U.S. Department of Justice
Federal Bureau of Investigation

FY 2027 FBI Budget Request to Congress

March 2026

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

I. Overview

A. Introduction

Budget Request Summary: The Federal Bureau of Investigation's (FBI's) Fiscal Year (FY) 2027 Budget request proposes a total of $12,530,273,000 in direct budget authority, of which $12,500,273,000 is for Salaries and Expenses (S&E) and $30,000,000 is for Construction.

The S&E request includes a total of 37,702 direct positions and 35,538 direct full-time equivalents (FTE). The positions include:

- 14,190 Special Agents (SAs)
- 3,016 Intelligence Analysts (IAs)
- 20,496 Professional Staff (PS)

The S&E program increases total $1,181,432,000; 2,050 positions (568 SAs, 77 IAs, and 1,405 PS); and 1,046 FTE for the following:

- $94,300,000 for Intelligence Community (IC) support
- $105,000,000 for national security system cybersecurity requirements
- $311,668,000 to combat violent crime
- $166,077,000 for counterterrorism
- $95,620,000 for cyber operations
- $73,215,000 for counterintelligence
- $111,120,000 for cybersecurity
- $144,775,000 for field investigative capabilities
- $29,432,000 for advanced training at Redstone Arsenal
- $18,941,00 to combat insider threats
- $31,284,000 for transparency of government and promoting public trust

The request includes $363,319,000 in technical adjustments and $346,066,000 in adjustments to base (ATBs) for continued support of the FBI's base operations.

Electronic copies of the Department of Justice's (DOJ) congressional budget submissions can be viewed or downloaded from: http://www.justice.gov/doj/budget-and-performance.

The FBI Strategy: The mission of the FBI is to *Protect the American People and Uphold the Constitution of the United States.* The FBI strategy has four priorities to drive its work and support its no-fail mission to make America safe: *Crush Violent Crime, Defend the Homeland, Rebuild Public Trust, and Fierce Organizational Accountability*.

The FBI Mission: To protect the American people and uphold the Constitution of the United States.

DOJ Strategic Goals: The FBI contributes to the achievement of the DOJ Strategic Goals: DOJ's Strategic Goals for FY 2026-2030 have not been finalized.

FBI Priorities:

- Crush Violent Crime
- Defend the Homeland
- Rebuild Public Trust
- Fierce Organizational Accountability

The FBI tracks the execution of its priorities—via the FBI Strategy process—by cascading priorities and executing strategic initiatives within branch and division strategies. This vertical alignment within the organization ensures the FBI enterprise is strategically focused on the same priorities and is working collectively toward the FBI Mission. Strategy review meetings are held with Operations Directors (ODs) and each branch and division to discuss progress toward the priorities, Key Performance Indicators (KPIs), and Key Strategic Initiatives (KSIs) throughout the fiscal year. FBI executive management routinely evaluates the organization's progress.

- KPIs capture the organization's performance, enabling data-driven decisions and measuring progress toward the mission of protecting the American people.
- KSIs are high-priority projects, sponsored by ODs to ensure leadership support across FBI Headquarters (HQ) divisions. KSIs range from short, high-priority efforts (e.g. Operation Summer Heat) to longer, major efforts. KSIs expand the FBI's capabilities and advance the FBI Strategy.

On an ongoing basis, HQ 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 over 60 Legat offices use this national guidance to formulate a field and Legat office threat prioritization and complete their own specific strategies. These threat and program strategies undergo mid-year and end-of-year evaluations, and each field and Legat office is held accountable to its strategy performance. FBI executives and program managers hold regular meetings to review and evaluate 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 will allow the FBI to build upon its historic, record-breaking achievements in FY 2025 and FY 2026, while also focusing on the future needs of the FBI. The FY 2027 budget request is designed to promote agile capabilities and strategies 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—supporting the larger FOs and enabling 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. In FBI FOs, Special Agents in Charge (SACs) report to the ODs, and Assistant Directors in Charge (ADICs) report directly to the Deputy Directors.

The FBI also operates 63 Legats and 37 sub-offices in 84 countries around the world. These offices are typically staffed with fewer than 10 people, who liaise with foreign counterparts and partners. These numbers fluctuate based on the global threat environment.

FBI HQ provides centralized operational, policy, and administrative support to FBI investigations and programs. Under the direction of the FBI Director and Deputy Directors, this support is provided by:

- The National Security Branch (NSB), which includes the Counterterrorism Division (CTD), the Counterintelligence Division (CD), the Directorate of Intelligence (DI), and the Threat Screening Center (TSC).
- The Criminal and Cyber Branch (CCB), which includes the Criminal Investigative Division (CID), the Cyber Division (CyD), the International Operations Division (IOD), and the Victim Services Division (VSD).
- The Field Services Response Branch (FSRB), which includes the Criminal Justice Information Services (CJIS) Division, the Critical Incident Response Group (CIRG), the Laboratory Division (LD), and the Operational Technology Division (OTD).

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

- The Infrastructure Branch (IB) oversees the IT Applications and Data Division (ITADD), the Information Management Division (IMD), the Office of the Chief Information Officer (OCIO), and the IT Infrastructure Division (ITID).
- The Human Capital Branch (HCB) includes the Human Resources Division (HRD), the Inspection Division (INSD), the Security Division (SecD), and the Training Division (TD).
- Administrative and Financial Management Support is provided by the Finance and Facilities Division (FFD), the Resource Planning Office (RPO), and the Office of Professional Responsibility (OPR).
- Specialized support is provided directly to the Director and Deputy Directors through several staff offices, including the Office of Engagement, the Office of Congressional Affairs, the Office of the General Counsel (OGC), the Office of Equal Employment Opportunity Affairs (OEEOA), and the Office of the Ombuds.

Budget Structure: The FBI's S&E funding is appropriated among four decision units (DUs), 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 DUs 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 DU. For example, all the

resources of the DI are allocated to the Intelligence DU, while all the resources of the CJIS Division are allocated to the CJS DU.

- Based on workload: Critical investigative enablers, such as the LD, the IOD, and the OTD, are allocated to the DUs based on workload. For example, 21 percent of the LD's workload is in support of CT investigations and, accordingly, 21 percent of the LD's resources are allocated to the CT/CI DU. These percentage assignments may be revised upon review of workload.
- Pro-rated across all DUs: Administrative enablers, such as the IBIB, the FFD, and the HRD, are pro-rated across all four DUs 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 United States 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 Integrated Program Management (IPM) and Threat Review and Prioritization (TRP) processes.

Transnational Criminal Organizations (TCOs): While still engaged in many of the traditional organized crime activities of loansharking, extortion, and murder, modern criminal enterprises have expanded to activities such as stock market fraud and manipulation, cyber-facilitated bank fraud and embezzlement, Darknet 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.

To address the persistent and ever evolving threat of Darknet drug trafficking, the FBI manages the Joint Criminal Opioid and Darknet Enforcement (JCODE) initiative. JCODE employs a comprehensive, enterprise-focused strategy designed to identify, disrupt, and dismantle criminal networks responsible for the production, distribution, and monetization of illicit drugs—particularly those leveraging Darknet marketplaces, cryptocurrency, and foreign-sourced precursor chemicals. JCODE strategically integrates narcotic, cyber, and financial and organized crime experts from 13 Federal law enforcement organizations and works alongside state and local partners nationwide. JCODE further extends its reach through close collaboration with Europol and foreign law enforcement partners to address global supply chains, financial flows, and infrastructure enabling these networks.

Foreign Terrorist Organizations (FTOs): In accordance with Executive Order (EO) 14159, Protecting the American People Against Invasion, the National Security Council (NSC) directed the establishment of Homeland Security Task Forces (HSTFs). Each HSTF is tasked to dismantle cartels and foreign gangs designated as FTOs and TCOs across the United States. The HSTF is co-led by the FBI and Homeland Security Investigations (HSI). Thirty regional HSTF offices and 29 satellite offices have been established and are fully operational, providing coverage across all 50 states, the District of Columbia, and U.S. territories.

The HSTF mission is to identify, investigate, and prosecute TCOs and FTOs engaged in complex, multi-faceted criminal activity. This task force construct is the first of its kind, employing a whole-of-government model to fight FTOs and TCOs by consolidating all of U.S. law enforcement, military, and intelligence efforts into a targeted approach, eliminating duplicative investigations and providing a more organized effort in combatting these threats. HSTFs differ from Joint Terrorism Task Forces (JTTFs) by focusing on complex, cross-border TCOs with a prosecution-driven end state, while JTTFs remain focused on foreign and domestic ideological terrorism.

The HSTFs have over 9,000 Federal agents, Task Force Officers (TFOs), and analysts dedicated to the mission. Those Federal components are joined by over 440 state and local agencies across the country; High Intensity Drug Trafficking Areas program partners; and hundreds of Intelligence Community (IC) analysts, Department of War (DOW) analysts, and Legats worldwide. The combined resources coordinate global efforts to achieve total elimination of these organizations' presence in—and their ability to threaten the territory, safety, and security of—the United States through extraterritorial command-and-control structures.

Violent Crime and Gangs: The FBI works across jurisdictions—with Federal, state, local, and tribal partners—to fight against violent crime in big cities and small towns across the nation.

The FBI's over 200 Violent Gang Safe Streets Task Forces and Violent Crimes Task Forces work to identify and target major groups operating as criminal enterprises. 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 the FBI's investigative expertise, surveillance, technical, and intelligence resources, as well as the FBI confidential human sources (CHSs), who 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.

Crimes Against Children (CAC) and Human Trafficking (HT): The FBI has several programs to identify and arrest child predators and recover missing and endangered children, including the Child Abduction Rapid Deployment team, the Child Sex Tourism Initiative, the Innocence Lost National Initiative (ILNI), the Innocent Images National Initiative, 90 Child Exploitation and Human Trafficking Task Forces (CEHTTFs), and 91 international violent crimes against children (VCAC) TFOs from 59 countries. Giving the FBI capacity to:

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

The FBI's CEHTTFs have continued to grow, expanding to 90 CEHTTFs nationwide, including approximately 800 TFOs from Federal, state, and local agencies. In FY 2025, these task forces conducted over 3,000 arrests. The FBI's Violent Crimes Against Children International Task Force (VCACITF) has established and furthered strategic partnerships worldwide through aggressive engagement with foreign law enforcement, utilizing extensive liaison, operational support, and coordination. VCACITF is the largest task force of its kind in the world and is composed of 95 International TFOs from various agencies—including Europol and Interpol—across 66 different countries. 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 prosecute only misdemeanor violations involving native subjects, and state and local law enforcement generally do not have jurisdiction within reservation boundaries. In FY 2025, there were 1,134 arrests, 927 indictments, 113 information leads, 234 judicial complaints, and 847 convictions in Indian Country.

The FBI's Indian Country and International Violent Crime program 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. The FBI supports joint investigative efforts with the BIA-Office of Justice Services and tribal law enforcement agencies and manages 26 Safe Trails Task Forces, which include over 200 Federal, state, local and tribal partner agencies.

Civil Rights: The FBI has primary responsibility to investigate all alleged violations of Federal civil rights laws, including hate crimes, color of law, and the Freedom of Access to Clinic Entrances (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. Through training, public outreach, law enforcement support, and investigations, the FBI takes a multi-faceted approach to detect, deter, and investigate hate crimes.

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.

White Collar Crime (WCC): The WCC program addresses public corruption, border corruption, election crimes, fraud against the government, environmental crimes, fraud and illicit finance, and healthcare fraud.

Public Corruption: Public corruption involves local, state, and Federal public officials utilizing their position for personal gain, or private citizens seeking to corrupt a public official. U.S. public officials are vulnerable to exploitation from individuals, businesses, foreign actors, and criminal organizations who seek to use the official's access and influence over government spending, policies, and processes. Government fraud can severely damage public trust, U.S. border security, electoral processes, neighborhood safety, judicial integrity, and public infrastructure quality. To counter this threat, the FBI cooperates and coordinates with its local, state, Federal, and tribal law enforcement partners.

Corruption at Borders and Ports of Entry: The 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 and law enforcement officials and local police officers for corrupt criminal activity. Corrupted officials assist these entities by providing intelligence and facilitating the movement of contraband across the borders. To address this threat, the FBI established the Border Corruption Initiative to develop a threat-tiered methodology targeting border corruption at all air, sea, and land ports of entry to mitigate national security threats.

Election Crimes: Election crimes—including voter and ballot fraud, voter suppression/intimidation, threats to election workers, and campaign finance violations—affect the integrity of the U.S. electoral process. 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 two election crimes coordinators in every FO who regularly receive specialized training on election crimes and voter fraud.

Environmental Crimes: The FBI continually works to combat, disrupt, and dismantle plans to negligently, knowingly, or willfully violate Federal environmental laws. Environmental crime is often associated with a variety of other crimes, including corruption, fraud against the government, economic crime, and money laundering

Health Care Fraud (HCF): The HCF threat is evolving as technology has increased the access, ease, and ability to conduct fraud schemes. HCF losses are estimated to be in the tens to hundreds of billions of dollars each year, affecting taxpayers and U.S. health plan beneficiaries. The FBI is the only agency investigating all aspects of the HCF threat, with other Federal and state law enforcement agencies addressing individual aspects.

Domestic Terrorism (DT): For more than a century, the FBI has occupied a critical role in protecting the United States from threats to the nation's 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.

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 encouraging radicalization and mobilization to violence.

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. Additionally, in recent years, heinous assassinations and other acts of political violence in the United States have dramatically increased. Commonly, this violent conduct relates to views associated with anti-Americanism, anti-capitalism, and anti-Christianity; support for the overthrow of the U.S. Government (USG); extremism on migration, race, and gender. and hostility towards those who hold traditional American views on family, religion, and morality. In September 2025, President Trump signed National Security Presidential Memorandum-7 (NSPM-7), directing the FBI and JTTFs to coordinate a comprehensive national strategy to investigate, prosecute, and disrupt entities and individuals engaged in acts of political violence and intimidation designed to suppress lawful political activity or obstruct the rule of law. As a result, the FBI oversees the recently created NSPM-7 Joint Mission Center (JMC). The JMC is composed of personnel from 10 agencies who possess CT and criminal operational and analytical expertise. The JMC is working to counter DT and organized political violence by integrating intelligence, operational support, and financial analysis to proactively identify networks and prosecute domestic terrorist and related criminal actors.

International Terrorism (IT): The FBI currently assesses international terrorists continue to pose one of the greatest, most immediate threats to the homeland.

Homegrown Violent Extremists (HVEs) inspired by violent Sunni extremist ideology aspire to carry out attacks in the United States or travel overseas to participate in terrorist activity. Four recent HVE attacks targeted religious institutions or individuals based on religious affiliation and cited the Israel-Hamas conflict as a motivating factor in their attacks. The 2025 New Year's Day attack in New Orleans, Louisiana, targeted civilians in a crowded public area and was the

deadliest HVE attack since 2016. In the last decade, 30 of the 33 IT-related attacks in the United States. were perpetrated by HVEs.

The Islamic State of Iraq and ash-Sham (ISIS) continues to pose a threat to U.S. interests, both domestically and abroad, through the group's ability to direct, enable, and inspire attacks. ISIS seeks direct confrontation with the United States and will exploit any opportunity to attack the United States or Western interests. The FBI continues to investigate U.S.-based individuals who provide support to ISIS, including those plotting attacks, providing financial aid, or disseminating and producing propaganda.

Al-Qa'ida and its global network remain committed to attacking U.S. and Western interests domestically and abroad, but their capabilities vary by affiliate. Al-Qa'ida senior leadership and its affiliates continue to issue statements and publish media calling for attacks against the United States and U.S. interests, some of which include guidance on how to acquire materials and ways to conduct attacks to create confusion and increase casualties.

Al-Qa'ida in the Arabian Peninsula (AQAP) continues to release English-language propaganda threatening U.S. officials and encouraging lone actor attacks under its Inspire branded publications and videos. The ongoing crisis in Yemen continues to keep AQAP on the forefront of concerns.

Since the 7 October 2023 attacks, the FBI has taken proactive steps to identify, analyze, and disrupt any potential threats stemming from this conflict. As of March 2026, there is no information to indicate Hamas itself has the intent or capability to conduct operations inside the United States, though the FBI cannot, and does not, discount the possibility.

Foreign Intelligence: The FBI's statutory counterintelligence (CI) authorities make it the lead USG agency to address threats to U.S. national and economic security, preserve democratic values, and enforce the rule of law. The foreign intelligence threat targets far more than USG secrets: hostile foreign actors include criminal organizations targeting non-government information, academic researchers leveraging American grant funding for the prestige of foreign-government technology programs, and corporations profiting from evading export controls and economic sanctions. The FBI also supports international norms and the American value of free speech by countering improper foreign interference in U.S. democratic processes, including efforts to manipulate public discourse and engage in transnational repression. The FBI addresses actions by oppressive governments who seek to silence dissent both abroad and within the United States, including targeting U.S. citizens and dissidents living in the United States. The FBI continues to adapt its foreign intelligence focus to address an evolving threat environment, drawing on the full extent of available tools and legal authorities, including partnerships with other USG components and allied nations.

The FBI has unique authorities to impose legal and financial consequences on threat actors through the enforcement of statutes against espionage, sensitive information mishandling, intellectual property theft, export, and other trade restrictions in support of U.S. national security. Through collection, analysis, and operations, the FBI CI program identifies potential targets of hostile foreign actors and insider threats, engages the entities who possess those targeted assets, and protects those assets, tangible and intangible, from irreparable harm.

Cyber: Nation-state actors and cyber criminals pose a growing threat to the United States through increased 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. Cyberattacks cause 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. Additionally, the rise of cryptocurrencies enables cybercriminals, terrorists, and nation-states to acquire tools, collaborate, and launder their criminal proceeds in new and challenging ways.

The FBI'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 United States—one the FBI's blend of criminal and intelligence authorities is uniquely positioned to address.

The FBI strategically imposes costs on cyber adversaries through unique authorities, world-class capabilities, and enduring partnerships. Human and technical resources 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 (NCIJTF), 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 May 2025, the FBI, in collaboration with domestic, international, and private sector partners, took steps to disrupt the LummaC2 malware-as-a-service platform. Actions taken included the repeated disruption of LummaC2's infrastructure, repeated seizure of the user panel, the seizure of approximately 2,300 domains by private sector partners, and a joint Cybersecurity Advisory with the Cybersecurity and Infrastructure Security Agency to help victims remediate. LummaC2 is an information stealer; once installed, it searches through a user's system and steals select information, including usernames, passwords, stored credit cards, and other sensitive data. In 2025, the FBI estimated around 10 million infections could be attributed to LummaC2, which was advertised across dark web forums. Due to the success of this operation, private sector partners characterized the collaboration and information flow with the FBI as a model for future partnerships with industry.

The FBI's commitment to defending the homeland from cyber threats extends to nation-state adversaries. In December 2025, the FBI and DOJ announced the extradition of a Ukrainian national, who was federally charged for allegedly conspiring with criminal groups backed by Russian intelligence. These groups conducted dozens of cyberattacks around the world, including attacks against U.S. critical infrastructure. This action was part of the FBI's ongoing efforts to disrupt state-sponsored cyber threats to the United States and interests abroad.

C. Intelligence-Driven Operations

The FBI's NSB serves as the strategic leader of the FBI's intelligence program, driving the integration of intelligence and operations and proactively engaging with Federal, state, and local law enforcement partners; the IC; and the private sector. The NSB oversees the intelligence program implementation of its six areas of focus: technology capabilities; information sharing; collection; exploitation and analysis; workforce success; and culture and mindset.

The NSB OD works closely with stakeholders across the enterprise to manage all FBI intelligence and national security operational components, including the CD, the CTD, the CyD, the DI, the High-Value Detainee Interrogation Group, and the TSC. Additionally, the NSB 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 NSB OD heads the FBI intelligence program, ensuring national security and law enforcement intelligence collection, production, and analysis are consistent with national priorities and adhere to tradecraft standards, policies, and processes. The OD is the primary point of contact for the FBI's engagement with the Office of the Director of National Intelligence (ODNI) on NIP matters; provides oversight of the FBI intelligence workforce, CHS program, foreign language program (FLP); and serves as Executive Agent for the National Virtual Translation Center (NVTC).

The FBI uses intelligence to understand criminal and national security threats to the United States and its interests. The FBI conducts operations to dismantle or disrupt those threats and produce raw intelligence and analysis via two primary activities:

- The FBI uses a standardized model for field intelligence, adapting to the size and complexity of small, medium, large, and extra-large FOs. There are 56 field intelligence programs, one in each FBI FO.
- FBI HQ's operational and specialized divisions manage all aspects of the intelligence cycle for a unique threat or vulnerability. Intelligence programs within FBI HQ integrate intelligence and operations and collaborate across work roles to ensure intelligence drives and supports operations.

II. Summary of Program Changes

Table is Unclassified					
Package Name	**Description**	**Pos.**	**FTE**	**Dollars ($000)**	**Page**
Salaries and Expenses Enhancements					
Intelligence Community Support	Requested resources will enhance FBI programs providing capabilities in direct support to Intelligence Community partners. The programs supported by these resources are classified.	44	22	$94,300	37
National Security System Cybersecurity Requirement	The requested resources will refresh legacy encryption equipment and ensure robust maintenance and sustainment.	0	0	$105,000	38
Combatting Violent Crime	The requested resources will enhance the FBI's ability to combat the presence of criminal cartels, foreign gangs, and transnational criminal organizations across the country. Specifically, the FBI will dedicate agents to regional Homeland Security Task Forces and primary field offices to combat criminal activities, including child exploitation, violent crime, narcotics trafficking, and foreign terrorist organization designated cartels and gangs.	686	351	$311,668	39
Counterterrorism	Requested resources will allow the FBI to develop artificial intelligence (AI)-powered, cutting-edge capabilities to respond to the impacts of global terrorism events; enhance and maintain enterprise platforms supporting the U.S. Intelligence Community; continue the implementation of NSPM-7 requirements; and lead law enforcement preparations for tactical response, explosives management, and render safe operations for the 2028 Los Angeles Olympic Games.	328	167	$166,077	56

Table is Unclassified					
Package Name	**Description**	**Pos.**	**FTE**	**Dollars ($000)**	**Page**
Salaries and Expenses Enhancements					
Cyber	Requested resources will increase the FBI's capacity for both unilateral and joint-enabled, sequenced operations with other Federal, state, local, and international partners, focused on three critical areas: Victim Engagement and Incident Response; Data Management, Exploitation, and Tool Development; and Cyber Workforce Development.	152	76	$95,620	60
Counterintelligence	The requested resources will enhance the FBI's ability to combat foreign adversary intelligence collection and subversion tactics against the United States	154	79	$73,215	61
Cybersecurity	Requested resources will allow the FBI to sustain and modernize operational enclaves to include Top Secret (TS) infrastructure; secure mission-critical systems; and maintain system transparency, accountability, and operational readiness.	37	19	$111,120	62
Field Investigative Capabilities	The requested resources will improve the FBI's investigative capabilities in the digital and forensic world, improve hiring and retention of highly specialized personnel, and support the operational and technical needs of the FBI's Tactical Task Force programs.	515	265	$144,775	70
21st Century Advanced Training at Redstone	Requested resources will support student costs to attend training at Redstone Arsenal, as well as establish operational support units at Redstone Academy overseeing training coordination, logistics, and support; developing intermediate and advanced curricula; and managing the advanced training Practical Problem Venues.	46	23	$29,432	74

Table is Unclassified					
Package Name	**Description**	**Pos.**	**FTE**	**Dollars ($000)**	**Page**
Salaries and Expenses Enhancements					
Insider Threat	As required by the Trusted Workforce 2.0 certification, requested resources will enable the FBI to fully comply with mandatory vetting processes and adhere to directives, laws, and policies via personnel vetting program reform for Investigative Service Providers.	72	36	$18,941	79
Transparency of Government and Promoting Public Trust	Requested resources will protect FBI networks and ensure compliance with statutory obligations for full transparency to the public. Resources will support the prevention of unauthorized disclosures of sensitive information; mitigate insider risk and threats of workplace violence; and safeguard national security information and assets. Resources will also reduce Freedom of Information Act (FOIA) request backlogs through technological advancements to automate processes and maximize productivity with integrity and consistency across the enterprise.	16	8	$31,284	84
Salaries and Expenses Enhancements Total		**2,050**	**1,046**	**$1,181,432**	

III. Appropriations Language and Analysis of Appropriations Language

Appropriations Language for Salaries and Expenses

For necessary expenses of the FBI for detection, investigation, and prosecution of crimes against the United States, $12,500,273,000, of which not to exceed $216,900,000 shall remain available through September 30, 2028: Provided, That not to exceed $279,000 shall be available for official reception and representation expenses. Provided, That in addition to other funds provided for construction projects in this Act, the Federal Bureau of Investigation may use funding appropriated under this heading for operation and maintenance of secure work environment facilities and secure networking capabilities.

Analysis of Appropriations Language

The proposed language would modify the expiration of funds available for carryover from no-year to two-year. The proposed language would also allow the FBI to fund operation and maintenance of secure work environment facilities and secure networking capabilities from both the Salaries and Expenses and Construction accounts. Secure work environment facilities and networking requirements do not always require construction work funded from the FBI's Construction appropriation, so the flexibility to fund these requirements out of either appropriation account will allow the FBI to use funding consistent with the work being done.

IV. Program Activity Justification

A. Intelligence Decision Unit (IDU)

Intelligence DU Total	Direct Pos.	Estimate FTE	Amount ($000s)
2025 Enacted	5,877	5,850	$1,882,563
2026 Enacted	5,821	5,806	$1,888,259
Adjustments to Base and Technical Adjustments	130	135	$98,024
2027 Current Services	5,951	5,941	$1,986,283
2027 Program Increases	247	125	$156,620
2027 Request	6,198	6,066	$2,142,903
Total Change 2026-2027	**377**	**260**	**$254,644**

Program Description

The FBI's IDU is composed of the NSB, including the entirety of the DI; the intelligence functions within the CTD, CD, CyD, and CID; FO intelligence programs; the TSC; infrastructure and technology (e.g., Sensitive Compartmented Information Facilities [SCIFs] and the Sensitive Compartmented Information Network [SCINet]); and intelligence training. The IDU also includes a portion of the CIRG, FSRB, IOD, IMD, SecD, and VSD, based on the work those divisions complete in support of intelligence activities.

National Security Branch

As the leader of the FBI's intelligence program, NSB 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.

The FBI's Five-Year Intelligence Program Strategy guides NSB direction and oversight of all aspects of the FBI's intelligence work.

Directorate of Intelligence

The DI leads and 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 and inform decision-making. The DI carries out these functions through embedded intelligence elements in each FBI FO and at HQ. 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. The DI manages the Bureau Intelligence Council, composed of Senior National Intelligence Officers (SNIOs) and their deputies. SNIOs are a cadre of seasoned intelligence professionals whose work serves to amplify the FBI's perspective across the intelligence and policy communities. The DI also manages the FBI's Analytic Ombuds program, charged with upholding the IC Analytic Standards in all FBI analysis. The DI also oversees the Domestic Director of National Intelligence Representative Program, which fosters a strategic environment for unifying the IC domestically.

Intelligence Analysis

Intelligence analysis is essential to the FBI's ability to understand national security and criminal threats and develop a deeper understanding of potential and emerging 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:

- Recognize emerging threat streams to enhance domain knowledge and exploit collection opportunities;
- Enhance collection capabilities through the deployment of targeted strategies;
- Report raw intelligence in a timely manner;
- Identify and validate human and technical source collection opportunities;
- Perform domain analysis in the field to articulate the existence of a threat in a FO area of responsibility;
- Perform strategic analysis at HQ to ascertain the ability to collect against a national threat; and
- Recommend 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 current and future threat environments. FBI intelligence products also serve to inform the FBI's partners about ongoing and emerging threats.

Foreign Language Program (FLP)

The DI oversees all aspects of the FBI's FLP. The FLP provides exemplary foreign language solutions, analysis, and cultural expertise to advance the FBI's intelligence and law enforcement mission. The FBI's success in protecting the United States 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 FBI employees through ongoing language testing, assessments, and multi-tiered training strategies designed to build and sustain a high-performing intelligence workforce.

Language Analysis

Many major FBI investigations have 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 crush violent crime and defend the homeland. 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 (NVTC)

The NVTC provides timely, accurate, and agile translation services to national intelligence priorities to protect the nation and its interests. The NVTC was established under Section 907 of the USA PATRIOT Act (2001), designated an IC Service of Common Concern in 2014, and is executively managed by the FBI. Since its inception, the 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. The NVTC operates within a virtual model, connecting NVTC program staff, translators, FOs, and customers globally via a common web-based workflow management system.

Human Intelligence (HUMINT) Operations

The DI oversees all aspects of the FBI's HUMINT and CHS programs. The DI evaluates and ensures all FOs, Legats, and FBI HQ divisions manage their respective CHSs in compliance with FBI and IC 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, TFOs, and other IC/law enforcement agencies. Additionally, the DI is the primary stakeholder in the FBI's Positive Foreign Intelligence collection effort, conducting internal and external liaison with FBI operational divisions and other governmental agencies regarding HUMINT matters and coordinating cross-programmatic intelligence opportunities for CHS activities.

Ubiquitous Technical Surveillance (UTS)

The DI leads the FBI's effort to build an enterprise-wide UTS strategy to increase awareness of UTS risks across all programs and mitigate threats. The DI promotes UTS awareness and education and identifies mitigation measures through the development of tools and tradecraft. The UTS strategy ultimately safeguards operations, increases engagement with internal and external partners with technical expertise, and integrates 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. 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 intelligence and SA employees together at the beginning of their careers to underscore the importance and impact of integrated intelligence and operational methodology - a model continually utilized across the FBI's intermediate and advanced instruction courses.

Intelligence Technology

The FBI's Intelligence Technology program provides the services and applications necessary to support the intelligence mission 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 IC. Intelligence

Technology's comprehensive suite of services and applications ensures the workforce and FBI leadership have actionable intelligence necessary to support ongoing investigations, make informed decisions, facilitate opportunities, counter threats, and identify risks and vulnerabilities.

Threat Screening Center (TSC)

The TSC is a multi-agency organization administered by the FBI, responsible for managing the USG's consolidated approach to national security threat screening through watchlisting, identity resolution, encounter management, operational coordination, and information sharing. As such, the TSC manages and operates the Threat Screening System, which includes the USG's consolidated threat screening datasets for known or suspected terrorists (KSTs), non-KST military detainees, and Transnational Organized Crime (TOC) actors. Each dataset is logically separated and governed by its own nomination criteria, with potential nominations from law enforcement, the IC, and international partners. Identity intelligence contained within these datasets is provided to numerous screening, law enforcement, homeland security, and intelligence agencies as well as international partners to support threat actor screening activities.

Secure Work Environment (SWE)

The SWE program leverages SCIFs to analyze and share TS/Sensitive Compartmented Information (SCI) operational information internally and with IC and law enforcement partners. This facilitates collaborative work on national security cases in key programs, including cyber, counterintelligence, and counterterrorism. A SCIF is an accredited room or group of rooms, floors, or buildings where national security professionals collect, process, exploit, analyze, disseminate, and/or store SCI. SCIFs are outfitted with information technology (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.

B. Counterterrorism/Counterintelligence Decision Unit (CT/CI DU)

CT/CI DU Total	Direct Pos.	Estimate FTE	Amount ($000s)
2025 Enacted	13,252	12,168	$4,146,468
2026 Enacted	12,996	12,125	$4,189,469
Adjustments to Base and Technical Adjustments	302	305	$231,143
2027 Current Services	13,298	12,430	$4,420,612
2027 Program Increases	857	438	$608,592
2027 Request	14,155	12,868	$5,029,204
Total Change 2026-2027	**1,159**	**743**	**$839,735**

Program Description

The FBI's CT/CI DU encompasses the CT program, the Weapons of Mass Destruction Program (WMDP), the CI program, a portion of the Cyber/computer intrusion program, a portion of the CIRG, and the portion of the Legat program supporting the FBI's CT and CI missions.

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—or aided and abetted those engaged in—terrorist acts; and
- Provide crisis management support following terrorism acts against the United States and its interests.

The FBI aims to eliminate the risk of international and domestic terrorism by gathering intelligence from sources and using analysis to enhance prevention and exploit links between terrorist groups and their support networks. Training, finances, recruiting, logistical support, pre-attack planning, and preparation are all critical components of terrorist operations. These factors create vulnerabilities in planning and execution, and the FBI focuses on building a comprehensive intelligence base to exploit these vulnerabilities. Threat information and intelligence is shared with partner agencies to create and maintain efficient threat mitigation and provide timely and accurate analysis to the IC and senior policy makers.

The FBI is committed to stopping terrorism at any stage, from thwarting those intending to conduct an act of terrorism, to investigating those who provide financial or other support to terrorist operations. FBI HQ maintains oversight of all CT investigations, employing and enhancing a national perspective focused on creating an inhospitable terrorist environment.

The FBI has a multi-year CT strategic plan, focused on:

- 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 HUMINT to affect disruptions and help anticipate adversaries' future intentions; and
- 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 FBI has divided CT operations geographically and by threat, with each program focusing on different aspects of terrorism threats. These components are staffed with SAs, IAs, and subject matter experts (SMEs), 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 IC through daily meetings with IC executives; regular exchange of personnel among agencies; and joint efforts in specific investigations with the National Counterterrorism Center, the TSC, and other multi-agency entities.

With terrorists' broad international reach, coordination with foreign partners is crucial. The FBI has increased its overseas presence and now routinely deploys SAs and crime scene experts to assist in the investigation of overseas attacks. Their work has played a critical role in successful international operations.

Weapons of Mass Destruction Program (WMDP)

The WMDP, within the CTD, leads USG law enforcement and domestic intelligence efforts to prevent and neutralize WMD threats to the homeland and support interests abroad. The WMDP unifies law enforcement authorities, intelligence analysis capabilities, and technical subject matter expertise into an effective national approach to prevent and respond to threats.

To accomplish its unique and challenging mission to prepare, assess, and respond to WMD threats, the WMDP integrates intelligence, scientific, and technological components into WMD cases and in support of their partners.

Counterintelligence Program

The DOJ takes seriously its responsibility to investigate, disrupt, and prosecute threats to America's national and economic security, both from hostile foreign nations and from insider threats. These threats include not only traditional espionage efforts but also foreign influence operations, economic espionage, and critical infrastructure attacks to undermine confidence in the U.S.' representative democracy and way of life. In response to these wide-ranging threats, the FBI, together with CI partners and other Federal law enforcement, seeks to identify the potential assets targeted by hostile actors, engage the entities who possess those assets, and protect them.

EO 12333 assigns the FBI Director, under the Attorney General, the authority to collect foreign intelligence and conduct CI activities within the United States, including as the coordinator of joint activities by the IC. Therefore, the FBI is the lead domestic intelligence and law enforcement agency and has substantial authorities to investigate and disrupt threats to America's national and economic security. 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, and critical infrastructure sectors and disrupting the open exchange of ideas that support participatory democracy. Through partnerships, task forces, and other information sharing agreements, the FBI takes a whole-of-government approach to detect threats, deter hostile activity, neutralize threat actors, and impose consequences on nations and individuals who seek to undermine national security.

The FBI also maintains strong relationships with allied nations to collectively combat violations against international security, share information on malign influence activities in domestic politics, and jointly enforce economic sanctions against rogue regimes to counter weapons proliferation. The FBI continues to adapt its CI priorities and posture to address the evolving and multifaceted threat posed by strategic nation-state competitors who seek to reshape the international order away from a free, open, secure, and prosperous world.

Computer Intrusion Program (Cyber)

As a law enforcement agency and a member of the IC, the FBI has a unique lens into cyber adversaries' motivations and the tactics they use to conduct illicit activity. By combining investigative information with intelligence, the FBI can identify who is conducting 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.

The FBI's cyber mission is to impose costs on cyber adversaries using its unique authorities; world class capabilities; and enduring partnerships, ensuring U.S. safety; security; and confidence in a digitally connected world. The FBI's cyber strategy seeks to enhance both the

capability and capacity of its workforce to conduct joint, sequenced operations with its partners. The strategy focuses on:

- Standardizing investigative squads—consisting of agents, analysts, and technically trained personnel—across FBI field offices.
- Developing tools to further investigations, joint operations, and information sharing with domestic and international partners and private industry.
- Leveraging the NCIJTF to address significant ransomware threats and illicit activity involving virtual currency.
- Recruiting, hiring, training, and retaining a highly skilled cadre of personnel who conduct cyber investigations, collect technical evidence, support operations, and 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 and international partners and private industry.

The FBI has relentlessly pursued disruption opportunities against the entire spectrum of cyber threats. In September 2025, the FBI and United Kingdom (UK) partners secured the arrest of a key member of Scattered Spider, a cybercriminal group linked to 120 network intrusions and more than $115.million in ransom payments. The arrest followed a takedown of a major source of malware in LummaC2, demonstrating the FBI's success in targeting both cyber criminals and their supporting infrastructure.

The FBI has been equally relentless in pursuit of nation-state cyber adversaries. In July 2025, FBI personnel worked with Italian partners to secure the arrest of Chinese espionage hacker Xu Zewei. The FBI also collaborated with many domestic and international agencies to release a critical advisory for defending against Salt Typhoon, a Chinese Communist Party-sponsored group that attacked the telecommunications sector and the privacy of Americans and allies around the globe. The FBI was able to put threat-hunting guidance in the hands of network defenders and notify at least 80 victim countries.

Critical Incident Response Program (CIRG)

CIRG facilitates the FBI's readiness, response, and resolution to critical incidents and special events, integrating tactical response, negotiation, behavioral analysis and assessments, surveillance, hazardous device detection, render safe programs, Counter-Unmanned Aircraft Systems (C-UAS), and crisis management resources. CIRG personnel are on call to respond to crisis incidents requiring immediate law enforcement response, support FBI special event planning and coordination, and provide specialized training to FBI field personnel and state, local, Federal, tribal, and international law enforcement partners. This includes the Hazardous Devices School (HDS) certification and recertification, all U.S. public safety bomb technicians' advanced training, and all U.S. public safety bomb squad accreditations. Similarly, the recently established National C-UAS Training Center (NCUTC) serves as the nation's primary training venue for state, local, tribal, and territorial law enforcement C-UAS operations. NCUTC delivers standardized C-UAS operator certification for eligible law enforcement and correctional personnel.

The CIRG encompasses the Hostage Rescue Team, a full-time national tactical counterterrorism team, and manages the Special Weapons and Tactics (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 UAS program. The SOG is composed of armed agents who surveil potentially violent targets, while SSG's unarmed investigative specialists cover targets unlikely to be violent. CIRG manages the FBI's C-UAS program, performing detect, track, locate, identification, and mitigation missions, as well as the NCUTC. In addition, CIRG oversees the National Center for the Analysis of Violent Crime program and provides behavioral analysis and assessments for complex and time-sensitive investigations across multiple programs.

C. Criminal Enterprises/Federal Crimes (CEFC) Decision Unit

CEFC DU Total	Direct Pos.	Estimate FTE	Amount ($000s)
2025 Enacted	13,420	13,431	$3,963,725
2026 Enacted	13,125	12,881	$3,887,134
Adjustments to Base and Technical Adjustments	723	714	$347,253
2027 Current Services	13,848	13,595	$4,234,387
2027 Program Increases	899	458	$361,685
2027 Request	14,747	14,053	$4,596,072
Total Change 2026-2027	**1,622**	**1,172**	**$708,938**

Program Description

The CEFC DU encompasses all HQ and field programs supporting the FBI's criminal investigative missions, primarily managed by the CID. The DU includes:

- HSTFs, cartel/gang FTO programs, and TOC programs;
- Violent crime, Indian country crime, CAC, HT, and gang/criminal enterprise programs;
- Criminal intelligence programs and the criminal investigative components of the CyD programs, including criminal computer intrusions, the Internet Crime Complaint Center, and a share of the FBI's Legat program;
- Public corruption, civil rights, international human rights, and international corruption programs; and
- Financial crimes program.

The structure of the FBI's criminal intelligence program maximizes resource efficiency; improves investigation and intelligence gathering; focuses on criminal enterprise threats; and promotes intelligence collection, exchange, and dissemination throughout the FBI and other authorized agencies.

Homeland Security Task Forces, Foreign Terrorist Organizations, Transnational Organized Crime, Violent Crime, and Crimes Against Children

The FBI's HSTF FTO and TOC Program work to disrupt and dismantle transnational criminal organizations posing the greatest threat to U.S. economic and national security. Transnational organized crime is a global threat, encompassing several criminal activities including drug trafficking, money laundering, HT, 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 domestic violent crimes, violent crimes committed against U.S. citizens overseas, violent gangs, major crimes in the FBI's jurisdiction on tribal lands, CAC, and HT.

Cyber Program

The Cyber program equally supports counterterrorism/counterintelligence and criminal investigations, combatting cyber adversaries through unique authorities, joint enabled operations, timely intelligence sharing, and proactive engagement. For additional details, see the Computer Intrusion Program entry in the CT/CI DU section.

Law Enforcement Attaché Program

FBI Legat offices work hard to crush violent crime and forge key connections with law enforcement personnel around the world. FBI SAs working internationally use their unique skills and knowledge to coordinate investigations while protecting U.S. interests. Legats partner daily with the FBI's criminal and intelligence divisions, foreign law enforcement, and U.S. and foreign intelligence and security services to achieve this mission.

The IOD includes a major training component, allowing the FBI to maintain its position at the forefront of law enforcement expertise and further develops FBI vetted teams critical to overseas operations.

D. Criminal Justice Services (CJS) Decision Unit

CJS DU Total	Direct Pos.	Estimate FTE	Amount ($000s)
2025 Enacted	2,543	2,516	$650,957
2026 Enacted	2,500	2,478	$644,594
Adjustments to Base and Technical Adjustments	55	49	$32,965
2027 Current Services	2,555	2,527	$677,559
2027 Program Increases	47	24	$54,535
2027 Request	2,602	2,551	$732,094
Total Change 2026-2027	**102**	**73**	**$87,500**

Program Description

The CJS DU is primarily composed of all programs in the CJIS Division, as well as a portion of the LD, which provides criminal justice information and forensic services to the FBI's state and local law enforcement partners, and the TD, which provides state and local training programs.

Criminal Justice Information Services Division

The mission of the CJIS is to equip law enforcement, national security, and IC partners with the criminal justice information needed to protect the United States while preserving civil liberties. The CJIS includes several major program activities supporting this mission, all described below.

Next Generation Identification (NGI) System

The NGI system has the nation's largest and most efficient electronic repository of biometric and identity history information and provides continual, timely, and accurate identification services to the criminal justice and non-criminal justice community. The NGI system services connectivity for 114,488 Federal, state, local, territorial, and tribal law enforcement and non-criminal justice customers. The NGI system also provides interoperability with the biometric matching systems of the Department of Homeland Security (DHS) and the DOW.

The NGI system continues to operate at a high-performance level of 99.78 percent and exceeds all availability and accuracy performance goals. From a ten-print perspective, the NGI system algorithm, when combined with human examiners, continues to satisfy the 99.99 percent accuracy rate and facial recognition searches exceed 99 percent accuracy.

National Crime Information Center (NCIC)

The NCIC system is a database of documented criminal justice information submitted by and available to law enforcement agencies 24 hours a day, 365 days a year. The NCIC provides critical information to Federal, state, local, and tribal criminal justice agencies. The system contains over 19.5 million active records organized into 22 files including: Wanted Persons, Missing Persons, Unidentified Persons, Immigration Violators, Protection Order, Supervised Release, the National Sex Offender Registry, Identity Theft, Gang, TSC, Protective Interest, National Instant Criminal Background Check System (NICS) Denied Transactions, Violent Persons, Extreme Risk Protection Order, Article, Gun, License Plate, Vehicle, Securities, Boat, and Vehicle/Boat Part. The FBI is charged by Title 28, Code of Federal Regulations, Section 20, to manage the system.

The operational availability of the NCIC system is vital for the law enforcement and criminal justice communities. The safety of law enforcement personnel and the public depends upon this availability, which is supported by an average uptime of 99.8 percent over the past 12 months. The NCIC system processes 10.8 million transactions per day 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 FBI is preparing for the next major upgrade to the NCIC system, known as NCIC Third Generation, to provide modern, streamlined, and enhanced capabilities to the user community.

National Instant Criminal Background Check System (NICS)

The NICS is a national system established to enforce provisions of the Brady Handgun Violence Prevention Act of 1993 (Brady Act). Federal firearms licensees (FFLs) utilize NICS to determine whether receipt of a firearm to a prospective purchaser would violate state or Federal law. The system ensures the timely transfer of firearms to those not specifically prohibited and denies transfer to prohibited persons.

The Brady Act allows the FBI three business days to decide 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 FBI. The FBI's NICS mission is to complete all checks prior to the third business day.

The FBI processed 27,114,169 NICS transactions in FY 2025. Based on several new initiatives—the publishing of a new Federal regulation, increasing background check support for state and local partners and a recent U.S. Supreme Court decision expanding the definition of firearms—the FBI is anticipating an increase in Federal background checks in FY 2026 and 2027.

The Bipartisan Safer Communities Act (BSCA) expanded background checks for people under the age of 21 (U21), to include juvenile criminal and mental health records. The BSCA requires a three-business day background check to determine if a potential prohibiting juvenile criminal or mental health adjudication exists under Title 18 United States Code (U.S.C.) § 922 (d), (g), or (n), or state, local, or tribal law for all U21. The BSCA also requires the FBI to notify the licensee if cause exists to further investigate potential disqualifying juvenile records within the three-business-day time frame. In addition, 18 U.S.C. § 922(a)(1)(C)(iii) requires the FBI's NICS team, when cause exists, to continue research for a ten-business-day 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 2022, the FBI has denied 4,782 transactions.

National Data Exchange (N-DEx)

The N-DEx system is an unclassified national strategic investigative information sharing system enabling criminal justice agencies to search, analyze, and share Federal, state, local, and tribal records across jurisdictional boundaries. The N-DEx contains over two billion searchable records contributed by over 8,500 criminal justice agencies including incident, arrest, and booking reports; pretrial investigations; supervised release reports; calls for service; photos; and field contact/identification records. The N-DEx system also connects many regional and local information-sharing systems and is positioned to bridge gaps in the many areas of the country where no system or program currently exists.

N-DEx users can discover relationships between seemingly unrelated people, property, crimes, and locations; generate integrated biographies of subjects; link information across jurisdictions; and coordinate efforts between agencies in a secure online environment.

National Threat Operations Center (NTOC)

The NTOC is the FBI's central intake point for reporting violations of Federal law and threats to national security. Operating around the clock, NTOC streamlines information by managing calls and electronic tips from the public, FOs, and the WMD tip line. NTOC's Threat Intake Examiners (TIEs) receive threat information from around the world, complete preliminary research and analysis, and document relevant information in the Threat Intake Processing Systems (TIPS) database. TIEs analyze threats, determine urgency, and refer information to the appropriate FBI entity or law enforcement agency for action. The NTOC communicates directly with state, local, and tribal partners on urgent threat-to-life (TTL) matters, providing timely and actionable information.

The NTOC received over two million calls and electronic tips in FY 2025, including more than 6,800 TTL tips, which were referred to FOs and fusion centers. The NTOC holdings, accessible through TIPS, improve investigations and enhance situational awareness across areas of responsibility. TIPS users can access audio recordings of complaints, request certified copies of tips, create personalized search subscriptions, and receive alerts for matching records. TIPS users can also directly suggest functionality enhancements via the TIPS Feedback site.

Bioterrorism Risk Assessment Group (BRAG)

The BRAG conducts bioterrorism security risk assessments, analyzing data from various databases to determine if a person is restricted from accessing biological select agents and/or toxins. The BRAG is as a resource for FBI WMD coordinators, as it houses identifiable information, fingerprints, and photos of approximately 10,000 individuals who possess, use, or transfer biological select agents and/or toxins.

Criminal History Analysis Team (CHAT)

The mission of the CHAT is to provide exceptional customer service to appellants and respond to all initial firearm background check denial challenges within the mandated five business day timeframe. The CHAT also performs in-depth reviews of available criminal history records, requests record modifications, and details case specifics for requests for information related to firearm purchase denials. The Fix NICS Act of 2018 modified the Brady Act to require a 60-day determination on appeals once the FBI 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. The CHAT received 14,891 VAF applications during FY 2025, a 51 percent increase from FY 2024.

In addition, an agreement between the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) and the FBI was finalized, allowing individuals to use administrative appeals processes to attempt to resolve record-related issues revealed during a NICS background check, initiated as part of the individual's National Firearms Act application.

Uniform Crime Reporting (UCR)

The FBI's UCR program serves as the national clearinghouse for the collection of data regarding crimes reported to law enforcement. 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, which is the basis for public releases including Crime in the United States, Law Enforcement Officers Killed and Assaulted, Hate Crime Statistics, the National Use-of-Force Data Collection, and the Law Enforcement Suicide Data Collection. These publications fulfill the FBI's obligations under Title 28, U.S.C. § 534.

The FBI Crime Data Explorer (CDE) is the interactive public-facing website for UCR data. The CDE provides multiple visualizations and infographics to summarize the massive amount of UCR data collected. The UCR program leverages the CDE to release crime data at more frequent intervals outside the annual reports and publications.

Law Enforcement Enterprise Portal (LEEP)

The FBI's LEEP is a gateway for thousands of criminal justice, intelligence, and military community members to gain access to critical data protected at the controlled unclassified information level in one centralized location. LEEP users can securely access national security, public safety, and terrorism information contained within dozens of Federal information systems. LEEP enables users to transfer and use information efficiently and effectively in a consistent manner across multiple organizations and systems to accomplish operational goals.

Laboratory Division (LD)

The FBI's laboratory is a world-renowned, full-service Federal forensic laboratory. The LD applies scientific capabilities and technical services to the collection, processing, and exploitation of evidence to support the FBI, other Federal duly constituted law enforcement and intelligence agencies, and some state and foreign law enforcement partners in support of investigative and intelligence priorities. The LD provides 15 different forensic science disciplines (DNA analysis, forensic facial imaging, latent fingerprint analysis, general chemistry, cryptanalysis, firearms toolmarks, gunshot residue, bullet trajectory, shoeprint and tire tread identification, etc.) in support of FBI investigations and other government agencies. In FY 2025, the FBI laboratory processed over 4,700 submissions of evidence, almost half in support of violent crimes, taking ruthless offenders off the street. The LD has been deployed nearly 160 times in support of large-scale complex crime scenes and mass casualty events.

Training Division (TD)

In addition to training FBI SAs and PS personnel, the TD provides instruction for law enforcement partners, both at the FBI Academy and throughout the United States at state, regional, and local training facilities. These training sessions cover the full range of law enforcement training topics in furtherance of the overall FBI mission and priorities to crush violent crime, defend the homeland, rebuild public trust, and provide fierce organizational accountability.

Annually, TD holds four sessions of its principal course, the National Academy (NA). The NA is a 10-week residential leadership development program, accredited by the University of Virginia, for senior law-enforcement leaders worldwide. Since 1935, TD has held four NA sessions each year at the FBI Academy.

Recently, TD hosted the following number of students for its annual NA sessions:

- FY 2023, 883 students, including 98 international students (11 percent of total students)
- FY 2024, 914 students, including 101 international students (11 percent of total students)
- FY 2025, 999 students, including 85 international students (9 percent of total students)

V. Program Increases

A. Intelligence Community Support

Organizational Programs: Counterintelligence, Criminal, Operational Technology, Threat Screening Center, Office of the Chief Information Officer

Program Increase: Positions 44 Agent 1 Atty 0 FTE 22 Dollars $94,300,000 ($87,659,000 non-personnel)

Description

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

B. National Security System Cybersecurity Requirement

Organizational Program: Office of the Chief Information Officer (OCIO)

Program Increase: Positions 0 Agent 0 Atty 0 FTE 0 Dollars $105,000,000 (all non-personnel)

Description

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

C. Combatting Violent Crime

Organizational Program: Criminal Investigative, Critical Incident Response Group, Lab, Threat Screening Center

Program Increase: Positions 686 Agent 231 Atty 7 FTE 351 Dollars $311,668,000 ($110,401,000 non-personnel)

Description

The FBI's dedicated focus to combatting violent crime has resulted in historic results safeguarding the safety and security of the American people. The FBI's actions against criminal actors in 2025 led to:

- Over 50,000 total arrests (30,000 of those violent offenders), a nearly 100 percent increase from 2024, with record-breaking reductions in violent crime and murders across the nation;
- Over 2,100 kilos of fentanyl seized, up 30 percent from the year prior (enough to kill 159 million Americans);
- Almost 6,600 innocent children located; a 22 percent increase from 2024;
- 2,300 child predators arrested; a nine percent increase from 2024; and
- Over 450 human traffickers arrested; a 22 percent increase from 2024

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

Justification

Agent Support Combatting Criminal Programs: 63 positions (0 SAs) and $8,173,000 (all personnel)

The FBI requests resources to enhance its Professional Staff (PS) complement to support combatting criminal activity through a number of investigative programs. Combatting criminal activity and mitigating the overlapping threats criminal actors pose are among the FBI's top priorities. These programs and activities include crimes against children and human trafficking (CAC/HT), combatting emerging threats, and TCOs.

Crimes Against Children/Human Trafficking (CAC/HT) Program: 33 Positions (0 SAs) and $3,795,000 (all personnel)

The FBI's CAC/HT program has seen a significant rise in the number of complaints, tips, investigations, sophistication, and techniques utilized by offenders to evade law enforcement. In response, the FBI is requesting 13 Staff Operations Specialists (SOSs) and 20 PS positions to further combat the CAC/HT threat. With additional dedicated personnel, the FBI's CAC/HT program will be better positioned to properly address this evolving threat and achieve the mission to protect children and apprehend the most atrocious offenders. Requested resources will support the recently created dedicated HT program at FBI HQ and enhance the CAC program, while increasing analytical capabilities and keeping pace with emerging technologies. This will allow the program to align with the increased field dedicated CAC/HT resources to effectively manage the threat.

The HT program covers both sex trafficking and labor trafficking and includes investigating crimes with a domestic or foreign nexus for both adult and minor victims. Sex trafficking is the recruitment, harboring, transportation, provisioning, or obtaining of an individual who, under force, fraud, or coercion, is induced to perform a commercial sex act. Investigations can involve a U.S. Person (USPER) victim, non-USPER victim, or both, as the FBI must investigate allegations of sex trafficking regardless of the victims' nationality. Labor trafficking occurs when USPER or non-USPER victims are compelled to perform labor or services using force or threats of force; physical restraint or threats of physical restraint; serious harm or threats of serious harm; abuse or threatened abuse of law or legal process; or coercion.

The sex trafficking of minors (STM) is one of the most complex forms of child sexual exploitation, as offenders target and lure vulnerable children to engage in sex trafficking activities and other forms of sexual exploitation through manipulation, drugs, and/or violence. Once a trafficker gains control over a child, they often use acts of violence, intimidation, or psychological manipulation to keep the child engaged in sex trafficking. STM investigations fall under the ILNI—implemented in 2003 to address children being recruited or forced into commercial sex—and are supported by DOJ and the National Center for Missing & Exploited Children (NCMEC).

Domestic and international HT investigations of either adult or minor victims are resource-intensive, requiring significant resources at FBI HQ and FOs to adequately mitigate the threat. Advances in technology are major challenges to overcome in HT investigations as they have made it easier for traffickers to target, recruit, and exploit victims around the world without detection. Human traffickers conduct business operations easily due to increases in online monetary exchanges and anonymizing software.

On January 20, 2025, President Trump signed EO 14159, Protecting the American People Against Invasion, establishing the HSTF objective of dismantling cross-border human smuggling and trafficking networks and ending the scourge of human smuggling and trafficking, with particular focus on such offenses involving children. The DOJ National Strategy relies on a whole-of-government approach to enhance capabilities to prevent HT, prosecute HT cases, and support and protect HT victims and survivors. The DOJ National Strategy will be implemented under the direction of the National Human Trafficking Coordinator designated by the Attorney General. As a result of the DOJ National Strategy, the FBI must coordinate with other agencies on numerous tasks, including:

- Participating in nationwide intelligence sharing among law enforcement partners to investigate and dismantle cross-border human trafficking enterprises;
- Identifying and dismantling HT operations within the United States;
- Continuing a victim-centric, multi-agency approach to investigate HT; and
- Adhering to protocols for case referrals to state, local, tribal and territorial partners.

The FBI's VCAC program has a team of personnel detailed to NCMEC on a full-time basis to conduct centralized coordination and analysis of domestic and international child exploitation case information. Embedded personnel coordinate the utilization of FBI and NCMEC resources to ensure the most effective response to child abductions, parental kidnappings, HT of children, and sexual exploitation of children matters. NCMEC is a private, nonprofit organization established in 1984 under a Congressional mandate and works in cooperation with the DOJ's Office of Juvenile Justice and Delinquency Prevention. As the nation's resource center for child

protection, NCMEC spearheads national efforts to locate and recover missing children and raises public awareness to prevent child abduction, molestation, sexual exploitation, and the victimization of children. Since 2022, embedded personnel have seen an increase in reporting of child abductions, sexual exploitation, trafficking, sexual exploitation, and victimization of children, including the review of over 47,000 cyber tips by FBI personnel between calendar years 2024 and 2025. As each cyber tip involves multiple stages of analysis prior to dissemination to a FO-based SA, increased personnel resources will increase the timeliness and efficiency of the FBI-NCMEC process.

Through the CAC program's VCACITF, the FBI continues to establish an increasingly robust and effective capability to pursue priority initiatives and investigations beyond national borders. Offenders are effectively capitalizing on technology advances to avoid law enforcement detection while engaging in increasingly larger, more sophisticated, and violent child sexual exploitation conspiracies. The operative detection and investigation of these activities increasingly require coordination with foreign partners, and the VCACITF (composed of 91 members from 59 countries) provides the FBI with real-time coordination of operational activities and investigations against priority and high-impact targets.

Combatting Emerging Threats: 16 positions (0 SAs) and $2,320,000 (all personnel)

The FBI requests 16 positions to address gaps on emerging threats, synthetic opioids, violent crime, transnational gangs, and TOC schemes emanating from China. These global threats are increasingly cross-programmatic, requiring a unique, tailored intelligence analysis and mitigation strategy. Specialists are required to assist with evolving criminal threats, expanding the FBI portfolio in both the international and domestic space. In 2025, the President signed EO 14159, Protecting the American People Against Invasion, establishing of the HSTF to combat and eliminate criminal cartels, foreign gangs, and TCOs and dismantle human smuggling and trafficking networks. Subsequently, the Homeland Security Council drafted the original proposal outlining the requirements to establish the HSTF, and in doing so identified the two lead components as the DOJ, through the FBI, and the DHS, through the HSI. This has increased investigative tempo and centralized efforts of high-priority threats, such as the focus on synthetic opioids. The FBI has made significant progress in this space in the past year and requests additional personnel to continue at this pace and efficiency against the threats.

The requested personnel resources will allow for adequate tactical support to address the immediate, reactive needs of high-priority initiatives and threats to include synthetic opioids, cyber enabled fraud, and Chinese TCOs.

Transnational Organized Crime: 14 positions (0 SAs) and $2,058,000 (all personnel)

Targeting the world's most dangerous drug traffickers is a dynamic and evolving mission with many challenges. The FBI is uniquely positioned to respond to these global threats impacting the United States and its interests abroad. To continue combatting the fentanyl epidemic, the FBI must augment its TOC program with additional personnel to bolster investigative efforts. The FBI has investigative resources and technical tools to attack the threat in multiple ways, from historical drug trafficking investigations targeting TCOs, to identifying and developing tools to combat Darknet threats. To improve the FBI's capability to combat emerging technologies and the expansive threat landscape, the FBI requires this personnel enhancement. These additional personnel will help the FBI to stay ahead of the cartel threat and technological advancements being used by illicit actors. Given many TOC networks are growing in severity and magnitude,

the expansion of the FBI's criminal capabilities domestically and internationally is necessary to mitigate these overseas threats more effectively.

The FBI is seizing record-breaking amounts of fentanyl each year. Fentanyl is largely produced outside the United States, often by cartels obtaining the precursor chemicals from other countries. Every state has felt the impact of illicit fentanyl in varying degrees, including remote areas with the most vulnerable populations. Cartels traffic narcotics into the United States via hidden compartments, and the southwest border remains a key entry point for drug trafficking via land conveyances due to its extensive perimeter. Initiating impactful cross-border investigations, supporting partners, and sharing information targeting Mexican cartels enables the FBI to tactically combat the epidemic. Strategically placing additional resources will further enhance collaboration with foreign partners and address cross-programmatic deficiencies.

The FBI requests 14 personnel to provide critical investigative support to investigations. Increasing the PS cadre supporting investigations provides critical tactical support, operational research, data exploitation, and computer analysis to assist in moving cases to prosecution.

ALAT Operational Costs: 28 positions (0 SAs, 0 Attys) and $7,580,000 ($2,820,000 non-personnel)

The FBI currently assigns SAs and IAs to support criminal investigative work abroad and coordinate with host country law enforcement and intelligence agencies to enhance FBI investigations, develop sources, and identify new threats. Successful FBI investigations—across all threats—rely heavily on the FBI's overseas presence and the coordination provided by both SAs and IAs.

In FY 2025, the FBI assigned 40 IAs abroad, located in 36 Legat offices. These IAs play a vital role in partner engagement and intelligence sharing; the relationships with host nation partners and the IC within the embassy are imperative to providing operational support to local FO operations.

To expand the many successes IAs stationed overseas have accomplished the FBI is requesting 28 IA positions. These positions will allow the FBI to strategically place personnel to combat criminal threats, and to provide vital support to all the threats the FBI works to mitigate.

The FBI will assign the 28 IAs as follows:

- Asia (5 IAs) – Many of the partnerships the FBI maintains throughout Asia support increased information sharing and operational support of CI and cyber cases, which almost always have a foreign nexus and require partner support. Additionally, the FBI has recently increased engagement and had operational success on scam compounds and fentanyl production factories located in the region.
- Africa (5 IAs) – The threats worked by offices in Africa have frequently focused on CT threats. This partnership is vital, specifically to the increasing threats in West Africa and the Horn of Africa. Criminal threat reporting has increased across the African continent, and as such, FBI Legat offices have increased coordination with law enforcement partners.
- Middle East (4 IAs) – The Middle East offices have historically focused on CT and CI threats and provide valuable support to FBI offices investigating these threats. Additionally, countries such as Oman and Qatar have become key interlocutors with the

United States on a variety of international matters. Having enhanced intelligence support in these offices would vastly increase intelligence sharing on all threats facing the FBI.

- Americas (2 IAs) – The partnerships developed and maintained with host nation partners in the Americas have proven immensely important as the FBI has sharpened its focus on crushing violent crime.
- Five Eyes (1 IA) – Partnerships with partners in the UK, Canada, New Zealand, and Australia are some of the most beneficial for advancing operations throughout the FBI. In both the UK and Australia, FBI IAs are co-located with their foreign partners to share and collaborate seamlessly.
- Europe and Eurasia (10 IAs) – The FBI maintains strategic and well-developed partnerships with many countries throughout Europe and Eurasia. The IAs assigned to these offices adeptly work all threats and share intelligence to drive operations in FBI FOs. Depending on the office, IAs work criminal investigative matters, such as drug and illicit materials trafficking and TOC; CI threats arising from Chinese and Russian influence in the area; dark web fraud; and CT travel routes.
- U.S. Northern Command (NORTHCOM) (1 IA) – The FBI and NORTHCOM share responsibility to protect the United States from adversaries, both foreign and domestic. NORTHCOM serves as the DOW's lead for homeland defense and Defense Support of Civil Authorities, while the FBI is the lead domestic intelligence and law enforcement agency. Adding an FBI IA to NORTHCOM will assist in identifying threats straddling the line between homeland security and homeland defense.

The FBI is requesting $2,100,000 for Assistant Law Enforcement Attaché (ALAT) operational travel and temporary duty assignments required for assistance—in combatting crime and in fentanyl and TOC investigations—such as meetings with witnesses, victims, and case support. The FBI also requests $720,000 to support seven Foreign Service Nationals (FSNs) for Legats in Mexico and Central/South America. The FSNs will improve engagements with country partners and provide benefits to Legat's mission. FSNs identify and strengthen constantly changing liaison contacts, translate during meetings for investigative documents, and respond to requests for information (RFI) from key law enforcement agencies.

Cartels, Fentanyl, and Immigration Enforcement: 148 positions (135 SAs, 5 Attys) and $77,070,000 (all personnel)

The FBI fights violent crime and gang activity by focusing on three key attributes: intelligence, partnerships, and expertise. To enhance these traits, the FBI collects, analyzes, and shares actionable information; collaborates with Federal, state, and local partners; and combats the increased use technology through training and sharing best practices. To build on the FBI's historic successes in FY 2025 and 2026, the FBI requests:

- 126 field SAs—approximately two per FO—to address priority threats including violent crime, gangs, TOC, FTOs, immigration enforcement, and illicit fentanyl.
- Nine (9) Legat SAs and two (2) IAs in Central and South America to combat TCOs and opioid threats and protect the homeland from emerging international threats.
- Six (6) Forensic Accountants (FoAs) embedded in HSTFs, to disrupt and dismantle FTOs through financial analysis.

- Five (5) Attorneys to provide legal and policy guidance on complexities surrounding mandatory services, assistance, and rights of those involved in FBI investigations, ensuring the FBI remains compliant with statutory requirements.

The FBI maintains violent crime and gang investigative programs in every FO, with a mission to identify, disrupt, and dismantle the most egregious violent gangs and criminal enterprises through intelligence-driven, proactive, and sustained enterprise investigations. Violent Crimes Task Forces (VCTFs) and Safe Streets Gang Task Forces (SSGTFs) lead efforts to eradicate violent crime plaguing communities across the United States The FBI currently operates over 225 VCTFs and SSGTFs throughout the country, composed of over 2,000 TFOs working in unison with hundreds of FBI SAs and IAs. In FY 2025, TFOs accomplished 7,663 arrests, 1,919 disruptions, and 159 dismantlements of violent criminal enterprises and gangs. Collectively, these task forces leverage investigative, analytical, and prosecutorial resources to combat violent crime, gangs, and criminal enterprises, and requested resources will bolster the FBI's VCTF and SSGTF footprint across the United States

Homeland Security Task Forces/Border Offices

The mission of HSTFs is to end the presence of criminal cartels, foreign gangs, and TCOs in the United States; dismantle cross-border human smuggling and trafficking networks, with a particular focus on offenses involving children; and use all available law enforcement tools to faithfully execute the laws of the United States. HSTFs are deployed in every state, as well as Washington, D.C. and Puerto Rico, as the FBI works diligently with HSI to reduce duplicative efforts and ensure resources are used effectively and efficiently in TCO and FTO investigations.

Initiating cross-border investigations, supporting partners, and sharing information targeting Mexican cartels enables the FBI to combat the epidemic from a tactical perspective. Strategically placing additional resources will further enhance collaboration with partners and address cross-programmatic deficiencies. The geographic distance between the UnitedStates. and Mexico ports of entry provides TCOs substantial opportunity to exploit vulnerabilities and smuggle illegal narcotics, including fentanyl, into the United States.

Requested resources will allow the more effective management of HSTF priorities as the FBI works to end the presence of criminal cartels, foreign gangs, and TCOs efficiently and effectively. The FBI will continue to leverage HSTFs and other Federal, state, and local partnerships to go after "command and control" elements of cartels, both within and outside the United States, and additional SAs and FoAs, disseminated geographically, will greatly mitigate the threat. There are thousands of active FTOs and cartel investigations, and additional personnel will identify, disrupt, and dismantle the leadership of those organizations.

Opioid Crisis

Requested resources will address lines of effort outlined in the NSC's Counter Fentanyl Strategic Implementation Plan, requiring significant coordination across agencies and platforms to identify nefarious activity and combat distributors of narcotics around the world. The FBI, in collaboration with domestic and foreign law enforcement partners, pursues TOC actors trafficking narcotics into the United States. An increased level of fidelity is necessary for the FBI to address the growing threat posed by TCOs conducting activities detrimental to U.S. national security, public health and safety, and economic stability.

Targeting the world's most dangerous drug traffickers is a dynamic and evolving mission with many challenges. The FBI is uniquely positioned to respond to these global threats and must

support the TOC program with additional personnel to combat the fentanyl and opioid epidemics. To improve capabilities to combat the threat posed by emerging technologies, additional SAs will be embedded in areas with high fatal overdose rates, allowing the FBI to stay ahead of the cartel threat and the technological advancements used by illicit actors.

Assistant Law Enforcement Attaché

The FBI requests 11 ALAT positions to address criminal threats emanating from a significant increase in drug trafficking activity and migration into the United States. To maintain an embedded investigative presence and provide operational support, the FBI must build upon a network of trusted partners, simultaneously strengthening counterparts' capabilities to combat national security and criminal threats locally. The requested nine (9) Legat SAs and two (2) IAs will be assigned to Mexico and countries in Central and South America, allowing for more focused engagement with host country partners and increased ability to conduct interviews, collect evidence, execute joint operations, facilitate training/travel, provide explosives assistance, and collect and share intelligence.

In addition to deploying SAs and IAs abroad, the FBI oversees task forces and vetted teams (VTs) composed of host country law enforcement officers to conduct investigations and operations. Successful FBI investigations rely heavily on the invaluable overseas presence and coordination provided by BLOs, ALATs, and VTs to target OCONUS threats. Through global partnerships, the FBI can better target trafficking organizations, financial infrastructure, and distribution networks.

Requested resources are imperative for the FBI to continue to combat the threat posed by the fentanyl and opioid epidemics, violent crime and gangs, and TCOs. As threat actors continue to evolve, additional personnel and operational resources will allow the FBI to stay ahead of technological advances leveraged by these criminals. The scope and detrimental impacts of TOC networks are expanding and corresponding growth of the FBI's criminal capabilities at home and abroad is necessary to mitigate threats.

Additionally, the FBI requests five (5) Attorneys to provide legal and policy guidance pertaining to complexities surrounding violent crime and gangs, TOC, fentanyl, immigration, victim services, investigative issues assistance, human rights, and statutory requirements. The Attorneys will address key topics related to privacy, services, and FBI authorities, such as the role in interviews and the legal obligation to disclose a subject's identity.

FBI Police Officers: 45 Positions (0 SAs) and $12,137,000 (all personnel)

In FY 2025, the FBI announced it would relocate its headquarters from the J. Edgar Hoover Building (JEH) to the Ronald Reagan Building and International Trade Center (RRB), located at 1300 Pennsylvania Avenue NW, Washington, D.C. The JEH is currently staffed with 86 FBI Police Officers, who serve in shifts to provide 24/7 coverage to protect FBI personnel, facilities, and information from criminal acts and unauthorized access. The RRB will require additional coverage, and with the overlapping occupancy of both buildings and the larger square footage of the RRB, the existing 86 Police Officers are not sufficient to maintain the FBI's current security posture. The FBI requires 20 of the requested positions to fully secure and successfully transition to and maintain coverage of the RRB as the new headquarters location.

Additionally, FBI FOs face increasing threats to personnel and facilities (nearly 500 in FY 2025 alone), National Security Special Events (NSSEs), dignitary visits, high-profile events, and other unplanned crisis situations. The FBI has increasingly relied on the FBI Police Officers to deploy

to these FOs to protect FBI personnel and provide support to the existing security apparatus in place. To meet this demand and effectively respond to dynamic security requirements the FBI requires 25 additional police officer positions.

***Federal Deoxyribonucleic Acid (DNA) Databasing and Laboratory Forensics and Analysis*: 45 positions (0 SAs) and $23,435,000 ($16,415,000 non-personnel)**

Requested resources will effectively scale operations to allow the FBI to address legally mandated DNA collections from the DHS, DOJ, and other Federal law enforcement agencies for entry into the Combined DNA Index System (CODIS). The average DNA submission rate is between 360,000 to 480,000 samples per year, and current base resources are sufficient to process approximately 100,000 samples per year. Additional resources are critical to process DNA submissions into CODIS in a timely manner and provide life-saving investigative leads to law enforcement.

The DNA Fingerprint Act of 2005 mandates DNA analysis of all federally convicted offenders, arrestees, and non-U.S. citizen detainees, and it requires the FBI process DNA samples in a timely manner for investigative leads to local, state, and Federal law enforcement agencies (LEAs). After April 2020, DHS DNA collection expansion required previously exempted DHS component agencies to now routinely collect DNA and sample submissions rose to more than 50,000 per month, or seven times the historical volume. With the end of the COVID-19 pandemic and the rescission of Title 42, the monthly submission average rose to 146,000, including in February 2024 when more than 180,000 samples were submitted. These large and sustained volume increases quickly outpaced DNA program resources. At the end of FY 2024, the CODIS processing backlog had reached 1.8 million, increasing by an average of 75,000 samples per month.

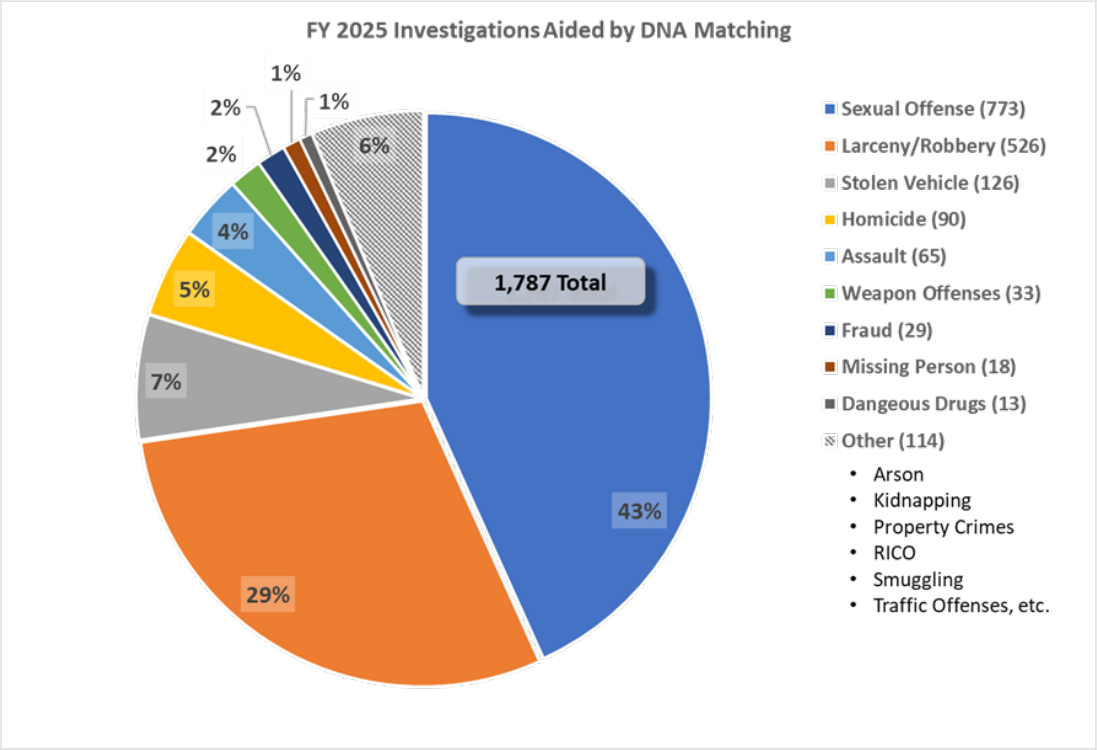
Prior to the DHS DNA expansion, the FBI allotted approximately $7.0 million in base non-personnel resources annually for mandated DNA database work. Once the rule change was recognized in FY 2020, the FBI simultaneously requested budget enhancements and reallocated base resources to attempt to mitigate anticipated growth in requirements. In FY 2023, the FBI applied an $8.1 million budget enhancement and $39.8 million in reprioritized non-personnel base resources to increase processing to 60,000 samples per month. In FY 2025, due to changing policies, there was a significant downward shift in U.S. border apprehensions, lowering the volume of DNA samples to roughly 40,000 samples per month. While this allowed the LD to begin addressing the accumulated backlog of samples, additional sustained funding is needed to maintain backlog elimination efforts and achieve a “steady-state” DNA processing operation in FY 2027 and beyond.

Requested resources will retain skilled contract personnel, procure critical supplies and reagents, incorporate new Rapid DNA technology into operations, and provide storage solutions in facilities. Additional details on these investments are as follows:

- $1,000,000 for 10 sample intake and processing technician contract support staff.
- $15,415,000 for collection kits, Rapid DNA confirmation, chemicals, and other lab supplies to process, track, and store samples to generate CODIS-eligible DNA profiles.

As the highest volume contributor to CODIS, the FBI experiences ongoing increases in DNA matches resulting from recent collection enforcement. In addition, the FBI has collaborated with DHS component agencies to build automated and streamlined workflows to minimize cost and administrative burden. Requested resources will support DNA-related mandates and avoid submission levels outpacing FBI processing capacity and subsequent increases to the DNA backlog. Backlogs delay entry of DNA profiles into CODIS, increasing the likelihood of arrestees and non-U.S. detainees being released before they are identified through investigative leads.

Laboratory Forensics



The LD's mission is to collect, analyze, and share timely scientific and intelligence driven information for FBI FOs; state, Federal, and international law enforcement and intelligence agencies; defense and counterterrorism partners; as well as Federal and state prosecutors. The division's efforts support FBI FO operations through critical forensic exploitation of evidence related to immigration enforcement and public safety, with a focus on violent crime, national security, and terrorism. The LD staff apply state-of-the-art techniques to the collection and processing of evidence across 15 forensic disciplines to include biometrics (DNA & latent prints), firearms, chemistry, and improvised explosive device (IED) analysis. The LD's area of responsibility also includes national DNA database, forensic genealogy, chemical, biological, radiological, and nuclear forensic analysis, mass disaster/shooting deployment and processing, UAS exploitation, accreditation, and expert testimony. An additional 45 forensic personnel would support the LD's need to assist in high-profile cases and provide timely support for evidence processing.

Hazardous Devices School (HDS) Bandwidth Expansion: $8,000,000 (all non-personnel)

The FBI requests $8,000,000 to train, certify, and re-certify Public Safety Bomb Technicians (PSBTs). A total population of approximately 3,000 PSBTs represent 464 local, state, and Federal Public Safety Bomb Squads (PSBSs) to achieve a safe, reliable, repeatable, and predictable national response to IEDs and WMDs.

Current resource levels necessitate a two-year wait between PSBS candidate selection and arrival for training and certification. This creates a shortage of certified PSBTs for bomb squads around the country, leading to critical national security gaps. PSBT staffing challenges are projected to increase as personnel leave the profession and suitable replacements are not efficiently identified. The enrollment backlog negatively impacts not only the FBI but also partners at hundreds of local, county, and state agencies.

Of the total requested resources, $2,500,000 will support 15 contract instructors to mitigate increased demand for the U.S. PSBT certification course, consisting of one week of virtual training and six weeks of in-person instruction at the FBI's HDS facility on Redstone Arsenal in Huntsville, Alabama. The FBI typically executes eight certification courses annually with 32 students per cohort. To address demand and alleviate the two-year enrollment backlog, the FBI would expand to 12 certification courses annually. Having additional certified PSBTs will subsequently increase demand for U.S. PSBT re-certification courses by approximately 30 percent, so additional contract instructors will provide the resources necessary for throughput.

PSBT equipment totaling $3,500,000 will meet the projected increase in training volume. The FBI's HDS program requires fit outs for seven teams, each consisting of four students.

HDS Bomb Technician Team Fit Out Non-Personnel Request Summary			
Equipment	**Quantity**	**Unit Cost**	**Total Cost**
F6 Spartan Robot	1	$370,200	$370,200
Bomb Suits with Helmet	2	$42,000	$84,000
X-Ray Processor	1	$22,000	$22,000
X-Ray Generators	2	$6,000	$12,000
Rigging Kit	1	$8,000	$8,000
Assorted Power and Hand Tools	1	$2,000	$2,000
Percussion Actuated Non-Electric Disrupter Stand	3	$600	$1,800
Total Per Team	-	-	$500,000

Finally, $2,000,000 in requested resources will support training-related travel for courses required to complete the U.S. PSBT certification and re-certification courses.

HDS Training Travel Non-Personnel Request Summary	
Course/Conference	**Cost**
Re-Certification Course	$450,000
National Bomb Squad Commander's Conference	$450,000
Crisis Response Training	$400,000
Tactical Bomb Technician Certification	$270,000
Maritime Operations for Bomb Technicians	$180,000
New Bomb Squad Commander's Symposium	$130,000
Underwater Hazardous Devices Countermeasures	$120,000
Total Travel Request	**$2,000,000**

Homeland Security Task Force Coordination: 9 positions (0 SAs) $1,404,000 (all personnel)

The FBI requests Management and Program Analyst (MAPA) personnel increases to support five specialty teams—Precursors, Illicit Finance, Maritime/Aviation, Scam Centers, and Consolidated and Foreign Priority Organization Targets list. These analysts will serve as a force multiplier to field analysts across the country who are often over-tasked with operational support requests from SAs—with an average ratio of one embedded field analyst to support a squad of eight to13 SAs. They will also conduct link analysis to connect investigations across the country and interagency.

Additionally, the FBI requires resources to dedicate one Forensic Accountant (FoA) to the National Coordination Center (NCC) to enhance investigations with complex illicit finance/money laundering needs beyond field capabilities, particularly to assist interagency partners who do not have robust financial investigation resources and rely on the NCC to support those needs. The FBI has grouped the 30 HSTF main offices and the 29 Primary Reporting offices into nine regions. Dedicating an FoA to four of the regions to manage and oversee HSTF personnel, operations, state and local overtime funding, budget allocations, and other administrative functions will increase the bandwidth of SAs and front-line supervisors, thus enabling them to pursue HSTF investigations.

HSTF Hiring and Capabilities Build Out: 114 positions (0 SAs) and $16,595,000 (all personnel)

To meet and implement the robust HSTF requirements, the FBI requests 114 PS positions and $16,595,000 (all personnel).

To meet increased mission requirements in the field, 29 positions will be placed in FOs across the United States. These positions will provide general administrative field support and are vital to the FBI's ability to perform the HSTF mission. The remaining 85 requested positions will support the FBI's Training, Security, and Human Resources Divisions. These positions are required to hire, train, and retain over 400 HSTF employees, of which 300 are SAs. Within the 85 positions, 18 positions are required for background investigations to properly clear and adjudicate TS clearances; 20 positions will support the Basic Field Training Course as well as critical and required training to prepare new employees; and 47 positions will support hiring and recruitment initiatives to ensure the FBI is staffed to support the HSTF mission.

National Instant Criminal Background Check System: 10 positions (0 SAs) and $16,114,000 ($15,135,000 non-personnel)

The FBI requests 10 positions to increase capacity to process mandated background checks for firearm purchases. Based on several new initiatives—the publishing of a new Federal regulation, increasing background check support for state and local partners and a recent U.S. Supreme Court decision expanding the definition of firearms—the FBI is anticipating an increase in Federal background checks in FY 2026 and 2027.

The FBI is supporting DOJ efforts to re-establish a Federal program allowing citizens prohibited from possessing or acquiring firearms to apply for relief and restore their rights. The program requires the FBI perform a background check on the requestor and return an eligibility recommendation to DOJ. This initiative is a top priority of the Administration, is expected to be implemented swiftly, and will result in an immediate increase in background checks. The FBI has also been requested to support partner agencies in making eligibility determinations for state alternative permitting purposes. Currently, although transactions are processed through NICS,

the research and final determination lie with state and local agencies. The ATF has proposed the FBI handle full processing - including determination - for state alternative firearm permit checks to increase consistency and accuracy in determinations. These permits negate the need for a point-of-sale check, and the FBI's involvement would significantly increase the validity of and confidence in determinations. If implemented, the FBI could experience an increase in annual volume up to an additional 1,680,000 checks. For reference, in FY 2025, the FBI performed 1,255,015 firearm parts checks.

The FBI requests the annualization of $10,207,000 in non-personnel funding provided by the BSCA to ensure required software development supports established requirements. A backlog remains of nearly 500 system maintenance and improvement requests to streamline the NICS user interface and improve manual processes associated with quality assurance, improved training environments, and interactive review portals.

The FBI also requests $4,928,000 in non-personnel funding to sustain an additional system development team, supporting critical enhancements to the continued development of NICS. The FBI procures expertise in the areas of technical analysis, systems engineering, independent evaluations, proof of concept development, and research and development, resulting in an increased number of automated final determinations without human intervention.

Rapid DNA: 17 positions (3 SAs) and $11,577,000 ($8,000,000 non-personnel)

Rapid DNA Implementation: 8 positions (0 SAs) and $9,140,900 ($8,000,000 non-personnel)

Per section 2(b) of the Rapid DNA Act of 2017, the FBI is required to provide oversight of Rapid DNA technologies and capabilities, funding implementation in FBI FOs, and providing staff for program oversight. The Rapid DNA Act of 2017 allows Federal, state, and local booking agencies—those responsible for recording and documenting information about a person who has been arrested—to process DNA samples taken from qualifying arrestees and detainees using a Rapid DNA instrument. The arrestee or detainee DNA profile is immediately loaded into CODIS and searched against unsolved crimes of special concern, returning results within minutes and allowing for continued detention. Additionally, the arrestee or detainee sample is searched against all crimes in CODIS within 24 hours.

The ability to successfully implement Rapid DNA in the 36 FBI FOs with the greatest booking volumes requires considerable planning and training. Requested resources will enable the FBI to implement Rapid DNA instrumentation in a staggered manner to at least eight booking stations per year. As booking locations are onboarded, funding will be shifted to service agreements and supplies. The FBI also collaborates with state and local agencies through JTTFs on mass arrest events. These operations provide a unique opportunity to deploy Rapid DNA technology onsite, process DNA of arrested individuals in real time, and immediately upload samples into CODIS, potentially linking arrestees to other unsolved crimes. The personnel resources requested for these efforts are as follows:

- Four (4) Auditors to conduct annual audits of booking facilities as required by FBI policy—*Standards for the Operation of Rapid DNA Booking Systems by Law Enforcement Booking Agencies*—as well as state CODIS agencies implementing Rapid DNA. Audits of select local or municipal sites may also be required to ensure states are correctly enforcing policy. Auditors will visit each state within the first year of implementation, and a minimum of every three years thereafter, to ensure compliance.

- Three (3) Rapid DNA Technicians to oversee the mass arrest program and deploy to mass arrest events for Rapid DNA instrument operation.
- One (1) Rapid DNA Program Manager to oversee implementation of Rapid DNA at booking facilities, including training personnel, coordinating annual audit requirements, installing instrumentation, and managing reagent and supply logistics.

Deployable Mass Fatality Incident and Large Crime Scene Response: 9 positions (3 SAs) and $2,436,100 (all personnel)

The FBI often deploys to mass casualty incidents and large crime scenes to assist with evidence collection and victim identification. Samples at these sites are ideal for Rapid DNA as they contain significant amounts of DNA for processing and Rapid DNA technology is 10-20 times less sensitive than other DNA laboratory techniques. The ability to process evidence in the field can hasten investigative processes to assist Federal, state, and local crime scene investigators.

The FBI maintains three Operational Response Centers (ORCs) strategically located across the United States. for effective deployment of Rapid DNA technology. The FBI's *2025 Quality Assurance Standards for Forensic DNA Testing Laboratories* permits the use of Rapid DNA systems for appropriate forensic crime scene samples due to recent improvements in the technology. Data from the field can be transferred to the laboratory for interpretation by qualified DNA analysts. Requested personnel resources for Rapid DNA deployments are as follows:

- Three (3) SAs to coordinate Rapid DNA deployment from each ORC location.
- Three (3) Rapid DNA Technicians for mass fatality/crime scene response.
- Three (3) Rapid DNA Analysts to report on mass fatality and crime scene data.

Impact on Performance

The requested resources will allow the FBI to more successfully combat the threats posed by the current fentanyl and opioid epidemics, violent criminals and gangs, TOC networks, and FTOs. Criminal actors are continuing to evolve, so personnel and operational development will allow the FBI to stay ahead of technological advances leveraged by illicit actors. The severity and magnitude of the impacts of TOC networks are growing, and an expansion of the FBI's criminal capabilities at home and abroad is necessary to mitigate threats. The requested resources will also allow the FBI to continue to provide oversight of Rapid DNA technologies and capabilities, NICS, Federal DNA Databasing, and Laboratory Forensics and Analysis.

Funding

1. Base Funding

FY 2025 Enacted				FY 2026 Enacted				FY 2027 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
8,815	3,490	9,260	$1,918,418	11,428	13,254	11,748	$2,504,834	11,885	5,179	11,979	$2,675,230

2. Personnel Increase Cost Summary

Type of Position/Series	FY 2027 Request ($000)	Positions Requested	Full Year Modular Cost per Position ($000)	Annualizations ($000)			
				2nd Year	3rd Year	FY 2028 (net change from 2027)	FY 2029 (net change from 2028)
Attorney	$1,520	7	$346	$90	$0	$628	$0
Data Analyst	$207	1	$280	$27	$30	$27	$30
Electronic Technician	$8,086	25	$404	($54)	$12	($1,342)	$300
Engineer	$254	1	$339	$15	$51	$15	$51
Foreign Intelligence Analyst	$414	1	$514	($11)	$11	($11)	$11
Foreign Special Agent	$8,613	9	$1,100	($262)	$23	($2,354)	$207
Forensic Accountant	$799	6	$209	$85	$12	$512	$72
Information Technology	$1,129	9	$200	$98	$23	$881	$207
Intelligence Analyst, Field	$221	1	$280	($20)	$81	($20)	$81
Intelligence Analyst, HQ	$1,151	5	$298	($1)	$54	($3)	$270
NICS / NTOC	$979	10	$145	$49	$22	$489	$220
Police & Guards	$12,137	45	$330	($98)	$7	($4,412)	$315
Professional Support	$7,455	52	$207	$58	$42	$3,017	$2,184
Special Agent, Field	$116,174	222	$616	($53)	$70	($11,869)	$15,540
Staff Operations Specialist	$4,175	33	$184	$42	$36	$1,381	$1,188
Adjusted CART Examiner, Field	$471	3	$157	$0	$0	$0	$0
Adjusted Data Analyst	$390	3	$130	$0	$0	$0	$0
Adjusted Electronic Technician	$292	2	$146	$0	$0	$0	$0
Adjusted Foreign Intelligence Analyst	$4,760	28	$170	$0	$0	$0	$0
Adjusted Forensic Accountant	$185	1	$185	$0	$0	$0	$0

Type of Position/Series	FY 2027 Request ($000)	Positions Requested	Full Year Modular Cost per Position ($000)	Annualizations ($000)			
				2nd Year	3rd Year	FY 2028 (net change from 2027)	FY 2029 (net change from 2028)
Adjusted Information Technology	$720	5	$144	$0	$0	$0	$0
Adjusted Professional Support	$28,814	201	$143	$0	$0	$0	$0
Adjusted Staff Operations Specialist	$2,320	16	$145	$0	$0	$0	$0
Total Personnel	**$201,267**	**686**	**$6,670**	**($34)**	**$474**	**($13,059)**	**$20,676**

3. Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	FY 2027 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2028 (net change from 2028)	FY 2029 (net change from 2029)
Equipment	$66,015	N/A	N/A	$0	$0
Travel and Transportation of Persons	$650	N/A	N/A	$0	$0
Advisory and Assistance Services	$4,928	N/A	N/A	$0	$0
Other Services	$37,608	N/A	N/A	$0	$0
Supplies and Materials	$1,200	N/A	N/A	$0	$0
Total Non-Personnel	**$110,401**	**N/A**	**N/A**	**$0**	**$0**

4. Justification for Non-Personnel Annualizations

Equipment: Non-personnel funding and out years is needed to support the significant expansion of the FBI's C-UAS program, Rapid DNA technologies and capabilities, and the procurement of software and analytical tools.

Travel and Transportation of Persons: Travel costs are required in out years to support the enhancement and current FBI personnel working compliance and audit management on a multitude of FBI programs.

Advisory and Assistance Services: Once requested government employees are established, and the FBI is able to reduce its reliance on contract staff, OIA requires ongoing training to support the professional growth and development of its skilled and specialized personnel (i.e., Continuing Professional Education training for auditors and Compliance Certifications for compliance staff). Funding will also continue to support system and data analytics tools operations and maintenance.

Other Services: A significant portion of requested other services relates to the high sample volume related to the DNA collection analysis and backlog, The accumulated backlog will require a multiyear reduction effort and full annualization. Other items include a multitude of

tools and contracts which will require out year sustainment to combat violent crime, TOC, and Immigration efforts.

5. Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2028 (net change from 2027)	FY 2029 (net change from 2028)
Current Services	11,885	5,179	11,979	$2,475,912	$199,318	$2,675,230	N/A	N/A
Increases	686	238	351	$201,267	$110,401	$311,668	($13,059)	$20,676
Grand Total	**12,571**	**5,417**	**12,330**	**$2,667,179**	**$309,719**	**$2,986,898**	**($13,059)**	**$20,676**

D. Counterterrorism

Organizational Program: Counterterrorism, Critical Incident Response, Inspection, Office of General Counsel

Program Increase: Positions 328 Agent 130 Atty 5 FTE 167 Dollars $166,077,000 ($92,754,000 non-personnel)

Description

The 2028 Los Angeles (LA28) Olympic Games Security Preparations: The FBI requests $60,000,000 (all non-personnel) to fulfill its intelligence, hostage rescue, tactical response, explosives management, and render safe responsibilities in order to safeguard the LA28 Olympic Games.

Please refer to the classified addendum for additional information on the FBI's counterterrorism request.

Justification

LA28 Olympic Games Security Preparations: $60,000,000, all non-personnel

The Secretary of Homeland Security designated the LA28 Olympic and Paralympic Games as an NSSE. Per Presidential Policy Directive 22, during an NSSE, the FBI is lead agency responsible for coordinating intelligence, crisis management, counterterrorism, hostage rescue, WMD/render safe and bomb management. EO 12333 mandates the FBI provide accurate and timely intelligence regarding capabilities, intentions, and activities of foreign powers, organizations, or persons and their agents to make informed decisions for national defense. Requested resources will support planning, exercises, and training ($15.0 million); facilities, infrastructure, and security upgrades ($30.0 million); and deployment of personnel ($15.0 million).

The FBI will incur costs across three FYs to support the LA28 Olympic Games as follows:

- FY 2027: $15.0 million for planning, exercises, and training; $30.0 million for securing facilities, infrastructure, security upgrades and equipment; and $15.0 million to secure lodging contracts for the operational deployment period.
- FY 2028: $5.0 million for planning, exercises, and training; $35.0 million for operational deployments; and $20.0 million for facility upgrades and equipment.
- FY 2029: $10.0 million to reconstitute venues and remove equipment.

The Olympic Games will be held primarily in Los Angeles, California, with hundreds of thousands of visitors—including U.S. and foreign dignitaries. The Olympic Games are an international phenomenon, making them an attractive target for state and non-state actors and lone offenders to carry out acts of violence or destruction. Evolving technologies also present new threats, requiring persistent attention, expertise, and resources to maintain effective preparedness and response. For example, unmanned systems technology (i.e., drones) operating in air, ground, surface, sub-surface, and underground domains, are rapidly developing and proliferating with both positive and adverse implications for security interests. Additionally, hazardous devices and their use by state and non-state actors remain a weapon of choice globally and an enduring threat. The landscape has expanded beyond internationally focused terrorist groups to include lone offenders and groups of determined violent extremists with the requisite access and knowledge to employ hazardous devices.

For the past two years, the FBI has been working diligently with USG agencies, state and local officials, and the U.S. Olympic Committee to gather resource requirements for prevention, mitigation, and response to substantial threats or incidents. FBI estimates the following associated costs:

- Planning, Exercises, and Training: requirements include planning conferences; tabletop, command post, full-scale, communications, and interagency exercises; venue/site surveys; and coordination with/training for state and local partners. Securing the Olympics requires a coordinated, collaborative effort between Federal, state, and local law enforcement agencies, and exercises/planning conferences are essential to establish a unified team; identify gaps, weaknesses, and vulnerabilities; and ensure the proper resources are positioned correctly throughout the Olympics.
- Infrastructure: given the number of venues, area covered, and scope of competition, the strategic location of personnel in emergency operations centers, joint operations centers, and command posts across the greater Los Angeles area is of utmost importance. In addition to upgrading existing facilities and mobile command post vehicles, temporary operations centers will be required. Infrastructure funding will include network facilities, security upgrades, computer equipment, and connectivity to the International Police Coordination Center across rented facilities, FBI facilities, and warehouses. Finally, restoring and reconstituting facilities may be required for original intended purposes.
- Deployment: expenses associated with personnel deployments are required including lodging, vehicle rental, airfare, meals, and parking, which will be elevated in an already high-cost area due to significantly increased demand around the Olympics. Lodging for expected deployment dates of July 7 to August 28, 2028, must be secured at least one year in advance to ensure availability. Leveraging deployment estimates from the most recent U.S.-hosted Olympic games—the 2002 Salt Lake City Winter Olympics—the 2028 Los Angeles Olympics expects to leverage approximately 1,300 FBI personnel.

Impact on Performance

The requested resources will allow the FBI to adequately prepare for and secure the LA28 Olympic Games. Diverse actors threaten the safety and security of the American people, Olympic athletes, and international visitors during these games, and effective planning helps to prevent against terrorism, cyber, and large-scale public safety incidents. These resources not only protect people and infrastructure but also ensure the LA28 Olympic Games run smoothly and project a positive image of the United States as the host country.

Funding

1. Base Funding

FY 2025 Enacted				FY 2026 Enacted				FY 2027 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
5,285	2,692	4,833	$1,049,651	5,256	2,692	4,773	$1,034,017	5,263	2,693	4,830	$1,112,698

2. Personnel Increase Cost Summary

Type of Position/Series	FY 2027 Request ($000)	Positions Requested	Full Year Modular Cost per Position ($000)	Annualizations ($000)			
				2nd Year	3rd Year	FY 2028 (net change from 2027)	FY 2029 (net change from 2028)
Computer Scientist	$4,628	16	$372	$49	$47	$787	$752
Data Analyst	$621	3	$280	$27	$30	$80	$90
Engineer	$254	1	$339	$15	$51	$15	$51
Forensic Examiner – Scientist	$1,447	6	$322	$57	$48	$342	$288
Intelligence Analyst, HQ	$2,533	11	$130	($1)	$54	($7)	$594
Professional Support	$1,290	9	$185	$58	$42	$522	$378
Special Agent, Field	$15,699	30	$126	($53)	$70	($1,604)	$2,100
Adjusted Attorney	$780	5	$156	$0	$0	$0	$0
Adjusted Data Analyst	$520	4	$130	$0	$0	$0	$0
Adjusted Electronic Technician	$292	2	$146	$0	$0	$0	$0
Adjusted Forensic Accountant	$555	3	$185	$0	$0	$0	$0
Adjusted Information Technology	$1,728	12	$144	$0	$0	$0	$0
Adjusted Professional Support	$11,630	94	$124	$0	$0	$0	$0
Adjusted Special Agent, Field	$26,706	100	$267	$0	$0	$0	$0
Adjusted Staff Operations Specialist	$4,640	32	$145	$0	$0	$0	$0
Total Personnel	**$73,323**	**328**	**$3,050**	**$152**	**$342**	**$135**	**$4,253**

3. Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	FY 2027 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2028 (net change from 2027)	FY 2029 (net change from 2028)
Equipment	$10,106	N/A	N/A	$0	$0
Travel and Transportation of Persons	$50,794	N/A	N/A	$0	$0
Other Services	$31,854	N/A	N/A	$0	$0
Total Non-Personnel	**$92,754**	**N/A**	**N/A**	**$0**	**$0**

4. Justification for Non-Personnel Annualizations

Equipment: The FBI requires a command post for the LA28 Olympic Games, including a briefing room and video technology. The FBI also requires forensic software and tools.

Travel and Transportation of Persons: The FBI requires recurring funding to ensure the LA28 Olympic Games are properly secured.

5. Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2028 (net change from 2027)	FY 2029 (net change from 2028)
Current Services	5,263	2,693	4,830	$1,059,684	$53,014	$1,112,698	N/A	N/A
Increases	328	130	167	$73,323	$92,754	$166,078	$135	$4,253
Grand Total	**5,591**	**2,823**	**4,997**	**$1,113,007**	**$145,769**	**$1,278,776**	**$135**	**$4,253**

E. Cyber

Organizational Program: Cyber, Criminal Investigative, Operational Technology, Counterintelligence

Program Increase: Positions 152 Agent 37 Atty 2 FTE 76 Dollars $95,620,000 ($61,449,000 non-personnel)

Description

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

F. Counterintelligence

Organizational Program: Counterintelligence, Directorate of Intelligence

Program Increase: Positions 154 Agent 90 Atty 0 FTE 79 Dollars $73,215,000 ($26,941,000 non-personnel)

Description

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

G. Cybersecurity

Organizational Program: Office of the Chief Information Officer, IT Infrastructure, IT Applications & Data

Program Increase: Positions 37 Agent 0 Atty 0 FTE 19 Dollars $111,120,000 ($105,032,000 non-personnel)

Description

The FBI's enterprise cybersecurity program is an essential part of protecting its most important asset: information. Due to the importance, tempo, and complexity of the FBI's mission, information resides in more than 450 information technology (IT) systems and is utilized daily by the workforce. The FBI requests 37 positions and $111,120,000 ($105,032,000 non-personnel) to harden these systems against advanced cyber adversaries; adopt new, secure technology innovations; and remain compliant with requirements set forth in Federal statutes.

Justification

Network Enterprise Redesign Initiative (NERI) with Life Cycle Management: 17 positions (0 SAs) and $42,750,000 ($40,000,000 non-personnel)

The FBI requests $42,750,000 ($40,000,000 non-personnel) to establish and sustain a dedicated network equipment life-cycle replacement program, based on a 10-year operational-life standard. This investment is critical to maintaining modern, secure, and reliable enterprise network infrastructure supporting FBI core mission functions; mitigating operational risks associated with aging equipment; reducing unplanned outages; and enabling scalable Artificial Intelligence (AI)-ready infrastructure required for timely, mission-critical information sharing.

Requested resources will allow the FBI to remain agile and responsive in detecting, disrupting, and deterring evolving threats across all domains. As the volume, velocity, and complexity of FBI data grows, leveraging advanced analytics, including AI and machine learning (ML) capabilities, is increasingly dependent on robust network performance and availability. Modern investigative and intelligence operations require real-time access to distributed data sources, high-throughput transport, and resilient systems supporting data-intensive applications.

The FBI's enterprise network connects over 35,000 government personnel across more than 1,000 locations, and maintaining the performance, security, and reliability of this infrastructure is critical to mission success. Industry best practice and manufacturer guidance recommend replacing network equipment every 8-10 years to avoid operating unsupported devices lacking security updates and software patches. Currently, a significant portion of the FBI's IT infrastructure, particularly on classified networks, is operating beyond end-of-life and cannot be patched for vulnerabilities or covered under maintenance contracts. As a result, components of the IT infrastructure are vulnerable to failure, causing network outages and introducing growing cyber risk, compounding over time without an identified and sustained funding source.

In FY 2020, the FBI launched NERI to address cybersecurity concerns stemming from a preponderance of legacy equipment and network connections vulnerable to modern cyber-attacks. From FY 2020 to FY 2024, the FBI invested over $200million to modernize approximately one-third of its enterprise network, primarily within the Unclassified domain, improving reliability, enabling automation, strengthening cybersecurity, and laying the foundation for compliance with Federal mandates such as Zero Trust Architecture and Trusted Internet Connections 3.0.

A key element of modernization efforts under NERI has been the consolidation of more than 600 fragmented networks, reducing operational complexity and technical debt and creating the unified, enterprise-scale infrastructure required for AI and ML readiness. This investment ensures the FBI can address cyber vulnerabilities from legacy devices, sustain mission readiness, and enable secure, AI-driven capabilities across the enterprise.

The FBI is also requesting additional IT specialist positions: six positions for network engineering, seven positions for network management, and four positions for network enclave support. These intermediate/senior network engineers include a Supervisory IT Specialist and will provide multi-tier enterprise engineering support for NERI, including Consolidated Transport Network, Internet Consolidated Network, and classified enclaves across FOs, RAs, Legats, and data centers. Network engineers ensure enterprise networks are resilient, scalable, and capable of supporting AI workloads, cloud connectivity, and advanced data flows. Their responsibilities include patch management, Security Technical Implementation Guide compliance, Operating System and network device hardening, and continuous security posture validation. These roles are critical to maintaining accreditation, enforcing Zero Trust principles, and ensuring the network can securely support AI systems, sensitive data, and interagency information sharing.

SCINet Infrastructure: $27,820,000 (all non-personnel)

The FBI requests $27,820,000 to support and sustain the SCINet (the FBI's Top-Secret network) infrastructure and the FBI's related facility requirements for SWE. In 2010, the ODNI issued Intelligence Community Directive 705, directing agencies to ensure SCIFs comply with uniform security requirements issued by the Director of the National Counterintelligence and Security Center. The requested resources support applying the SWE standards for physical and IT infrastructure for retrofitting, relocating, expanding, securing, improving, and/or new construction buildout to each area of responsibility. This mandate includes the FBI's over 1,100 SCIFs in FOs, RAs, Legats, and off-sites and ensures the investments support continued collaboration between the FBI and other IC agencies.

Funds will ensure sufficient hardware refresh, address critical cyber and information security requirements, and provide necessary engineering and maintenance support of this infrastructure. These activities are critical to supporting the FBI's national security mission and its collaboration with IC partners.

Cybersecurity: 10 positions (0 SAs) and $22,893,000 ($21,638,000 non-personnel)

The FBI requests 10 positions and $22,893,000 ($21,638,000 non-personnel) for enterprise cybersecurity preparedness, establishing a foundation for continued improvements through the secure introduction of AI to address future threats and risks.

Secure Adoption of AI: $2,900,000 (all non-personnel)

To adopt AI securely and in alignment with EO 14179, Removing Barriers to American Leadership in Artificial Intelligence, the FBI must have a workforce skilled in the design, development, and implementation of AI capabilities, as well as a team dedicated to its deployment in accordance with the legal requirements outlined by the National Institute of Standards and Technologies (NIST) as the foundation for receiving an Authorization to Operate (ATO). Requested resources will provide seven AI Information System Security Engineer contractors to coordinate responses to IT system threats, monitor and assess risk, oversee

compliance with the Federal Information Security Modernization Act, and execute the Security Assessment and Authorization (SAA) process for all FBI information systems.

Forward-Deployed Cybersecurity: $8,738,000 (all non-personnel)

Since FY 2023, the FBI has been conducting cybersecurity assessments of FOs, RAs, and offsite locations, evaluating approximately 47 percent of FBI locations to date. Requested resources will increase cybersecurity team activities for multiple FBI locations per month; establish a Cyber Impact Team to conduct follow-up assessments; and refresh end-of-life technical equipment.

Automation of Cybersecurity Assessments: $7,000,000 (all non-personnel)

The FBI will leverage AI to enhance its SAA process, via the following activities:

- Security assessment team creation and tool acquisition ($3,100,000): Resources will transform the labor-intensive implementation of the NIST Risk Management Framework—used to grant ATOs and required by statute for each of the FBI's over 450 information systems—leveraging an AI assessor tool to reduce time required to achieve an ATO via six technical contractors and cloud hosting on three secure enclaves.
- Enterprise vulnerability scanning modernization ($3,900,000): Detection of vulnerabilities across the FBI's IT footprint is critical to ensure patches are applied and systems and data are not compromised. Requested funding will establish a primary server in an existing FBI data center, with standard FBI system redundancy capabilities, providing six contractors to integrate all FBI systems into the new infrastructure.

Cybersecurity Program Management $3,000,000 (all non-personnel)

As the FBI's technology footprint has expanded in size and complexity with cloud and AI systems, it has become increasingly difficult to ensure all systems and technologies follow legal and policy requirements. Requested resources will create a team to monitor and track the FBI's key security requirements including multi-factor authentication, data encryption, and vulnerability management. Contract staff will focus on data collection, reporting, and deconfliction to determine how to direct future investments most efficiently and effectively.

Augment the FBI's Information Security Workforce: 10 positions ($1,255,000 all personnel)

As required by law, the FBI must conduct a full security assessment of all IT systems prior to deployment. The FBI's cybersecurity preparedness program is dependent on skilled information security personnel to undertake these assessments and requires 10 additional IT Specialists (ITSs) to fully support these security assessments and authorizations.

Enterprise Cybersecurity Monitoring Modernization: 10 positions (0 SAs) and $13,657,000 ($11,574,000 non-personnel)

The FBI requests 10 positions and $13,657,000 ($11,574,000 non-personnel) to modernize cybersecurity monitoring capabilities; close existing gaps; mitigate enterprise risk; and protect the FBI from cyber threats posed by hostile nation states, TCOs, and lone wolf actors. Monitoring, detecting, and responding to threats against the FBI's IT systems and data spans over 1,300 systems, applications, and networks across multiple enclaves, and the FBI must collect and maintain data to address cyber and insider threat incidents consistent with applicable law. Requested resources will modernize the FBI's cybersecurity threat monitoring, detection, and response capabilities while simultaneously shortening the implementation and compliance

timeline for EO 14028, Improving the Nation's Cybersecurity and EO 14144, Strengthening and Promoting Innovation in the Nation's Cybersecurity (as amended by EO 14306).

Enterprise Cybersecurity Data Pipeline (ECDP): 10 positions and $8,657,000 ($6,574,000 non-personnel)

Requested resources will support the development of an ECDP capable of moving over 30 terabytes of daily log data from Unclassified and Secret systems, applications, and networks into a centralized log repository located on the FBI's primary Secret enclave. When this log data is in transit, specific subsets most critical to cybersecurity monitoring, detection, and response—OMB Memorandum M 21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents (or its successor)—will be standardized and diverted to the FBI's Security Information and Event Management (SIEM) tools, where custom alerts are generated and triaged for further analysis and response. Remaining log data will reside in the centralized repository for up to 30 months and remain available for advanced cyber threat hunting and incident response by system owners and cybersecurity experts. Housing this data on a Secret-level system, instead of across enclaves, enables simplified research and monitoring as well as advanced threat hunting through classified cyber threat tactics, techniques, and procedures identified by FBI and other IC partner investigations.

Requested resources include the following personnel and non-personnel assets:

- Three Data Analysts
- Two Data Engineers
- Two Data Scientists
- Three ITSs
- Data normalization tool ($1,574,000)
- Bulk data cross-domain solution ($2,000,000)
- Cloud storage costs ($3,000,000)

Cyber Threat Intelligence Platform (CTIP): $1,500,000 (all non-personnel)

Requested resources will secure an industry standard CTIP to enable more effective and efficient threat hunting capabilities within the FBI's centralized log repository and SIEM. This investment will allow the Enterprise Security Operations Center's (ESOC) incident response operations to avoid manual processes and instead provide critical capabilities for gathering, analyzing, and sharing threat intelligence. The ability to consolidate and correlate threat data from disparate sources increases the accuracy and timeliness of threat assessments, improving overall decision making and decreasing risk to the FBI's cybersecurity resilience.

Security Orchestration, Automation & Response (SOAR): $1,500,000 (all non-personnel)

Requested resources will secure a SOAR tool for automatic incident response via connected alerts from ESOC's SIEM, CTIP, and other data sources to define, prioritize, and drive standardized incident response activities. A SOAR will significantly improve ESOC's efficiency by handling low-risk security alerts without manual intervention, enabling ESOC staff to focus on the most critical of the 20,000 monthly network events.

FBI Enterprise Developer Services (FEDS) Centralized Logging: $2,000,000 (all non-personnel)

FEDS Centralized Logging hosts FBI enterprise infrastructure to meet EOs 14028 and 14144 (as amended) requirements for all IT assets, collecting and managing substantial volumes of data and enabling analytics and monitoring for threat detection and response. This ingest and centralization is critical to correlate events—such as user access of systems and login times—and allows ESOC's incident response teams to identify patterns not visible in isolated logs for faster incident response. Additionally, centralized logging facilitates automated alerts and threat detection and improves both the speed and accuracy of threat identification.

FEDS Centralized Logging requires $2,000,000 for "around-the-clock" engineering support across four separate logging instances on Unclassified, Secret, and Top-Secret enclaves. These efforts will enable ESOC to identify and respond to enterprise cybersecurity incidents and permit owners to support and maintain their systems and applications with built-in monitoring tools. The scope of work is growing as more IT systems send logs to the centralized instance, and as cybersecurity incidents and attacks from adversaries increase, ESOC will rely heavily on the incident response and monitoring capabilities provided by FEDS Centralized Logging.

Data Warehouse System (DWS)/Insight Modernization: $4,000,000 (all non-personnel)

The FBI requests $4,000,000 for contract support to further design, develop, and deploy a consolidated solution for DWS and Insight, systems utilized for the storage, processing, and handling of Foreign Intelligence Surveillance Act (FISA) and FISA Amendments Act (FAA) 702 data. This consolidated solution will strengthen oversight of FISA and FAA 702 data while streamlining reviews by SAs and IAs. Additional funding to support modernization efforts will allow the FBI to enhance adherence to FISA Court, DOJ, and FBI policies and procedures.

These investments would create efficiencies in developing standardized compliance capabilities for the FBI's FISA data holdings across standard minimization procedures, query, and data retention functions. O&M requirements would be consolidated under a single program management team, streamlining application enhancements by moving away from the current decentralized structure. Both Insight and DWS are critical applications used in support of national security investigations and provide key search, visualization, and triage capabilities. Planned enhancements will further enable SAs and IAs to efficiently review and triage large volumes of data collections in support of investigations, reinforcing two of the FBI's strategic priorities: Rebuilding Public Trust and Fierce Organizational Accountability.

Impact on Performance

Investing in these cybersecurity and infrastructure improvements will position the FBI to fully support modern law enforcement, enabling secure communications, rapid intelligence sharing, and coordinated operations to protect the American people and uphold the Constitution. As threats become increasingly digital and borderless, the FBI must evolve to support advanced cybersecurity, resilient infrastructure, and AI-driven capabilities. Requested resources will ensure the FBI can modernize all enclaves, secure mission-critical systems, and maintain transparency, accountability, and operational readiness.

Funding

1. Base Funding

FY 2025 Enacted				FY 2026 Enacted				FY 2027 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
213	6	204	$265,519	253	9	207	$251,108	253	9	206	$256,584

2. Personnel Increase Cost Summary

Type of Position/Series	FY 2027 Request ($000)	Positions Requested	Full Year Modular Cost per Position ($000)	Annualizations ($000)			
				2nd Year	3rd Year	FY 2028 (net change from 2027)	FY 2029 (net change from 2028)
Computer Scientist	$579	2	$372	$49	$47	$98	$94
Data Analyst	$621	3	$280	$27	$30	$80	$90
Engineer	$761	3	$339	$15	$51	$45	$153
Information Technology	$1,631	13	$200	$98	$23	$1,273	$299
Adjusted Professional Support	$2,496	16	$156	$0	$0	$0	$0
Total Personnel	**$6,088**	**37**	**$1,346**	**$189**	**$151**	**$1,496**	**$636**

3. Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	FY 2027 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2028 (net change from 2027)	FY 2029 (net change from 2028)
Equipment	$6,574	N/A	N/A	$0	$0
Travel and Transportation of Persons	$2,000	N/A	N/A	$0	$0
Other Services	$96,458	N/A	N/A	-$4,000	$0
Total Non-Personnel	**$105,032**	**N/A**	**N/A**	**-$4,000**	**$0**

4. Justification for Non-Personnel Annualizations

In addition to increased cybersecurity capabilities, requested resources will foster coordinated efforts of multiple teams while fulfilling general activities required on a recurring basis. Out-year resources are required to maintain these initiatives so risk to the FBI infrastructure and integrity is effectively mitigated.

5. Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2028 (net change from 2027)	FY 2029 (net change from 2028)
Current Services	253	9	206	$49,979	$206,605	$256,584	N/A	N/A
Increases	37	0	19	$6,088	$105,032	$111,120	-$2,504	$636
Grand Total	**290**	**9**	**225**	**$56,067**	**$311,637**	**$367,704**	**-$2,504**	**$636**

H. Field Investigative Capabilities

Organizational Program: Critical Incident Response Group, Operational Technology

Program Increase: Positions 515 Agent 69 Atty 0 FTE 265 Dollars $144,775,000 ($43,068,000 non-personnel)

Description

The requested resources will improve the FBI's investigative capabilities in the digital and forensic world, improve hiring and retention of highly specialized personnel, and support the operational and technical needs of the FBI's Tactical Task Force programs. The FBI must address hiring challenges for hard-to-fill roles and locations, attract specialized talent in competitive markets, retain valuable employees, and secure critical skills to ensure mission continuity and operational readiness.

A significant portion of requested resources will allow the FBI to provide additional investigative support directly to the field. The FBI accomplishes this by providing personnel to key operational programs, such as the newly formed HSTF; directing investigative support through increased resources to the FBI's CIRG and DI programs; and increasing hiring and onboarding support through various human resources, training, and security personnel programs.

Additional information pursuant to the Field Investigative Capabilities request is included in the classified addendum.

Justification

Recruitment, Retention and Relocation Incentives: $15,000,000, all personnel.

The FBI requests $15,000,000 to support targeted recruitment, relocation, and retention incentives for priority hiring initiatives focused on mission-critical, hard-to-fill positions. These incentives are essential to sustaining operational readiness, addressing persistent staffing gaps, and ensuring the FBI can execute its statutory and national security responsibilities.

The FBI is focused on building a strong talent pipeline, recruiting professionals with specialized skills, directly enabling the FBI to meet statutory, operational, and national security requirements. Additionally, the FBI seeks individuals who are not only highly skilled but also adaptable, eager to learn, and capable of developing the specialized expertise needed to support intelligence and law enforcement, including expertise in Science, Technology, Engineering, and Mathematics (STEM). These positions need to be incentivized to get ahead of attrition and to hire people into positions in an exceedingly competitive job market where private sector companies and other government agencies can offer similar or more competitive financial compensation packages.

- Recruitment Incentives – Private sector compensation, flexibility, and recruitment incentives routinely exceed Federal pay structures, creating recruitment and retention challenges despite strong public service interest. Recruitment incentives improve offer acceptance rates, reduce time-to-hire and vacancy duration, and expand the qualified candidate pool.
- Retention Incentives – Prolonged vacancies or high attrition increase mission risk, impact operations, reduce analytic and technical capacity, and increase workload for current

personnel. Incentives will improve retention of experienced FBI personnel and protect investments in specialized training and certifications.

- Relocation Incentives – Many positions require relocation to hard-to-staff duty locations across the United States. Relocation incentives mitigate financial barriers associated with moving to high-cost locations and enable the FBI to ensure operational needs are met across diverse geographic locations.

Impact on Performance

The FBI faces increased difficulty recruiting and retaining qualified professionals due to intense competition from the private sector and other Federal agencies. Filling vacancies as quickly as possible and minimizing attrition rates will better position the FBI to ensure mission execution and operational readiness to combat criminal and national security threats. The targeted use of additional incentives will reduce vacancy duration, improve retention of experienced personnel and improve operational continuity and productivity.

Funding

1. Base Funding

FY 2025 Enacted				FY 2026 Enacted				FY 2027 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
17,766	8,726	17,216	$3,463,219	19,281	9,423	18,651	$3,806,507	19,669	9,753	18,812	$4,045,415

2. Personnel Increase Cost Summary

Type of Position/Series	FY 2027 Request ($000)	Positions Requested	Full Year Modular Cost per Position ($000)	Annualizations ($000)			
				2nd Year	3rd Year	FY 2028 (net change from 2027)	FY 2029 (net change from 2028)
Computer Scientist	$289	1	$372	$49	$47	$49	$47
Non-Agent Responder	$1,585	4	$500	($108)	$6	($432)	$24
Professional Support	$1,864	13	$207	$58	$42	$754	$546
Special Agent	$11,513	22	$616	($53)	$70	($1,176)	$1,540
Technically Trained Agent	$2,947	5	$681	($56)	$70	($280)	$350
Adjusted CART Examiner, Field	$2,669	17	$157	$0	$0	$0	$0
Adjusted Data Analyst	$1,430	11	$130	$0	$0	$0	$0
Adjusted Electronic Technician	$1,606	11	$146	$0	$0	$0	$0
Adjusted Forensic Accountant	$1,805	9	$201	$0	$0	$0	$0
Adjusted Information Technology	$3,456	24	$144	$0	$0	$0	$0
Adjusted Language Specialist	$3,280	20	$164	$0	$0	$0	$0
Adjusted Professional Support	$26,653	221	$121	$0	$0	$0	$0
Adjusted Special Agent, Field	$11,600	42	$276	$0	$0	$0	$0
Adjusted Special Surveillance Group	$4,410	35	$126	$0	$0	$0	$0
Adjusted Staff Operations Specialist	$11,600	80	$145	$0	$0	$0	$0
Special Agent Retainment Incentive	$15,000	0	$0	$0	$0	$0	$
Total Personnel	**$101,707**	**515**	**$3,985**	**($110)**	**$235**	**($1,085)**	**$2,507**

3. Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	FY 2027 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2028 (net change from 2027)	FY 2029 (net change from 2028)
Equipment	$25,822	N/A	N/A	$0	$0
Travel and Transportation of Persons	$1,000	N/A	N/A	$0	$0
Other Services	$5,000	N/A	N/A	$0	$0
Supplies and Materials	$11,046	N/A	N/A	$0	$0
Rental Payments to Others	$200	N/A	N/A	$0	$0
Total Non-Personnel	**$43,068**	**N/A**	**N/A**	**$0**	**$0**

4. Justification for Non-Personnel Annualizations.

The FBI requires this personnel funding to recur to ensure the FBI's ability to sustain hiring and retention benefits provided through this request.

5. Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2028 (net change from 2027)	FY 2029 (net change from 2028)
Current Services	19,669	9,753	18,812	$3,973,451	$71,963	$4,045,415	N/A	N/A
Increases	515	69	265	$101,707	$43,068	$144,775	($1,085)	$2,507
Grand Total	**20,184**	**9,822**	**19,077**	**$4,075,158**	**$115,031**	**$4,190,189**	**($1,085)**	**$2,507**

I. 21st Century Advanced Training at Redstone

Organizational Program: Training

Program Increase: Positions 46 Agent nine Atty two FTE 23 Dollars $29,432,000 ($18,982,000 non-personnel)

Description

The FBI requests 46 positions (9 SAs, 2 Attys) and $29,432,000 ($18,982,000 non-personnel) to provide operational support of intermediate and advanced training at Redstone Academy (RSA), which is the training component of the Richard Shelby Center for Innovation and Advanced Training in Huntsville, AL. Specifically, requested resources will establish three units at RSA—Redstone Academy Training Coordination and Support (RATCSU), Law Enforcement Skills Training (LESTU), and Redstone Academy Practical Training and Operations Research (RAPTOR)—overseeing training coordination, logistics, and support; developing intermediate and advanced curriculum; and managing the Practical Problem Venues (PPVs). The requested resources will directly impact and enhance the FBI's ability to combat violent crime and defend the homeland.

Justification

Huntsville Advanced Training: 46 positions (9 SAs, 2 Attys) and $29,432,000 ($18,982,000 non-personnel)

Redstone Academy includes the North Campus Innovation Center and National Security and Intelligence Center of Excellence buildings, and the South Campus PPVs. These facilities will allow the FBI to teach FBI employees and law enforcement partners to address the most complex, technologically advanced threats in real-world settings, while providing interdisciplinary learning opportunities for more holistic training. With more than 10,000 trainees anticipated annually, Redstone Academy will allow efficient use of resources, technology, and personnel as centrally located units reduce redundancies, foster collaboration between FBI divisions and law enforcement partners, and leverage economies of scale for cost savings and improved resource allocation.

The RATCSU will be a central hub governing scheduling, logistics, curriculum development, and evaluation for training events. Centralizing support will simplify administration, minimize duplication, standardize events, and disseminate consistent communications across Redstone Academy. This unit will process hundreds of training event requests and coordinate travel and accommodations for thousands of students annually. Curriculum development personnel will analyze, design, and develop advanced learning materials, preparing students to investigate the most complex cases. Instruction on safely operating in a UTS environment will underpin all training, including how to exploit UTS data to advance investigations. Working closely with operational divisions and law enforcement partner agencies, the FBI will deliver mission-focused and large-scale integrated field exercises, preparing students to work together mitigating threats. The request also includes two Attorney positions to provide legal and policy support and ensure regulatory compliance.

LESTU will deliver advanced law enforcement skills training, tactical skills training, active shooter training, and Law Enforcement Training for Safety and Survival (LETSS). Offered to FBI SAs, TFOs, and other law enforcement partners, LETSS teaches skills to handle critical situations in high-risk environments. This unit will provide Defensive Tactics and Firearms

instructor certifications, as well as high-performance physical fitness training, defensive tactics re-certification training, and quarterly firearms qualifications for law enforcement personnel.

RAPTOR will oversee daily operations of the PPVs—36 acres of comprehensive, state-of-the-art facilities with capacity to train 150 FBI and other government agency personnel daily in a monitored UTS environment; conduct R&D; and test and evaluate new technologies before deployment. RAPTOR will provide advanced operations and tradecraft training using practical scenarios and role players for real-world experiences with UTS and other technologies, such as UAS, counter-UAS, WMD, cyber-attacks and disruptions, and video surveillance. RAPTOR will collect curriculum and venue requirements, ensuring learning objectives are achieved and training operations are supported. RAPTOR personnel will serve as Principal Safety Officers over all PPV activity, oversee non-lethal training weapons, manage training from the PPV Command Center coordinated with Redstone Arsenal safety and command entities, and provide UTS data collected during training scenarios to end-users for analysis.

The table below details the full Redstone Academy staffing plan.

Position/Function	**Quantity**
Redstone Academy Training Coordination and Support	
MAPA Supervisor	1
MAPA Scheduling/Communications	1
MAPA Lodging/Transportation	1
MAPA Conferences/Events On-Site Support	2
Writer/Editor	1
Program Analyst Training Evaluations	1
Instructional Systems Specialist	3
Multimedia Specialist	2
Attorney	2
Law Enforcement Skills Training Unit	
Unit Chief	1
Instructor	4
MAPA	1
Law Enforcement Specialist	3
Redstone Academy Practical Training and Operations Research Unit	
Unit Chief	1
Program Manager – Technology/R&D	2
Command Center Watch Commander	2
Command Center Chief Controller	1
Trainer	4
Law Enforcement Specialist	3
Command Center Controller – ITS	4
MAPA	2
Electronics Technician	2
Equipment Specialist	2
Total	**46**

The request includes $3,469,000 in non-personnel resources for software development, licensing, equipment, and travel, including $1,197,000 to incorporate Redstone Academy scheduling,

curricula, and classroom management into FBI systems; $510,000 for physical fitness, tactical, firearm, and LETSS training equipment; and $244,000 for travel costs. Another $1,518,000 will purchase operational and test equipment for R&D in the PPV infrastructure.

The request also includes $15,435,000 for training travel costs to supplement efforts to build and consolidate the FBI's advanced training programs within the National Capital Region and surrounding localities through relocation to the Redstone Academy. The funds will allow the FBI to maximize usage of FBI Redstone training classrooms and PPVs. Intermediate and advanced training will support all investigative programs and will prepare personnel to swiftly and safely execute their missions to crush violent crime, protect the American people and uphold the Constitution of the United States.

Impact on Performance

Requested resources will allow the FBI to establish the Redstone Academy and deliver essential training to FBI employees and law enforcement partners. The FBI’s existing training personnel are operating at full capacity to support basic training requirements, preventing the development and delivery of advanced training for complex threats. Dedicated logistics personnel will coordinate and streamline training resources and processes, eliminate redundancies, and ensure seamless operations. RAPTOR will provide invaluable hands-on training, bridging the gap between theoretical knowledge and practical application. Together, these investments will elevate the FBI's advanced training programs, helping highly skilled professionals perform and excel. With foundational work required prior to operations and significant lead time anticipated for hiring, personnel resources must be onboard during construction and in advance of PPV substantial completion expected in 2028.

Funding

1. Base Funding

FY 2025 Enacted				FY 2026 Enacted				FY 2027 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
0	0	0	$0	0	0	0	$0	0	0	0	$0

2. Personnel Increase Cost Summary

Type of Position/Series	FY 2027 Request ($000)	Positions Requested	Full Year Modular Cost per Position ($000)	Annualizations ($000)			
				2nd Year	3rd Year	FY 2028 (net change from 2027)	FY 2029 (net change from 2028)
Attorney	$434	2	$345	$90	$0	$179	$0
Electronic Technician	$647	2	$404	($54)	$12	($107)	$24
Information Technology	$502	4	$200	$98	$23	$392	$92
Professional Support	$4,158	29	$207	$58	$42	$1,682	$1,218
Special Agent, Field	$4,710	9	$616	($53)	$70	($481)	$630
Total Personnel	**$10,451**	**46**	**$1,772**	**$139**	**$147**	**$1,665**	**$1,964**

3. Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	FY 2027 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2028 (net change from 2027)	FY 2029 (net change from 2028)
Other Services	$18,982	N/A	N/A	$0	$0
Total Non-Personnel	**$18,982**	**N/A**	**N/A**	**$0**	**$0**

4. Justification for Non-Personnel Annualizations

Full recurral is requested for the ongoing sustainment and maintenance costs associated with the Richard Shelby Center for Innovation and Advanced Training (RSCIAT).

Non-personnel funding and recurral is needed for procurement of software licenses for personnel to perform their jobs. These licenses will need to be renewed annually; therefore, there is a recurring cost.

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2028 (net change from 2027)	FY 2029 (net change from 2028)
Current Services	0	0	0	$0	$0	$0	N/A	N/A
Increases	46	11	23	$10,451	$18,982	$29,432	$1,665	$1,964
Grand Total	**46**	**11**	**23**	**$10,451**	**$18,892**	**$29,432**	**$1,665**	**$1,964**

J. Insider Threat

Organizational Program: Security

Program Increase: Positions 72 Agent 1 Atty 2 FTE 36 Dollars $18,941,000 ($8,180,000 non-personnel)

Description

The FBI requests 72 positions (1 SA, 2 Atty) and $18,941,000 ($8,180,000 non-personnel) to comply with the Trusted Workforce (TW) 2.0 framework required by the Office of the Director of National Intelligence (ODNI) and the Office of Personnel Management (OPM).

The TW 2.0 initiative began in 2018 to streamline new hire onboarding processes, enable mobility in the Federal workforce, provide insight into workforce behaviors, and make informed trust determinations. As an Investigative Service Provider (ISP), the FBI must comply with TW 2.0 when conducting personnel Background Investigations (BIs) for employees, contractors, and Task Force Officers. The FBI also supports BIs for Other Government Agencies, including the DOJ and the White House. As such, other agencies rely on the FBI to uphold the standards set forth in TW 2.0, as well as other laws, EOs, and Office of Management and Budget Circular A-11 guidance governing the execution of BIs.

Justification

Trusted Workforce 2.0: 72 positions (1 SA, 2 Atty) and $18,941,000 ($8,180,000 non-personnel)

The FBI is currently operating as a certified TW 1.5 agency and has successfully implemented some TW 2.0 requirements for personnel vetting processes. To achieve TW 2.0 certification, the FBI must incorporate TW 2.0 requirements into all personnel vetting scenarios:

- Initial Vetting: the collection of information needed to assess whether an individual is trusted to protect people, property, information, and mission;
- Continuous Vetting (CV): information used to verify an individual's current and prior background investigation, adjudication, and clearance history;
- Upgrades: data sources, interviews, and other investigative requirements of a higher investigative tier;
- Transfer-of-Trust: the acknowledgement and acceptance of a previous background investigation or CV conducted by another ISP; and
- Re-Establishment-of-Trust: risk-management approach to reestablish trust with a former insider seeking to return to perform work for or on behalf of the USG.

In FY 2024, ODNI released Federal Personnel Vetting Performance Management Standards outlining requirements for various stages of the vetting process. Within these requirements, the FBI must address timeliness-related functions for each phase of the personnel vetting scenarios. To satisfy the requirements of ODNI, the FBI's CV tool and the modernized case management system—Background Evolution and Security Transformation (BEAST)—require additional automation and technical development to track each phase of these processes. In addition, an increase in personnel is required to successfully accomplish ODNI measures

to meet the decreased completion time allotted for each phase of the review. As such, the FBI requests the following 72 positions to support the implementation of TW 2.0:

- 40 Security Specialists (SSs)
- One Lead SS
- One Program Manager
- 17 Program Analysts
- Five Information Technology Specialists
- Two Attorneys
- One Paralegal Specialist
- One Special Agent
- Four Management and Program Analysts

The FBI requests $8,180,000 in non-personnel funding to address software enhancements, maintain the CV tool and BEAST, procure equipment, and provide training as follows:

- CV Tool and O&M ($2,680,000): to maintain and enhance the FBI's CV tool, used to aggregate ODNI data and deconflict internal FBI holdings, allowing for workflow automation and cross-agency information sharing, and as the case management system to assist FBI security personnel with continuous risk evaluation;
- BEAST System ($4,000,000): to address TW 2.0-specific developmental needs and O&M for BEAST, the FBI's centralized system for conducting timely intake, investigations, and adjudication determinations. Additionally, this funding will address connectivity to external partner systems—such as the National Background Investigation Services application and Social Security Administration systems—and incorporate a complete overhaul of the Personnel Vetting Questionnaire as the replacement to the SF-86 and required by TW 2.0;
- Publicly Available Social Media Information Checks ($350,000): to address social media exploitation tool acquisition, use, and retention of publicly available information to enhance personnel security vetting, as well as IT infrastructure development and maintenance to protect the FBI from cybersecurity-related risks and threats;
- Polygraph Program Enhancements ($900,000): to ensure Polygraph Examiners receive adequate training and equipment to carry out the personnel vetting mission; and
- National Training Standards (NTS) Implementation and Travel ($250,000): to incorporate NTS for individuals performing background investigations, national security adjudications, and suitability adjudications in compliance with ODNI and OPM mandates. Training will be designed to ODNI, OPM, and FBI requirements to inform and create a workforce of SMEs. Travel funding will allow FBI personnel to participate in TW 2.0-related meetings and conferences with external partner agencies, interagency information exchanges, and stakeholder and executive engagements.

Impact on Performance

Requested resources will enable the FBI to fully comply with TW 2.0 personnel vetting processes and keep pace with ever-evolving missions, threat indicators, threat landscapes, workforces, and technology. Additionally, these resources will enable the FBI to successfully adhere to all directives, laws, and policies for its role in personnel vetting program reform as an ISP. This request will position the FBI to make sound determinations and safeguard national security information.

Funding

1. Base Funding

FY 2025 Enacted				FY 2026 Enacted				FY 2027 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
37	0	37	$11,892	37	0	37	$11,952	37	0	37	$12,130

2. Personnel Increase Cost Summary

Type of Position/Series	FY 2027 Request ($000)	Positions Requested	Full Year Modular Cost per Position ($000)	Annualizations ($000)			
				1st Year	2nd Year	FY 2028 (net change from 2027)	FY 2029 (net change from 2028)
Attorney	$434	2	$345	$90	$0	$179	$0
Information Technology	$628	5	$200	$98	$23	$490	$115
Professional Support	$9,176	64	$207	$58	$42	$3,713	$2,688
Special Agent, Field	$523	1	$616	($54)	$70	($53)	$70
Total Personnel	**$10,761**	**72**	**$1,368**	**$192**	**$135**	**$4,329**	**$2,873**

3. Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	FY 2027 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2028 (net change from 2027)	FY 2029 (net change from 2028)
Other Services	$1,150	N/A	N/A	$0	$0
Operation and Maintenance of Equipment	$7,030	N/A	N/A	$0	$0
Total Non-Personnel	**$8,180**	**N/A**	**N/A**	**$0**	**$0**

4. Justification for Non-Personnel Annualizations

Other Services: The FBI requests the full recurral of funding related to polygraph examinations ($900,000) and continue incorporation of NTS ($250,000) in the outyears.

Operation and Maintenance of Equipment: The FBI requests full recurral of costs related to continual development and O&M for the CV tool ($2,680,000), development and O&M needs for the BEAST system ($4,000,000), and continued support for publicly available information checks ($350,000).

5. Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2028 (net change from 2027)	FY 2029 (net change from 2028)
Current Services	37	0	37	6,189	$5,941	12,130	N/A	N/A
Increases	72	3	36	$10,761	$8,180	$18,941	$4,329	$2,873
Grand Total	**109**	**3**	**73**	**16,950**	**$14,121**	**31,071**	**$4,329**	**$2,873**

K. Transparency of Government and Promoting Public Trust

Organizational Program: Information Management, Inspection

Program Increase: Positions 16 Agent 0 Atty 0 FTE 8 Dollars $31,284,000 ($28,990,000 non-personnel)

Description

The FBI requests 16 positions (0 SAs, 0 Attys) and $31,284,000 ($28,990,000 non-personnel) to proactively identify insider risk, reduce FOIA request backlogs and subsequent litigation, and eliminate unauthorized disclosures. Requested resources will enable the FBI to protect the American people, uphold the Constitution, and provide transparency into the work done to accomplish the mission.

Justification

User Activity Monitoring (UAM) Technology: $11,400,000 (all non-personnel)

The FBI is strategically shifting its insider risk identification posture from traditional reactive activities to enhanced proactive approaches, allowing for early detection and mitigation. Central to this shift is the anticipated procurement of a risk management suite in FY 2026 with two interconnected functions: a UAM collection agent containing an analysis/workflow interface; and a behavioral analytics module. Once procured, the FBI requires $11,400,000 (all non-personnel) to support O&M of the suite.

The UAM module will serve as the FBI's primary monitoring and logging tool, capturing and analyzing all employee activity as required by EO 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, mandating all FBI networks are protected by monitoring and auditing user activity. The system generates real-time alerts, audit logs, and reports to notify insider threat analysts of potential risks, such as unauthorized access to sensitive data or files. The system also provides robust forensic capabilities critical to support DOJ and FBI insider threat and CI investigations. Additionally, the suite hosts a behavioral module, using advanced analytics across all FBI-managed endpoints to detect anomalous and high-risk user activity indicative of insider threats. Requested resources will support the following O&M requirements in the UAM suite: software fees; platform host fees; storage and backup costs; and SME support.

Freedom of Information Act Processing: 16 positions and $12,884,000 ($10,590,000 non-personnel)

The FBI strives to provide the American people with accurate and timely responses to requests made under the Freedom of Information and Privacy Acts—Title 5 U.S. Code, Sections 552 and 552a respectively—together referred to as FOIPA. The FBI's FOIPA program is recognized for having among the highest request volumes in the Federal Government. Enacted in 1966, the FOIA statute directs Federal agencies to process requests within 20 business days, absent unusual circumstances. However, FBI compliance with this mandate is not possible given the high request volume, directly contributing to the rising backlog and subsequent expenses for FOIPA lawsuits. The FBI requests 16 positions (0 SAs) and $8,884,000 ($6,590,000 non-personnel) to mitigate the growth in unaddressed work and litigations resulting from the volume of incoming FOIPA requests. FOIPA workload has grown to almost 11,000 pending requests and near 500 pending litigations, totaling over 10 million pages awaiting processing. In addition, the

FBI requests non-personnel resources for technological advancements to automate processes and maximize productivity.

FOIPA processes require the ability to receive and respond to incoming requests, conduct record searches, and forward records to processing queues. Additional Government Information Specialists and contract support will increase productivity, resulting in a reduced backlog as each analyst will process on average an additional 9,600 pages and close 257 cases per year. This will strengthen FBI compliance with EO responses, Congressional inquiries, Attorney General and Director of National Intelligence record dissemination projects, and enterprise-level transparency initiatives. Contract staff will also develop and maintain automation processes via the integration of the FBI's AI/ML prototype into the FOIPA case management solution. Results of these streamlined, automated efforts will include the identification of protected information and statutory exemptions within millions of pages of FOIPA releases annually.

Requested resources will allow the FBI to consistently meet statutory obligations for increasing requests and litigations; to comply with the President's promise to provide full transparency on the FBI's activities to the American public; to highlight the FBI's commitment to government transparency; and to mitigate the risk of potential legal sanction due to non-compliance with FOIA statutes and increased Congressional oversight.

In addition, the FBI requests $4,000,000 (all non-personnel) to obtain a document processing system to serve as a singular solution for the collection, review, and production of all outside-entity document requests, such as FOIA; civil litigation; criminal discovery; Congressional; public affairs; Inspector General; Government Accountability Office; the White House; and other agencies. Currently, FOIA processing entities in the FBI's information management program leverage a single system to address requests. To ensure document integrity and consistency across the enterprise and prevent undermining FOIA productions via other releases, a consolidated ingest system is required.

Digital Watermarking Solution: $7,000,000 (all non-personnel)

The FBI requests $7,000,000 to procure and deploy a digital watermarking solution capable of embedding unique digital forensic watermarks in commonly shared documents to mitigate unauthorized disclosures from the FBI's classified and unclassified networks.

Digital watermarking embeds a unique overt or covert forensic marker into emails and other commonly used file types, making it possible to attribute leaked information via screen photography or other non-traditional means back to the user. If information is exfiltrated from an FBI-managed endpoint, the watermarking solution can trace the document back to an employee or group of employees. Requested resources include software licensing fees and contract personnel, but not storage and data transport costs required for future years; this will be addressed through a future budget request.

Impact on Performance

The FBI strives to gain and keep the American people's trust, and requested resources will ensure compliance with statutory obligations for full transparency to the public, as well as protect all FBI networks. The implementation, operation, and maintenance of specific tools will prevent unauthorized disclosures of sensitive FBI information—while also mitigating insider risk and threats of workplace violence—and safeguard national security information and assets. Finally, requested resources will allow the FBI to address growing backlogs of FOIA requests and associated lawsuits with integrity and consistency across the enterprise.

Funding

1. Base Funding

FY 2025 Enacted				FY 2026 Enacted				FY 2027 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
223	0	208	$43,434	225	0	211	$45,592	225	0	212	$48,049

2. Personnel Increase Cost Summary

Type of Position/Series	FY 2027 Request ($000)	Positions Requested	Full Year Modular Cost per Position ($000)	Annualizations ($000)			
				2nd Year	3rd Year	FY 2028 (net change from 2027)	FY 2029 (net change from 2028)
Professional Support	$2,294	16	$207	$58	$42	$928	$672
Total Personnel	**$2,294**	**16**	**$207**	**$58**	**$42**	**$928**	**$672**

3. Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	FY 2027 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2028 (net change from 2027)	FY 2029 (net change from 2028)
Other Services	$28,990	N/A	N/A	$0	$0
Total Non-Personnel	**$28,890**	**N/A**	**N/A**	**$0**	**$0**

4. Justification for Non-Personnel Annualizations

Non-personnel funding and recurral is needed for O&M to sustain the UAM module, to include software fees; platform host fees; storage and backup costs; and SME support.

Non-personnel funding and recurral is needed to sustain FOIPA resources for technological advancements to automate processes and maximize productivity as well as a document processing system to serve as a singular solution for the collection, review, and production of all outside-entity document requests.

Non-personnel funding and recurral is needed to sustain a commercial digital watermarking solution capable of embedding unique digital forensic watermarks in commonly shared documents to mitigate unauthorized disclosures from the FBI's classified and unclassified networks.

5. Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2028 (net change from 2026)	FY 2029 (net change from 2027)
Current Services	225	2	212	$38,081	$9,968	$48,049	N/A	N/A
Increases	16	0	8	$2,294	$28,990	$31,284	$928	$672
Grand Total	**241**	**2**	**220**	**$40,375**	**$38,958**	**$79,333**	**$928**	**$672**

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 $30,000,000 in the Construction account for the SWE program and other construction projects.

***SWE*:** SWE funds are used to apply IC SWE standards to FBI facilities – both their physical (e.g., SCIFs) and IT infrastructure 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 is expanding its footprint across the base, positioned among some of the nation's top defense, law enforcement, and technology organizations.

North Campus Rendering

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 delivered in FY 2025 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.

South Campus Rendering

The 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. In September 2025, the FBI awarded a construction contract to expand training and technology capabilities at the South Campus. This facility is scheduled for substantial completion in 2028. Through this contract, the FBI will construct Practical Problem Venues (PPVs), which will enable personnel to conduct advanced training and test technologies in settings that mimic real-world scenarios. In addition, in 2024, the FBI awarded a contract to construct the South Campus Academic Zone (AZ), which includes technology labs and classroom space; design for this project is almost complete and construction has already begun.

The unique synergy between the AZ and the PPVs will enable FBI personnel to conduct research and devise technologies in the AZ that can then be applied in the PPVs.

***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 training, equipping these positions with the skills to investigate the nation's most critical threats. 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 is 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 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 DOW. 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, 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, the Clarksburg RA – satellite office of the Pittsburgh Field Office, 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.

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; $30,000,000 to remain available until expended.

Analysis of Appropriations Language

No substantive change

VII. Glossary

Acronym	Title
ADIC	Assistant Director in Charge
AI	Artificial Intelligence
ALAT	Assistant Law Enforcement Attaché
ATB	Adjustments to Base
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
ATO	Authorization to Operate
Atty	Attorney
BIA	Bureau of Indian Affairs
BLO	Border Liaison Officer
BRAG	Bioterrorism Risk Assessment Group
BRF	Ballistics Research Facility
BSCA	Bipartisan Safer Communities Act
CAC	Crimes Against Children
CCB	Criminal and Cyber Branch
CD	Counterintelligence Division
CDE	Crime Data Explorer
CEFC	Criminal Enterprises and Federal Crimes
CEHTTF	Child Exploitation and Human Trafficking Task Forces
CHAT	Criminal History Analysis Team
CHS	Confidential Human Source
CI	Counterintelligence
CID	Criminal Investigative Division
CIRG	Critical Incident Response Group
CJIS	Criminal Justice Information Services
CJNG	Cartels Jalisco Nueva Generacion
CJS	Criminal Justice Services
CODIS	Combined DNA Index System
CT	Counterterrorism
CT/CI	Counterterrorism/Counterintelligence
CTD	Counterterrorism Division
CTIP	Cyber Threat Intelligence Platform
C-UAS	Counter-Unmanned Aircraft System
CyD	Cyber Division
DHS	Department of Homeland Security
DI	Directorate of Intelligence
DNA	Deoxyribonucleic Acid
DOW	Department of War
DOJ	Department of Justice
DT	Domestic Terrorism
DU	Decision Unit
ECDP	Enterprise Cybersecurity Data Pipeline
EO	Executive Order

Acronym	Title
ESOC	Enterprise Security Operations Center
FACE	Freedom of Access to Clinic Entrances
FBI	Federal Bureau of Investigation
FFD	Facilities and Finance Division
FFL	Federal Firearms Licensee
FLP	Foreign Language Program
FO	Field Office
FoA	Forensic Accountant
FOIA	Freedom of Information Act
FSN	Foreign Service Nationals
FSRB	Field Services Response Branch
FTE	Full-time Equivalent
FTO	Foreign Terrorist Organization
FY	Fiscal Year
HCF	Healthcare Fraud
HDS	Hazardous Devices School
HQ	Headquarters
HCB	Human Capital Branch
HRD	Human Resources Division
HSI	Homeland Security Investigations, a component of U.S. Immigration and Customs Enforcement
HSTF	Homeland Security Task Force
HT	Human Trafficking
HUMINT	Human Intelligence
HVE	Homegrown Violent Extremists
IA	Intelligence Analyst
IC	Intelligence Community
IDU	Intelligence Decision Unit
IED	Improvised Explosive Device
ILNI	Innocence Lost National Initiative
IMD	Information Management Division
InfB	Infrastructure Branch
INSD	Inspection Division
IOD	International Operations Division
IPM	Integrated Program Management
ISIS	Islamic State of Iraq and ash-Sham
IT	Information Technology
ITADD	IT Applications and Data Division
ITID	IT Infrastructure Division
ITS	Information Technology Specialist
JCODE	Joint Criminal Opioid and Darknet Enforcement
JEH	J. Edgar Hoover Building
JMC	Joint Mission Center

Acronym	Title
JTTF	Joint Terrorism Task Force
KPI	Key Performance Indicator
KSI	Key Strategic Indicator
KST	Known or Suspected Terrorist
LD	Laboratory Division
LEA	Law Enforcement Agencies
LEEP	Law Enforcement Enterprise Portal
Legat	Law Enforcement Attaché
LETSS	Law Enforcement Training for Safety and Survival
MAPA	Management and Program Analyst
NCIC	National Crime Information Center
NCIJTF	National Cyber Investigative Joint Task Force
NCMEC	National Center for Missing and Exploited Children
N-DEx	National Data Exchange
NGI	Next Generation Identification
NICS	National Instant Criminal Background Check System
NIP	National Intelligence Program
NIST	National Institute of Standards and Technologies
NSB	National Security Branch
NSC	National Security Council
NSSE	National Special Security Event
NTOC	National Threat Operations Center
NTP	National Threat Priority
NVTC	National Virtual Translation Center
OCIO	Office of the Chief Information Officer
OD	Operations Director
ODNI	Office of the Director of National Intelligence
OEEOA	Office of Equal Employment Opportunity Affairs
OGC	Office of the General Counsel
OPR	Office of Professional Responsibility
ORC	Operational Response Center
OTD	Operational Technology Division
PPV	Practical Problem Venue
PS	Professional Staff
PSBT	Public Safety Bomb Technicians
R&D	Research and Development
RA	Resident Agency
RAPTOR	Redstone Academy Practical Training and Operations Research
RFI	Request for Information
RPO	Resource Planning Office
RRB	The Ronald Reagan Building and International Trade Center
S&E	Salaries and Expenses
SA	Special Agent

Acronym	Title
SAC	Special Agent in Charge
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCINet	Sensitive Compartmented Information Network
SecD	Security Division
SIEM	Security Information and Event Management
SME	Subject Matter Expert
SOG	Special Operations Group
SSG	Special Surveillance Group
STM	Sex Trafficking of Minors
SWAT	Special Weapons and Tactics
SWE	Secure Work Environment
TCO	Transnational Criminal Organizations
TD	Training Division
TFO	Task Force Officer
TOC	Transnational Organized Crime
TRP	Threat Review and Prioritization
TS	Top Secret
TSC	Threat Screening Center
TTL	Threat to Life
U21	Under the age of 21
UAM	User Activity Monitoring
UAS	Unmanned Aircraft Systems
UCR	Uniform Crime Reporting
U.S.	United States
USG	United States Government
USPER	U.S. Person
UTS	Ubiquitous Technical Surveillance
VCAC	Violent Crimes Against Children
VGSSTF	Violent Crime and Safe Streets Gang Task Forces
VCACITF	Violent Crimes Against Children International Task Force
VSD	Victim Services Division
VT	Vetted Team
WCC	White Collar Crime
WMD	Weapons of Mass Destruction
WMDP	Weapons of Mass Destruction Program