolution (CR), which is equal to the FY 2023 Enacted level. At this reduced level, the FBI cannot afford its current operational workforce. To account for necessary inflationary adjustments, the FBI estimates it will be required to reduce approximately 900 headquarters positions, including 200 agents, through attrition and reduced hiring under an FY 2024 CR. Any actual position reductions will depend on the outcome of the FY 2024 appropriation.

The FY 2025 President's Budget restores these 900 headquarters positions and associated funding through a combination of a technical adjustment of 630 positions and $149.0 million, plus this program increase. The positions requested to be restored through the technical adjustment and program increase are included in the table below.

	FY 2024 CR Reduction		FY 2025			
			Technical Adjustment		Program Increase	
Program	**Special Agent**	**Total**	**Special Agent**	**Total**	**Special Agent**	**Total**
Counterterrorism	-32	-98	20	61	12	37
Criminal Investigative	-30	-61	18	37	12	24
Criminal Justice Information Services	-3	-81	2	33	1	48
Critical Incident Response	-41	-70	24	40	17	30
Intelligence	-8	-65	5	40	3	25
Human Resources	-3	-27	3	27	0	0
National Security Management	-1	-2	1	2	0	0
Science & Technology	0	-2	0	0	0	2
Finance and Facilities	-1	-62	1	59	0	3
Information Management	-1	-40	1	39	0	1
Insider Threat	-1	-4	1	4	0	0
Inspection	-5	-10	5	10	0	0
International Operations	-9	-19	6	12	3	7
Information Technology	-2	-45	2	45	0	0
Laboratory	-5	-53	3	22	2	31
Executive Offices	-14	-53	14	53	0	0
General Counsel	-2	-23	2	15	0	8
Operational Technology	-16	-65	9	28	7	37
Security	-5	-52	5	51	0	1
Terrorist Screening	-1	-13	1	7	0	6
Training	-13	-32	13	32	0	0
Victim Services	0	-1	0	0	0	1
Weapons of Mass Destruction	-7	-22	4	13	3	9
Total	**-200**	**-900**	**140**	**630**	**60**	**270**

While this increase in resources will permit the FBI to mitigate the loss of positions, there remains an ongoing impact on non-personnel resources. Specifically, non-personnel reductions will be applied across all operational and support functions, including but not limited to, training and development opportunities for FBI personnel; contract support for efforts that address national security and law enforcement priorities; partnerships with State, local, international, and other Federal agencies; software, hardware, and technological equipment updates and maintenance; and direct support to case-related requirements.

Justification

The threats the Nation faces have never been greater or more diverse, and the expectations placed on the FBI have never been higher. The FBI's work can be seen in communities across the country through efforts to thwart international terrorists and hostile foreign intelligence services; investigations of sophisticated cyber-based attacks and internet-facilitated sexual

exploitation of children; and operations targeting violent gangs and transnational criminal organizations. It is imperative the FBI has the necessary resources to confront these threats. The 270 positions (60 SAs) and $85,363,000 ($20,000,000 non-personnel) included in this request will restore the remaining portion of the positions the FBI anticipates eliminating in FY 2024 due to budget shortfalls. While final decisions have not yet been made, the following list is a preliminary delineation of the 270 positions the FBI requests to restore in FY 2025:

- Criminal Justice Information Services: 48 positions including one Special Agent
- Counterterrorism: 37 positions including 12 Special Agents
- Operational Technology: 37 positions including seven Special Agents
- Laboratory: 31 positions including two Special Agents
- Critical Incident Response: 30 positions including 17 Special Agents
- Criminal Investigations: 24 positions including 12 Special Agents
- Intelligence Production: 25 positions including three Special Agents
- Weapons of Mass Destruction: nine positions including three Special Agents
- General Counsel: eight positions, including five Attorneys
- International Operations: seven positions including three Special Agents
- Terrorist Screening: six positions
- Operational Support (including Finance and Facilities, Information Management, Science and Technology, and Security): seven positions
- Victims Services: one position

Restoring these positions is critical to enabling the FBI to address its most important threat areas.

Countering terrorism remains the FBI's number one priority. The recent, brutal Hamas attack against Israel reminded anyone who had forgotten the threat of terrorism is real and dangerous – both abroad and right here at home. The FBI is responding to increased threats to the homeland from both international terrorist organizations and lone actors focused on targeting faith-based communities. The FBI is also tracking and countering potential terrorist threats from individuals who enter the country unlawfully, including over the southern border – a monumental task given the often sparse information available on their whereabouts and associates.

The U.S. faces many criminal threats, including financial and health care fraud; organized transnational and regional criminal enterprises; crimes against children; human trafficking; violence against election personnel; and public corruption. Criminal organizations – both domestic and international – as well as individual criminal activity represent a significant threat to security and safety for U.S. citizens. Given the violence seen in communities across the nation, a reduction in the FBI's efforts to curb this brutality is extremely harmful to the American people. Each day, the FBI works with its law enforcement partners to investigate cartel leadership to thwart efforts to exploit U.S. borders and traffic dangerous drugs across the country. Keeping pace with these threats is a significant challenge for the FBI.

The FBI not only investigates complex crimes, but also strives to assist victims in navigating the aftermath of a crime and the criminal justice process with dignity, respect, and resilience. Victims services personnel deploy to crisis and mass casualty events across the nation and support these victims even when the FBI is not the lead investigative agency.

The FBI provides many technical and scientific services to State, local, Tribal, Federal, and intelligence community partners. For instance, the Operational Technology program assists State and local agencies with digital forensics on child sexual exploitation cases, internet fraud,

and financial crimes. The FBI Laboratory provides over 20 different forensic science disciplines (DNA analysis, forensic facial imaging, latent fingerprint analysis, general chemistry, toxicology, cryptanalysis, firearms toolmarks, gunshot residue, bullet trajectory, shoeprint and tire tread identification, etc.) to State, local, and Tribal law enforcement agencies, in addition to supporting FBI investigations. In FY 2023, the FBI Laboratory processed over 4,000 submissions of evidence, almost half in support of violent crimes, taking ruthless offenders off the street. The FBI Laboratory has been deployed 65 times in support of large-scale complex crime scenes and mass casualty events, including Colleyville, TX; Buffalo, NY; and Highland Park, IL. The FBI Laboratory must be appropriately staffed to address its investigative caseload.

In addition to technical and scientific support, the FBI provides real-time sharing of criminal justice information to State, local, Tribal, and territorial law enforcement partners. Specifically, the National Threat Operations Center (NTOC) receives approximately 4,000 calls and e-tips a day – many of which involve threats to life or situations when getting information quickly to FBI FOs or State and local law enforcement is literally a matter of life and death. The FBI also operates the National Crime Information Center (NCIC) – a computerized database of documented criminal justice information available to virtually every law enforcement agency nationwide (90,000 State and local law enforcement agencies), 24 hours a day, 365 days a year – which is accessed 10 million times per day. This system has kept local officers safe by identifying passengers in traffic stops as terrorists, fugitives, and other violent offenders, before potentially violent interactions occur.

The $20.0 million in non-personnel funding will restore the resources required to support these 270 positions by ensuring they have adequate facilities, supplies, equipment, travel funding and contract support. Personnel require these resources to fulfill their work roles. Functional and safe facilities are the foundation for an effective workforce. The ability to purchase new and replacement equipment is critical to protecting against cybersecurity risks. Travel funding is required to allow personnel to: receive mandatory training, travel across the FBI's field office footprint to support investigations, and attend conferences and other developmental opportunities. Contract support, including contracts for investigative tools and technologies, is vital to the FBI's national security and criminal capabilities.

Impact on Performance

The outcome of the FY 2024 appropriation will determine the actual number of positions the FBI must reduce and thus the number of positions to be restored in FY 2025.[5] Restoring these positions and the associated funding in FY 2025 will lessen the long-term impact of any FY 2024 reductions on the FBI's ability to fulfill its mission. With these positions and funding restored in FY 2025, the FBI will also be able to better serve partner agencies. Examples of functions performed by these restored headquarters positions include but are not limited to the following:

- Supporting field investigations of national security and criminal threats;
- Conducting digital forensics to identify and rescue trafficked and exploited children;
- Surging to local communities to rescue U.S. citizens through the Hostage Rescue Team;
- Conducting watchlisting, screening and intelligence information sharing functions at the Terrorist Screening Center;
- Addressing Freedom of Information Act (FOIA) requests from the public; and
- Deploying in response to requests for victim assistance throughout the country.

[5] The FBI will provide an update upon enactment of a FY 2024 appropriation.

Funding

1. **Base Funding**

FY 2023 Enacted				FY 2024 Continuing Resolution				FY 2025 Current Services			
Pos	Agt/ Atty	FTE	($000)	Pos	Agt/ Atty	FTE	($000)	Pos	Agt/ Atty	FTE	($000)
270	65	270	$85,363	0	0	0	$0	0	0	0	$0

2. **Personnel Increase Cost Summary**

Type of Position/Series [6]	FY 2025 Request ($000)	Positions Requested	Full Year Modular Cost per Position [4] ($000)	Annualizations ($000)			
				2nd Year	3rd Year	FY 2026 (net change from 2025)	FY 2027 (net change from 2026)
Intelligence Analysts [5]	$9,804	40	$245	$0	$0	$0	$0
Professional Support [5]	$34,892	165	$211	$0	$0	$0	$0
Attorneys [5]	$1,057	5	$211	$0	$0	$0	$0
Special Agent [5]	$19,609	60	$327	$0	$0	$0	$0
Total Personnel	**$65,363**	**270**	**$994**	**$0**	**$0**	**$0**	**$0**

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

The request includes non-personnel resources to support the restored positions.

[6] Personnel costs reflect an estimated average cost of the position reduction in the FY 2024 budget. As a result, only for this enhancement, personnel funding does not align to the FBI's standard position cost modules.

Non-Personnel Item	FY 2025 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2026 (net change from 2025)	FY 2027 (net change from 2026)
Services	$12,083	N/A	N/A	N/A	N/A
Land and Structures	$3,080	N/A	N/A	N/A	N/A
Equipment	$2,406	N/A	N/A	N/A	N/A
Travel and Transportation of Persons	$1,579	N/A	N/A	N/A	N/A
Rent, Communication, and Utilities	$454	N/A	N/A	N/A	N/A
Supplies and Materials	$393	N/A	N/A	N/A	N/A
Printing and Reproduction	$5	N/A	N/A	N/A	N/A
Total Non-Personnel	**$20,000**	**N/A**	**N/A**	**N/A**	**N/A**

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

The non-personnel resources represent recurring costs required to support personnel. As a result, this funding should be fully annualized.

5. **Total Request for this Item**

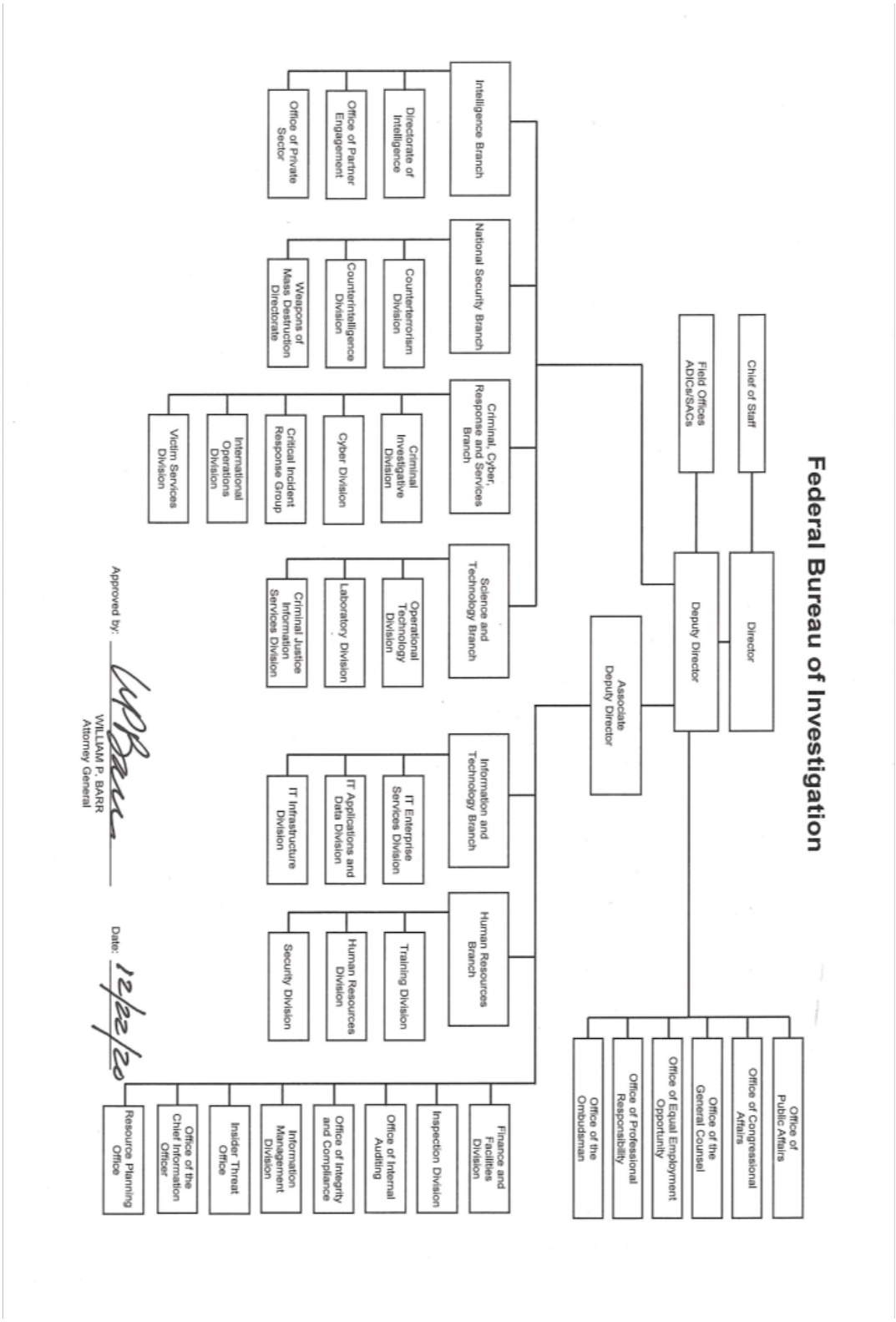
Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2026 (net change from 2025)	FY 2027 (net change from 2026)
Current Services	0	0	0	N/A	N/A	N/A	N/A	N/A
Increases	270	60	270	$65,363	$20,000	$85,363	$0	$0
Grand Total	**270**	**60**	**270**	**$65,363**	**$20,000**	**$85,363**	**$0**	**$0**

6. **Affected Crosscuts**

All crosscuts are affected.

VI. EXHIBITS

A. Organizational Chart

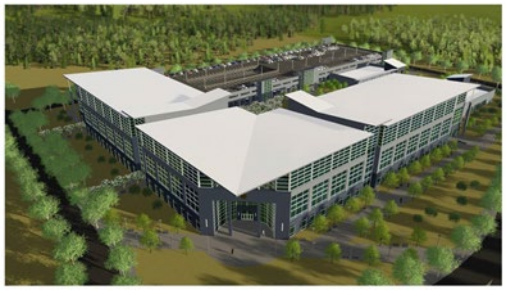


VI. CONSTRUCTION

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 law enforcement 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, law enforcement, 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 with a capacity to house approximately 330 personnel to monitor the FBI's network 24/7/365, provides network monitoring and insider threat detection essential to the protection of sensitive intelligence and information for the entire organization. A 250,000-square-foot Innovation Center to be delivered in FY 2024 seats 366 employees, provides shared seat capacity for up to 540 trainees and dedicated seat capacity for up to 200 trainees, and includes a state-of-the-art Kinetic Cyber Range.

The South Campus provides tremendous growth opportunities for the FBI and its law enforcement partners. The recently constructed Ballistics Research Facility (BRF) is the world's only law enforcement 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 law enforcement criminal proceedings.

The current and future FBI Redstone facilities discussed 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 not only trains FBI employees – it also hosts the best and brightest law enforcement personnel from around the world for 10 weeks at the National Academy and for 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 law enforcement 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 several other 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 law enforcement, national security, intelligence partners, and 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 Central Records Complex (CRC) in Winchester, Virginia, has the capacity to house approximately 1.7 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 FOs 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: The FBI has occupied the J. Edgar Hoover (JEH) building since 1974. Since that time, the infrastructure, including mechanical, electrical, and life and safety systems, has deteriorated as the FBI's mission expanded and evolved. The Administration recognizes the critical need for a new FBI headquarters and has begun a multi-year process of constructing a modern, secure facility from which the FBI can continue its mission to protect the American people.

In November 2023, the General Services Administration (GSA) selected Greenbelt, MD as the site on which to construct a Federally owned facility for at least 7,500 FBI headquarters personnel. The FBI identified serious concerns with the site selection process, and Congress and the GSA Office of Inspector General are conducting independent reviews of the process. While these reviews take place, the FBI and GSA are engaged in construction planning efforts.

The FY 2025 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, the FBI and GSA continue efforts to identify a Federally owned 750-1,000 seat location in the District of Columbia, which will allow the FBI to maintain close proximity to the DOJ and other law enforcement and government 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

VII. GLOSSARY	
ADIC	Assistant Director in Charge
Agt	Special Agent
AOR	Area of Responsibility
ATB	Adjustments to Base
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
Atty	Attorney
BRF	Ballistics Research Facility
BWC	Body Worn Camera
C2	Command and Control
CAC	Crimes Against Children
CAC/HT	Crimes Against Children/Human Trafficking
CARD	Child Abduction Rapid Deployment Team
CCRSB	Criminal, Cyber, Response, and Services Branch
CD	Counterintelligence Division
CEFC	Criminal Enterprises and Federal Crimes
CHRI	Criminal History Record Information
CI	Counterintelligence
CIA	Central Intelligence Agency
CID	Criminal Investigative Division
CIRG	Critical Incident Response Group
CJ	Criminal Justice
CJIS	Criminal Justice Information Services
CJS	Criminal Justice Services
COL	Color of Law
CP	Counterproliferation
CPOT	Consolidated Priority Organization Target
CST	Child Sex Tourism
CT	Counterterrorism
CT/CI	Counterterrorism/Counterintelligence
CTD	Counterterrorism Division
CyD	Cyber Division
DAG	Deputy Attorney General
DHS	Department of Homeland Security
DI	Directorate of Intelligence
DOD	Department of Defense
DOJ	Department of Justice
DT	Domestic Terrorism
DU	Decision Unit
EAD	Executive Assistant Director
eDO	Electronic Departmental Order
EO	Executive Order
EVC	Enterprise Vetting Center
FACE	Freedom of Access to Clinic Entrance
FBI	Federal Bureau of Investigation
FFD	Facilities and Finance Division

VII. GLOSSARY	
FFL	Federal Firearms Licensee
FHC	Firearm Handler Checks
FLP	Foreign Language Program
FO	FO
FTE	Full-time Equivalent
FY	Fiscal Year
GRU	Russian Military Intelligence
HDS	Hazardous Devices School
HQ	Headquarters
HQC	Headquarters City Offices
HRB	Human Resources Branch
HRD	Human Resources Division
HRT	Hostage Rescue Team
HT	Human Trafficking
HVE	Homegrown Violent Extremists
IA	Intelligence Analyst
IAFIS	Integrated Automated Fingerprint Identification System
IB	Intelligence Branch
IC	Intelligence Community
IC3	Internet Crime Complaint Center
IDU	Intelligence Decision Unit
III/Triple I	Interstate Identification Index
IIR	Intelligence Information Reports
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
ISIS	Islamic State of Iraq and ash-Sham
IT	Information Technology
ITADD	IT Applications and Data Division
ITB	Information and Technology Branch
ITESD	IT Enterprise Services Division
ITID	IT Infrastructure Division
JCODE	Joint Criminal Opioid and Darknet Enforcement
LD	Laboratory Division
LEEP	Law Enforcement Enterprise Portal
MAPA	Management and Program Analyst
MENACE	Mobile Encrypted Networks and Communications Exploitation
NAS	National Air Space
NCAVC	National Center for the Analysis of Violent Crime
NCIJTF	National Cyber Investigative Joint Task Force
NCITF	National Counterintelligence Task Force

VII. GLOSSARY	
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
NGI	Next Generation Identification
NIBRS	National Incident-Based Reporting System
NICS	National Instant Criminal Background Check System
NIP	National Intelligence Program
NITTF	National Insider Threat Task Force
NPPS	National Palm Print System
NSA	National Security Agency
NSB	National Security Branch
NTOC	National Threat Operations Center
NTP	National Threat Priority
NVTC	National Virtual Translation Center
OCA	Office of Congressional Affairs
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
OIC	Office of Integrity and Compliance
O&M	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
ORTA	Office of Research and Technology
OTD	Operational Technology Division
POC	Point of Contact
PS	Professional Staff
PS	Professional Support
RA	Resident Agency
RBS	Rap Back Services
RPO	Resource Planning Office
RSA	Redstone Arsenal
RSCIAT	Richard Shelby Center for Innovation and Advanced Training
S&E	Salaries and Expenses
SA	Special Agent
SAC	Special Agent in Charge
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCINet	Sensitive Compartmented Information Network
SecD	Security Division

VII. GLOSSARY	
SID	State Identification Number
SIIG	Strategic Intelligence Issues Group
SLTT	State, Local, Tribal, and Territorial
SOG	Special Operations Group
SSG	Special Surveillance Group
STB	Science and Technology Branch
SWE	Secure Work Environment
TAG	Transnational Anti-Gang Task Force
TCO	Transnational Criminal Organizations
TD	Training Division
TEDAC	Terrorist Explosive Device Analytical Center
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
UCN	Universal Control Number
UCR	Uniform Crime Reporting
ULF	Unsolved Latent File
UNet	Unclassified Network
US	United States
USG	United States Government
USIC	United States Intelligence Community
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