U.S. Department of Justice

Federal Bureau of Investigation

FY 2022 President's Budget Request

May 2021

Table of Contents

I. OVERVIEW

A. Introduction

Budget Request Summary: The Federal Bureau of Investigation's (FBI's) Fiscal Year (FY) 2022 budget request proposes a total of $10,275,753,000 in direct budget authority, of which $10,213,858,000 is for Salaries and Expenses (S&E) and $61,895,000 is for Construction.

The S&E request includes a total of 36,149 direct positions and 34,619 direct full-time equivalents (FTE); the positions include:

- 13,414 Special Agents (SAs)
- 3,216 Intelligence Analysts (IAs)
- 19,519 Professional Staff (PS)

The S&E program increases total $150,730,000; 384 positions (139 SAs, 104 IAs, and 141 PS), and 193 FTE, for the following:

- $40,000,000 for Cyber investigative capabilities
- $45,000,000 to countering Domestic Terrorism
- $18,792,000 for Counterintelligence matters
- $25,500,000 for McGirt resources
- $6,208,000 for Task Force Officer (TFO) Body Worn Cameras (BWCs)
- $15,230,000 for Cybersecurity

The request includes $215,442,000 in technical adjustments and adjustments to base (ATBs) for continued support of the FBI's base resources.

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

- $10,000,000 in increases for safety and strategic improvements at Quantico

The FBI continues to strategically assess current and prospective operations to ensure it meets mission requirements at the lowest possible cost to the United States (U.S.) taxpayer. The FY 2022 budget request is a product of these assessments and provides the resources to aggressively carry the effective execution of the FBI's strategic vision into the future.

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

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

The FBI Vision: Ahead of the threat.

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

- Strategic Goal 1: Enhance national security and counter the threat of terrorism
- Strategic Goal 3: Reduce violent crime and promote public safety
- Strategic Goal 4: Promote rule of law, integrity, and good government

The FBI Strategy: To focus strategic efforts across the enterprise, the FBI has eight mission priorities and 13 enterprise objectives, organized by four guiding principles (people, partnerships, process, and innovation).

FBI Priorities:

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

Enterprise Objectives:

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

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

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

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

The FBI's branches and divisions align their strategies to the FBI Strategy, via the enterprise strategy process, by cascading selected enterprise objectives and executing strategic initiatives or measures within their branch or division's strategy. This vertical alignment within the

organization ensures the FBI enterprise is strategically focused on the same objectives and working collectively toward the FBI mission and vision. Strategy review meetings are held with the Director and each branch and division to discuss progress toward the enterprise objectives throughout the fiscal year, and FBI executives routinely evaluates the organization's progress.

The FBI tracks the execution of its mission priorities via national threat strategies across headquarters (HQ) operational and intelligence programs, field offices (FO), and legal attaché (legat) offices through the Integrated Program Management (IPM) and Threat Review and Prioritization (TRP) processes. These processes enable threat issues to be identified across the organization with accompanying threat strategies. Every two years, headquarters operational divisions prioritize national threats, determine FBI National Threat Priorities (NTPs), and develop national threat strategies and guidance for threat mitigation. The 56 field offices and 64 legat offices use this national guidance to formulate a field office and legat threat prioritization and complete strategies specific to their areas of responsibility. These threat and program strategies undergo mid-year and end-of-year evaluations, and the field and legat offices are held accountable to their performance targets. FBI executives and program managers hold regular meetings to review and evaluate field office and legat office effectiveness throughout the fiscal year.

The FBI's budget strategy and future resource requirements and requests are designed to enable the FBI to address the current range of threats while also focusing on the future needs of the FBI. An increasing number of the FBI's programs and initiatives are multi-year and require phased development, deployment, and operations or maintenance funding. This budget request is designed to promote capabilities and strategies agile enough to meet ongoing, emerging, and unknown national security, cyber, and criminal threats.

Organization of the FBI: The FBI operates FOs in 56 major U.S. cities and approximately 350 resident agencies (RAs) throughout the country. RAs are satellite offices, typically staffed with fewer than 20 people, that support the larger field offices and enable the FBI to maintain a

presence in and serve a greater number of communities. FBI employees assigned to FOs and RAs perform most of the investigative and intelligence work for the FBI. Special Agents in Charge (SACs) and Assistant Directors in Charge (ADICs) of FBI field offices report directly to the Director and Deputy Director.

The FBI also operates 63 legat offices and 29 sub-offices in more than 70 countries around the world. These offices are typically staffed with fewer than 10 people who enable the FBI's presence in these countries and liaise with foreign counterparts and partners. These numbers fluctuate based on the global threat environment.

FBI Headquarters, located in Washington, D.C., provides centralized operational, policy, and administrative support to FBI investigations and programs. Under the direction of the FBI Director and Deputy Director, this support is provided by:

- The National Security Branch (NSB), which includes the Counterterrorism Division (CTD), the Counterintelligence Division (CD), and the Weapons of Mass Destruction Directorate (WMDD).
- The Intelligence Branch (IB), which includes the Directorate of Intelligence (DI), the Office of Partner Engagement (OPE), and the Office of Private Sector (OPS).
- The Criminal, Cyber, Response, and Services Branch (CCRSB), which includes the Criminal Investigative Division (CID), the Cyber Division (CyD), the Critical Incident Response Group (CIRG), the International Operations Division (IOD), and the Victim Services Division (VSD).
- The Science and Technology Branch (STB), which includes the Criminal Justice Information Services (CJIS) Division, the Laboratory Division (LD), and the Operational Technology Division (OTD).

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

- The Information and Technology Branch (ITB) oversees the IT Enterprise Services Division (ITESD), the IT Applications and Data Division (ITADD), and the IT Infrastructure Division (ITID).
- The Human Resources Branch (HRB) includes the Human Resources Division (HRD), the Training Division (TD), and the Security Division (SecD).
- Administrative and financial management support is provided by the Finance and Facilities Division (FFD), the Information Management Division (IMD), the Resource Planning Office (RPO), and the Inspection Division (INSD).
- Specialized support is provided directly to the Director and Deputy Director through a number of staff offices, including the Insider Threat Office (InTO), the Office of the Chief Information Officer (OCIO), the Office of Public Affairs (OPA), the Office of Congressional Affairs (OCA), the Office of the General Counsel (OGC), the Office of Equal Employment Opportunity Affairs (OEEOA), the Office of the Ombudsman, the Office of Professional Responsibility (OPR), the Office of the Ombudsman, and the Office of Integrity and Compliance (OIC).

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

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

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

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

- Based on workload: Critical investigative enablers, such as LD, IOD, and 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 ITB, FFD, and 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 U.S. and its Interests

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

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

Domestic terrorists who are motivated by a range of ideologies and galvanized by recent political and societal events in the United States pose an elevated threat to the Homeland in 2022. Enduring DT motivations pertaining to biases against minority populations and perceived government overreach will almost certainly continue to drive DT radicalization and mobilization to violence. Newer sociopolitical developments—such as narratives of fraud in the recent general election, the emboldening impact of the violent breach of the US Capitol, conditions related to the COVID-19 pandemic, and conspiracy theories promoting violence—will almost certainly spur some domestic terrorists to try to engage in violence this year.

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

Several factors could increase the likelihood or lethality of DT attacks in 2022 and beyond, including escalating support from persons in the United States or abroad, growing perceptions of government overreach related to legal or policy changes and disruptions, and high-profile attacks spurring follow-on attacks and innovations in targeting and attack tactics.

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

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

The conflicts in Syria and Iraq have served as the most attractive overseas theaters for Western extremists who want to engage in violence. More than 35,000 people from approximately 120 countries have traveled to join the fighting in Syria and Iraq, the large majority of which traveled to join ISIS. ISIS and other terrorist organizations in the region have used these travelers to facilitate terrorist activity beyond Iraq and Syria, particularly in their home countries, because returning foreign fighters can radicalize members of the communities that they originally came from.

ISIS has aggressively promoted its hateful message – attracting like-minded extremists, including Westerners – and has persistently used the Internet to communicate. ISIS blends traditional media platforms, glossy photos, in-depth articles, and social media campaigns that can go viral in a matter of seconds. No matter the format, the message of radicalization now spreads faster than thought possible just a few years ago through all forms of technology.

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

As a communication medium, social media is a critical tool exploited by terror groups. One recent example includes an individual arrested for providing material support to ISIS by

facilitating an associate's travel to Syria to join ISIS. The arrested individual had multiple connections via a social networking site with other like-minded individuals.

HVEs aspire to carry out attacks in the U.S. or travel overseas to participate in terrorist activity. Countering the HVE threat is especially challenging for law enforcement (LE) because HVEs often act with little to no warning. The FBI has HVE cases that span all 56 FBI field offices across all 50 states.

Foreign Intelligence: The foreign intelligence threat to the U.S. continues to increase as foreign powers seek to establish economic, military, and political preeminence and to position themselves to compete with the U.S. in economic and diplomatic arenas. The most desirable U.S. targets are political and military plans, technology, and economic institutions, both governmental and non-governmental. Foreign intelligence services continue to target and recruit U.S. travelers abroad to acquire intelligence and information. Foreign adversaries are increasingly employing non-traditional collectors – for example, students and visiting scientists, scholars, and business executives – as well as cyber-based tools to target, penetrate, and influence U.S. institutions.

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

Cyber: The U.S. faces increasingly sophisticated cyber operations that succeed by undermining trust in the things Americans rely on, such as software updates, medical research, school networks, and emergency services. By infiltrating and impersonating those trusted parties, both criminals and a growing number of nation-states are undermining the credibility, integrity, and availability of information and networks, with serious consequences for both national security and public safety.

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

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

As part of this strategy, and consistent with recommendations from the U.S. Cyberspace Solarium Commission, the FBI 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, led by senior executives from partner agencies, integrate operations and intelligence across agency lines to sequence actions for maximum impact against cyber adversaries.

The coordinated disruption of the infrastructure of a highly destructive malware known as Emotet is a successful example of these joint operations. In January 2021, the FBI applied lessons learned from past disruptions and led an unprecedented number of international partners in disabling multiple layers of the malware's infrastructure, making it more difficult for the actors to reconstitute. This operation leveraged the FBI's sophisticated techniques, unique authorities, and worldwide partnerships to disrupt malware that had infected over a million computers and caused millions of dollars in damage worldwide.

***White Collar Crime*:** The White-Collar Crime (WCC) program addresses public corruption, border corruption, corporate fraud, securities/commodities fraud, mortgage fraud and other financial institution fraud, health care fraud, other complex financial crimes (insurance, bankruptcy, and mass marketing fraud), and intellectual property rights.

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

The FBI's Public Corruption program also focuses on border corruption. The documented presence of corrupt border officials facilitates a wide range of illegal activities along both the northern and southern borders. Resource-rich cartels and criminal enterprises employ a variety of methods to target and recruit U.S. Border Patrol agents, Customs and Border Protection officers, and local police officers who can use their positions to assist with criminal activity. Corrupt officials assist these entities by providing intelligence and help move contraband across the borders. To help address this threat, the FBI established the National Border Corruption Task Force Initiative, which has developed a threat-tiered methodology targeting border corruption at all land, air, and seaports to mitigate the threat posed to national security.

The FBI has investigated election-related crimes, which are also covered under the Public Corruption program, for over three decades. These frauds and schemes run the gamut and can have a devastating effect on elections, as well as the public's faith in our electoral process. Election crimes include ballot fraud, election or polling place abuses, false voter registration,

violations of campaign finance laws, and bribes of public officials. Similarly, the FBI investigates voter intimidation and suppression, which can be deemed civil rights violations and investigated under the FBI's Civil Rights program (explained further in the "Civil Rights" portion of this document). The FBI is focused on preventing and stopping these crimes and has election crimes coordinators in all 56 FOs, who regularly receive specialized training on election crimes and voter fraud. The FBI is committed to uncovering and investigating money laundering facilitators (MLF) and organizations who mask the source of criminally-derived proceeds so the proceeds appear legitimate or promote illegal conduct. These facilitators and organizations may also mask the source of assets used to promote illegal conduct. Money laundering generally involves three steps: (1) placing illicit proceeds, which often includes virtual assets and currencies, into legitimate financial systems; (2) layering, or the separation of the criminal proceeds from their origin; and (3) integration, or the use of apparently legitimate transactions to disguise the illicit proceeds. Once criminal funds have entered legitimate financial systems, the layering and integration phases make it difficult to trace the proceeds. The FBI combats these illicit activities by working with the financial industry, private sector, and LE partners to identify asset sources, flows, and launderers. Specifically, the FBI targets professional money laundering gatekeepers and controllers, such as attorneys and financial institutions, since addressing these enablers has a larger disruption and dismantlement effect on criminal activities than focusing exclusively on the underlying unlawful activity.

The FBI also identifies and pursues investigations against the most egregious offenders involved in health care fraud and abuse, including criminal enterprises and other crime groups, corporations, companies, and providers whose schemes affect public safety. Besides federal health benefit programs such as Medicare and Medicaid, private insurance programs also lose billions of dollars each year to fraud schemes in every sector of the industry. The FBI actively investigates crimes targeting and disproportionately affecting senior citizens, in support of the Elder Abuse Prevention and Prosecution Act. Many of these crimes are linked to health care but can include a host of other scams. To counter these threats, the FBI is actively engaged with LE partners to build Health Care Fraud Task Forces in FOs throughout the U.S.

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

To enforce intellectual property rights, the FBI disrupts and dismantles international and domestic criminal organizations that manufacture or traffic in counterfeit and pirated goods and/or steal, distribute, or otherwise profit from the theft of intellectual property and trade secrets. The FBI works to combat these types of crimes by collaborating with the public and

private sectors, to include third-party entities like online marketplaces, payment service providers, and advertisers to obtain intelligence, gather leads, and identify and disrupt criminal activities.

As the COVID-19 pandemic spread across the U.S. and public and private relief funds became available for potential exploitation, the FBI has also observed schemes related to investment fraud, identity theft, healthcare, financial institution related fraud, unemployment insurance fraud, intellectual property, fraud against the government, and hoarding/price gouging. The FBI is responsible for investigating most of the Coronavirus Aid, Relief, and Economic Security (CARES) Act fraud and formed a Paycheck Protection Program (PPP) Fraud Working Group in coordination with the DOJ's Fraud Section and the Small Business Administration Office of Inspector General to ensure the FBI stays abreast of the latest fraud intelligence and trends, shares information, deconflicts, and establishes operational plans. Furthermore, the FBI also serves on an unemployment insurance fraud multi-agency working group, has published several Public Service Announcements, and works closely with federal and state partners to address and mitigate CARES Act and COVID-19-related threats.

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

Some of the most sophisticated TCOs increasingly rely upon encrypted, hardened device platforms. These platforms provide a secure communications network for TCOs to conduct criminal activity through highly modified mobile devices, rendering traditional collection methods (e.g., wiretaps) obsolete. These devices use private messaging apps to send text and picture messages to other trusted users, often without the ability to make voice phone calls. The devices also contain other security mechanisms, such as remote data destruction or "burn" features, which allow phone data to be erased remotely by the user. Often, these devices can operate via Wi-Fi signal, rather than cellular networks. Features such as the camera, microphone and GPS are often disabled for added security. To address TCO use of encrypted, hardened device platforms, the FBI established the Mobile Encrypted Networks and Communications Exploitation (MENACE) initiative. The mission of MENACE is to enhance investigations and coordinate intelligence, technology, and operations to drive the migration of criminal actors to encrypted platforms in which the FBI has exploitation capabilities. The FBI's CID is working closely with OTD to develop unclassified tools and techniques to exploit these encrypted communication platforms.

Preventing and combatting transnational organized crime (TOC) demands a concentrated effort by the FBI and federal, state, local, tribal, and international partners. In FY 2020, the FBI led

over 100 organized crime and major theft task forces, targeting TCO networks based in the Eastern and Western Hemispheres. The FBI has also focused on improving and expanding domestic and international partnerships and optimizing intelligence and operations collaboration through assistant legats and overseas vetted teams or task forces to support efforts against transnational criminal organizations abroad.

Illicit drug trafficking continues to be a growing threat. Large amounts of high-quality, low-cost heroin and illicit fentanyl are contributing to record numbers of overdose deaths and life-threatening addictions nationwide. The accessibility and convenience of the online drug trade contributes to the opioid epidemic in the U.S. TCOs introduce synthetic opioids to the country's market, including fentanyl and fentanyl analogues. The FBI has established a multi-faceted operational plan to address this evolving threat.

For example, in January 2018, DOJ's Office of the Deputy Attorney General directed the FBI and other federal LE partners to develop a strategic plan to disrupt and dismantle marketplaces facilitating fentanyl and opioid distribution. In response to the directive, the FBI established the Joint Criminal Opioid Darknet Enforcement (JCODE) Initiative, which brings together agents, analysts, and professional staff with expertise in drugs, gangs, health care fraud, and more, with federal, state, and local LE partners from across the USG. JCODE utilizes a whole of government approach by co-locating eleven federal agencies in a task force environment to leverage technical resources and capabilities to target the largest Darknet marketplaces and vendors. JCODE maintains a comprehensive, multi-pronged criminal enterprise strategy to target fentanyl and opioid trafficking on Darknet and Clearnet. This strategy focuses on identifying and infiltrating the marketplace administrative team, analyzing financial information, identifying and exploiting marketplace infrastructure, targeting vendors and buyers, and enabling the investigation and prosecution of these marketplaces. Additionally, JCODE has provided Darknet and cryptocurrency training to over 1,000 domestic and international LE agents and analysts. FBI offices across the country are replicating JCODE's framework and building JCODE operational teams, comprised of multi-agency partners and support investigations developed by JCODE. As a direct result of JCODE efforts, the FBI alone has opened hundreds of new investigations.

JCODE also collaborates extensively with international LE partners to include the European Union Agency for Law Enforcement (EUROPOL) to address the borderless Darknet environment. The subsequent global efforts of JCODE, to include Operation SaboTor (2019) and Operation DisrupTor (2020), respectively, resulted in the arrest of 230 Darknet criminal actors. Seizures included more than $13.5 million in cryptocurrency, cash, gold, over 150 firearms, and over 800 kilograms of opioids and other drugs in nine countries, including the U.S.

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

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

The FBI has dedicated specific resources to combat the threat of violence posed by MS-13. The atypical nature of this gang has required a multi-pronged approach, leveraging U.S. task forces, while simultaneously gathering intelligence and aiding international LE partners through the FBI's Transnational Anti-Gang Task Forces (TAGs). Initially established in El Salvador in 2007, there are now TAGs in El Salvador, Guatemala, and Honduras. Each TAG is a fully operational unit responsible for investigating MS-13 operating in the Northern Triangle of Central America and threatening the U.S. This program has achieved numerous successes by combining the expertise, resources, and jurisdiction of participating agencies involved in investigating and countering transnational criminal gang activity.

Crimes Against Children and Human Trafficking: The FBI has several programs to target child predators and recover missing and endangered children, including the Child Abduction Rapid Deployment (CARD) Team, the Child Sex Tourism (CST) Initiative, the Innocence Lost National Initiative (ILNI), the Innocent Images National Initiative (IINI), 85 Child Exploitation and Human Trafficking Task Forces, and 69 international violent crimes against children task force officers. The FBI has nationwide capacity to:

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

In 2005, the FBI created the CARD Team to provide a nationwide resource to support investigations of child abductions and critically missing children. CARD is composed of agents and intelligence analysts who provide investigative and technical resources to LE agencies following a child abduction. CARD members attend specialized training on child abduction investigative search techniques and technology and develop best practices through operational experience. CARD is supported by the FBI's Behavioral Analysis Unit, which assists with offender characteristics, victimology, and investigative interview and media strategies. CARD is a nationwide resource to LE at no cost to the requesting agency. The CARD priority is to provide

timely response to recover abducted children and arrest abductors. Deployed 181 times since its inception, CARD has aided in rescuing 88 live children, as well as arresting numerous offenders.

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

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

Indian Country (IC) Crimes: Due to jurisdictional issues and the remote nature of many reservations, the FBI is the primary LE entity in IC. The Bureau of Indian Affairs has a limited number of investigators, and they are not present on every reservation. Additionally, tribal authorities can generally only prosecute misdemeanor violations involving native subjects, and state and local LE generally do not have jurisdiction within reservation boundaries. In FY 2020, there were 935 arrests; 882 indictments, informations and/or complaints; and 545 convictions in IC.

The IC and Special Jurisdiction Unit (ICSJU) has developed and implemented strategies to address the most egregious crime problems in IC, pursuant to the FBI's jurisdiction. These matters generally focus on death investigations, child sexual assault and physical abuse, assault resulting in serious bodily injury, gang/criminal enterprise investigations, and financial crimes. ICSJU supports joint investigative efforts with the Bureau of Indian Affairs and tribal LE agencies and manages and conducts essential investigative training for 24 Safe Trails Task Forces, as well as approximately 150 FBI agents and LE partners focused on IC crimes. Although IC cases are generally reactive, many are cross-programmatic in nature, including Indian gaming, public corruption, and complex financial fraud.

On July 9, 2020, the Supreme Court's ruling in *McGirt v. Oklahoma* determined the territorial boundaries of the Muscogee Creek Nation (MCN) fall under federal IC jurisdiction, effectively making the FBI the responsible LE agency under the MCA for offenses committed by or victimizing a tribal member. The territorial boundaries of the MCN now under FBI jurisdiction encompass most of the city of Tulsa and approximately one million residents, including approximately 60,000 MCN tribal members.

The principles of the McGirt decision also apply to the status of the Cherokee, Chickasaw, Choctaw and Seminole tribal territories. The Cherokee and Chickasaw reservations were reaffirmed as falling under federal jurisdiction on March 11, 2021 and the Choctaw and Seminole reservations were reaffirmed on April 1, 2021. Combined, all five reservation territories encompass approximately 32,000 square miles, or 45 percent of the state of Oklahoma.

The total population within the combined borders is roughly 1.9 million, of which approximately 420,000 are enrolled tribal members.

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

A hate crime is a traditional criminal offense, such as murder, arson, or vandalism, motivated wholly or in part by an offender's bias against a victim's actual or perceived race, religion, national origin, disability, gender, gender identity, or sexual orientation. Investigating hate crimes is the leading priority of the FBI's Civil Rights Program, due to the devastating physical, emotional, and psychological toll these crimes take on individuals, families, and communities. Through training, public outreach, LE support, and investigations, the FBI takes a multi-faceted approach to detect, deter, and investigate hate crimes.

Preventing abuses of those acting with government: COL violations are actions taken by any person using the authority necessary to protect the health of American democracy. It is a federal crime for anyone acting under "color of law" to willfully deprive or conspire to deprive a person of a right protected by the Constitution or U.S. laws. COL applies to LE officers, as well as any public official or person conspiring with a public official operating with power given by a governmental agency, such as prosecutors, judges, or correctional officers. The FBI has investigative responsibility for federal COL matters involving local and state LE and concurrent responsibility with the Office of Inspectors General for other federal agencies. To mitigate these types of crimes, the FBI focuses on training and educating state, local, and federal partners as to COL statutes and elements of the crime to promote constitutional policing and the FBI's investigative process to promote cooperation.

Under the FACE Act, it is a federal crime for a person to use force, threat of force, or physical obstruction to intentionally injure, intimidate, or interfere with a person (or attempt to do so) because the person is or has been obtaining or providing reproductive health care services. It is also unlawful for a person to intentionally damage or destroy the property of a facility because it provides reproductive health services. It is also illegal to use force, threat of force, or physical obstruction to intentionally injure, intimidate, or interfere with a person (or attempt to do so) seeking to exercise their religious freedom a place of worship. The number of FACE Act violations remains relatively low, with occasional spikes during dates marking significant events in the pro-choice and pro-life movement. Regardless, the FBI prioritizes investigating these crimes, and the Civil Rights program works in conjunction with its domestic terrorism (DT) counterparts to do so.

The Civil Rights program also investigates voter suppression, as it is a civil rights violation to unlawfully deter voters from voting or to unduly influence them 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.

The FBI's International Human Rights (IHR) program employs investigative expertise, techniques, and legal authorities to identify, locate, investigate, and prosecute perpetrators of serious human rights or humanitarian law violations. These violations include genocide, torture, war crimes, recruitment or use of child soldiers, female genital mutilation, and providing material support to serious human rights offenses. The goal of the IHR program is to hold perpetrators of mass atrocities and serious human rights violators accountable to the rule of law in a U.S. or foreign country's judicial system and to prevent the U.S. from serving as a "safe haven" to those human rights violators. The International Human Rights Unit (IHRU) conducts this mission in close collaboration with the DOJ's Human Rights and Special Prosecutions Section, Immigration and Customs Enforcement/Homeland Security Investigations at the Human Rights Violators and War Crimes Center (HRVWCC), the Department of State Office of Global Criminal Justice, and the USIC.

Additionally, the IHR program seeks to increase the FBI's intelligence collection on human rights violations with a nexus to the U.S. perpetrated throughout the world. This leads to additional international human rights investigations, expands and strengthens the public's understanding of the FBI's mission in addressing human rights violations, and enhances the FBI's preventative response to human rights violators entering the U.S. through IHRU's partnership with the HRVWCC.

C. Intelligence-Driven Operations

The FBI's IB serves as the strategic leader of the FBI's intelligence program, driving the integration of intelligence and operations, and proactively engaging in information sharing with partners in federal, state, and local LE, the U.S. intelligence and private sector communities, as well as international partnerships. The IB oversees the intelligence program implementation of its six areas of focus: Workforce success, culture and mindset, technology capabilities, information sharing, collection, and exploitation and analysis.

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

The IB EAD heads the FBI intelligence program, ensuring the national security and LE intelligence functions of collection, targeting, domain, and threat analysis, and corresponding intelligence production, are consistent with national priorities and adhere to tradecraft standards, policies, and processes. The EAD is the primary point of contact (POC) 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, serves as Executive Agent for the National Virtual Translation Center (NVTC), and is responsible for the FBI's foreign language program (FLP).

The FBI uses intelligence to understand criminal and national security threats and to conduct operations to dismantle or disrupt those threats with the following methods:

- The FBI uses a standardized model for field intelligence that can adapt to the size and complexity of small, medium, and large offices. There are 56 intelligence programs, with one in each FBI FO.
- Fusion cells are intelligence teams in operational divisions designed to integrate all aspects of the intelligence cycle for a unique threat. Fusion cells integrate intelligence and operations and collaborate across work roles to ensure intelligence drives and supports operations. Fusion cells consist of intelligence analysts who perform the targeting, collection, domain, and threat analysis intelligence functions, primarily at the strategic, or national level. The structure and process of the fusion cells are designed to streamline intelligence support and more directly collaborate with operational personnel.

II. SUMMARY OF PROGRAM CHANGES

Item Name	Description	Pos.	FTE	Dollars ($000)	Page
Salaries and Expenses Enhancements					
Countering Domestic Terrorism	With the requested resources, the FBI will be able to better address national security threats by detecting and disrupting domestic terrorism activities, increasing information sharing with LE partners, and expanding the capacity to handle incoming tips from the public.	179	90	$45,000	5-1
McGirt Resources	The requested resources will allow the FBI to effectively address the increased operational need in the state of Oklahoma following the Supreme Court decision on *McGirt v. Oklahoma* while Federal, State, and tribal authorities work on longer term solutions. This ruling significantly expanded federal jurisdiction for crimes committed on tribal lands. Specifically, the requested resources will be used to enhance the FBI's capacity to address the increased investigations now falling under FBI jurisdiction.	0	0	$25,500	5-8
Cyber	The requested resources will increase the FBI's capacity for unilateral, joint, and enabled operations with other federal, state, local and international partners. The request focuses on the development of three critical areas: Cyber threat identification, analysis, and attribution; synchronized interagency operations; and cyber workforce development.	155	78	$40,000	5-12

Counterintelligence	This request is classified.	28	14	$18,792	5-18
Task Force Officer Body Worn Camera	With the requested resource, FBI will be able to provide software and video storage to store data and video from the body worn cameras (BWCs) of Federally deputized Task Force Officers (TFOs). This funding will allow the FBI to support storage of BWC video for TFOs whose parent agency mandates the use of BWCs while they serve on Federal task forces.	0	0	$6,208	5-19
Cybersecurity	The requested funding will allow the FBI to increase its cybersecurity posture and enable the FBI to proactively address cybersecurity vulnerabilities and the growing cyber threats posed by internal and external threats.	22	11	$15,230	5-23
Total, Salaries and Expenses Enhancements		**384**	**193**	**$150,730**	
Construction Enhancements					
Safety and Strategic Improvements to the Quantico Campus	This request supports the replacement of critical operational support facilities that will increase the safety of students, employees and visitors on the FBI's Quantico Campus.	0	0	$10,000	7-5
Total, Construction Enhancements		**0**	**0**	**$10,000**	

III. APPROPRIATIONS LANGUAGE AND ANALYSIS OF APPROPRIATIONS LANGUAGE

Appropriations Language for Salaries and Expenses

For necessary expenses of the Federal Bureau of Investigation for detection, investigation, and prosecution of crimes against the United States, $10,213,858,000 of which not to exceed $216,900,000 shall remain available until expended: Provided, that not to exceed $284,000 shall be available for official reception and representation expenses.

Analysis of Appropriations Language

No substantive change.

IV. PROGRAM ACTIVITY JUSTIFICATION

A. Intelligence Decision Unit

Intelligence Decision Unit Total	Direct Pos.	Estimate FTE	Amount ($000)
2020 Enacted	6,679	6,378	$1,764,562
2021 Enacted	6,644	6,316	$1,817,342
Adjustments to Base and Technical Adjustments	0	(86)	$66,993
2022 Current Services	6,644	6,230	$1,884,335
2022 Program Increases	113	57	$16,219
2022 Request	6,757	6,287	$1,900,554
Total Change 2021-2022	**113**	**(29)**	**$83,212**

1. Program Description

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

Intelligence Branch

As the leader of the FBI's intelligence program, IB drives collaboration to achieve the full integration of intelligence and operations throughout the FBI. The branch has centralized authority and responsibility for all FBI intelligence strategy, resources, policy, and functions for actively engaging with the FBI's partners across the intelligence, LE, and private sector communities. The FBI's Intelligence Program Strategy guides IB direction and oversight of all aspects of the FBI's intelligence work.

The SIIG provides FBI leaders with a consolidated, integrated perspective on threats while helping to integrate and balance the FBI's priorities with those of the broader USIC and USG. Led by a Deputy Assistant Director, the SIIG is made up of Senior National Intelligence Officers with subject-matter expertise on geographic and functional programs who help integrate the FBI's understanding of priority threat issues. The SIIG also houses the Bureau Control Office, which manages the FBI's sensitive compartmented information program.

Directorate of Intelligence

DI is the FBI's dedicated national intelligence workforce, with clear authority and responsibility for all FBI intelligence functions. DI's mission is to provide strategic support, direction, and oversight to the FBI's intelligence program, and its vision is to drive the complete integration of

intelligence and operations within the FBI. DI carries out these functions through embedded intelligence elements at HQ and in each FO.

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

The FBI's IA cadre performs the following functions:

- Understanding emerging threat streams to enhance domain knowledge and exploit collection opportunities;
- Enhancing collection capabilities through the deployment of collection strategies;
- Reporting raw intelligence in a timely manner;
- Identifying human and technical source collection opportunities;
- Performing domain analysis in the field to articulate the existence of a threat in a FO area of responsibility;
- Performing strategic analysis at HQ to ascertain the ability to collect against a national threat;
- Serving as a bridge between intelligence and operations;
- Performing confidential human source validation; and,
- Recommending collection exploitation opportunities at all levels.

The products generated by intelligence analysis ensure FBI investigative and operational strategies are based on an enterprise-wide understanding of the current and future threat environments. FBI intelligence products also serve to inform the FBI's partners about ongoing and emerging threats.

Foreign Language Program
The FLP provides quality language solutions, analysis, and cultural expertise to the FBI and its partners. The FBI's success at protecting the U.S. from future terrorist attacks, countering foreign intelligence operations and espionage, and dismantling transnational criminal enterprises is increasingly dependent upon maximizing the use and deployment of its linguist workforce, language tools, and technology. The FBI workforce has qualified capabilities in 142 languages and dialects, spanning approximately 100 FBI domestic and overseas locations. The FLP promulgates policies and compliance requirements to ensure integrity of intelligence products. Additionally, the FLP develops the foreign language skills of the FBI employees through ongoing language testing, assessments, and multi-tiered training strategies designed to build and sustain a high performing intelligence workforce.

Language Analysis
Nearly every major FBI investigation has a foreign language component, and the demand for highly qualified linguists and foreign language and culture training continues to increase. Language Analysts and English Monitoring Analysts are a critical component of the FBI's effort

to acquire and accurately process real-time, actionable intelligence to detect and prevent terrorist attacks against the nation. The FBI's Language Analysts address the highest priority foreign language collection and processing requirements in the FBI's counterterrorism, cyber, counterintelligence, and criminal investigative missions.

National Virtual Translation Center

The NVTC provides timely and accurate translation services to support national intelligence priorities and protect the nation and its interests. NVTC was established under Section 907 of the USA Patriot Act (2001) and designated a USIC service of common concern in 2014. Since its inception, NVTC has complemented USIC elements' foreign language translation capabilities by supporting tasks ranging from high-volume surges to immediate translation requirements in 142 languages and dialects. NVTC operates within a virtual model that connects NVTC program staff, translators, field offices, and customers globally via a common web-based workflow management system.

Intelligence Training

Ensuring the FBI's intelligence workforce is prepared with the necessary specialized skills and expertise is crucial to the FBI's ability to successfully fulfill its mission. The FBI's extensive intelligence training program leverages expertise within the organization and its partners in the intelligence and academic communities and private industry to ensure the best educational opportunities are available to the FBI's workforce. The FBI's training program identifies and coordinates the certification of adjunct faculty, communicates educational and developmental opportunities outside the FBI, and facilitates opportunities for research related to intelligence analysis. Moreover, the FBI uses an integrated approach to training bringing employees together at the beginning of their careers to help them understand the importance and impact of an integrated intelligence and operational methodology – a model that continues across the FBI's intermediate and advanced courses of instruction.

Office of Partner Engagement

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

Office of Private Sector

The primary mission of OPS is to protect the nation's economy and national security by strengthening the FBI's relationships with the U.S. private sector partners. OPS builds, supports, facilitates, and enhances strategic relationships between the FBI, private industry, and academia. OPS also develops tools to support those relationships, and facilitates information sharing, while maintaining an enterprise focus of the FBI's engagement efforts. OPS enhances understanding of

the private sector, to include academia and associations, increasing collaboration and information-sharing to mitigate risk and remain ahead of the threat. OPS works toward the following objectives: Facilitating one "FBI voice" by providing a consistent contact for the private sector; focusing on meaningful dialogue with private sector partners to build trust between the FBI and the private sector; and assisting companies whose innovative technologies may be targeted. OPS focusses on engaging the private sector on priorities including insider threat, emerging technologies, foreign influence, and lawful access. In addition to its main office at FBI HQ, OPS is represented in each FBI FO by at least one Private Sector Coordinator (PSC) to develop and maintain private sector partnerships in each FO's Area of Responsibility (AOR). OPS also manages two private sector information-sharing programs: The Domestic Security Alliance Council (DSAC) and InfraGard, promoting effective information exchanges through public-private partnerships.

Foreign Terrorist Tracking Task Force

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

Terrorist Screening Center

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

Infrastructure and Technology

The FBI's information technology infrastructure and technology help to manage, process, share, and protect classified and unclassified information critical to national security. Taken together, these efforts form a comprehensive system of security and efficiency. The classified part of the comprehensive system includes secure workspaces, or SCIFs, and a secure information sharing capability through the SCINet. It also includes the FBI enterprise network for processing, transmitting, storing, and sharing information at the Top Secret (TS)/Sensitive Compartmented Information (SCI) level, enabling FBI analysts to connect with the IC through a connection to the Joint Worldwide Intelligence Communication System (JWICS) and use powerful applications to extract and analyze intelligence data in an efficient and timely manner.

The unclassified part of the comprehensive system includes the FBI's ability to share unclassified information with other federal, state, and local governments and other partners through the CJIS' Law Enforcement Enterprise Portal (LEEP) system and its Unclassified Network (UNet), the FBI's unclassified network which includes connection to the public internet.

Secure Work Environment

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

2. Performance and Resource Tables

PERFORMANCE AND RESOURCES TABLE										
Decision Unit: Intelligence										
RESOURCES	**Target**		**Actual**		**Enacted**		**Changes**		**Requested (Total)**	
	FY 2020		**FY 2020**		**FY 2021**		**Current Services Adjustments & FY 2022 Program Changes**		**FY 2022 Request**	
	FTE	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
Total Costs and FTE	6,378	$1,764,562	6,275	$1,792,562	6,316	$1,817,342	(29)	$83,212	6,287	$1,900,554

Strategy Performance		FY17		FY18		FY19		FY20		FY21	FY22
		Target	Actual	Target	Actual	Target	Actual	Target	Actual	Target	Target
Measure (DOJ Objective 1.1)	Median velocity of Confidential Human Source (CHS)-derived Intelligence Information Reports (IIRs)	25 days or less	21.6	25 days or less	23.7	25 days or less	22.4	25 days or less	23	20 days or less	20 days or less
Measure (DOJ Objective 1.1)	Percent of FBI Intelligence Information Reports (IIRs) used in the development of United States Intelligence Community (USIC) Intelligence Products	12%	9%	12%	12%	12%	15%	15%	16%	15%	15%
Measure (DOJ Objective 1.1)	Percent of FBI Intelligence Information Reports (IIRs) citing National Intelligence Priorities Framework (NIPF) Priority 1 & 2 Requirements	80%	82%	80%	84%	80%	82%	80%	74%	80%	80%
Measure (DOJ Objective 1.1)	Number of Intelligence Training Courses Offered to State, Local, Territorial, and Tribal (SLTT) Partners	N/A	N/A	10	12	15	15	20	2	30	40
Measure (DOJ Objective 1.1)	Percent of net analyst-edits rejected by National Counterterrorism Center (NCTC) for inaccuracy	9%	3.1%	7%	.25%	7%	1.4%	5%	0.9%	5%	5%
Measure (DOJ Objective 1.1)	Percent of Terrorist Screening Data Base (TSDB) addition and deletion nominations processed within 24 hours of receipt	90%	99%	95%	99%	95%	99%	97%	99.6%	97%	98%

3. Resources and Strategies

Directorate of Intelligence

a. Performance Plan and Report for Outcomes

DI's vision is to "create a more secure nation through an integrated, agile, and innovative Intelligence Program that drives the FBI's ability to address current and emerging threats." All three performance measures identified for reporting in FY 2022 directly support this vision statement and will demonstrate work towards DI's vision. The performance measures ensure a drive for high quality intelligence while also mitigating risk. As the premier producer of valuable and actionable intelligence, DI will drive the complete integration of Intelligence and Operations through improving its collection and dissemination of intelligence that enables the FBI to identify and mitigate current and emerging threats.

Performance Measure: Median velocity of CHS-derived IIRs

FY19 Target: 25 days or less
FY19 Actual: 22.4 days
FY20 Target: 25 days or less
FY20 Actual: 23 Days
FY21 Target: 20 days or less
FY22 Target: 20 days or less

Performance Measure: Percentage of FBI IIRs used in the development of USIC Intelligence Products

FY19 Target: 12%
FY19 Actual: 15%
FY20 Target: 15%
FY20 Actual: 16%
FY21 Target: 15%
FY22 Target: 15%

Performance Measure: Percentage of FBI IIRs citing NIPF Priority 1 & 2 Requirements

FY19 Target: 80%
FY19 Actual: 82%
FY20 Target: 80%
FY20 Actual: 74%
FY21 Target: 80%
FY22 Target: 80%

Discussion

Median velocity of CHS-derived IIRs: The intent of this measure is to assess the speed with which FBI IIRs are disseminated to LE and USIC partners from the day of acquisition of information.

Percentage of FBI IIRs used in the development of USIC intelligence products: The intent of this measure is to assess the level of the USIC's usage of FBI IIRs in the development of USIC intelligence products.

Percentage of FBI IIRs citing NIPF Priority 1 & 2 requirements: The intent of this measure is to demonstrate the correlation between FBI's Priority Threats and USIC intelligence requirements.

FBI tagging to National Intelligence Priorities Framework (NIPF) priority 1 and 2 decreased 45% from Q1. IIR production decreased almost 20% from Q1. This measure fell under the performance target by six percentage points in FY20. The factors associated with COVID-19 pandemic may have contributed to this decline.

b. Strategies to Accomplish Outcomes

DI supports IB's Intelligence Program Five-Year Strategy, which outlines the strategic direction for moving forward in an ever-changing threat environment. The mission statement is to "provide insightful, timely, and actionable intelligence and support to uphold the Constitution and protect the American people." The vision statement is to "create a more secure nation through an integrated, agile and innovative Intelligence Program that drives the FBI's ability to address current and emerging threats." These performance measures identified for FY 2022 directly support the Intelligence Program Strategy and DOJ's Strategic Objective 1.1 by emphasizing the importance of incorporating intelligence in all that we do and the importance of building and maintaining partnerships with LE and USIC partners to identify and mitigate threats, including the FBI's mission priority: protect the U.S. from terrorist attack.

Office of Partner Engagement

a. Performance Plan and Report for Outcomes

OPE currently offers three intelligence training courses for Fusion Center and state and local LE partners, to include Intelligence for Supervisors (IntelSup), Analytic Writing for Fusion Centers (AWFC), and Introduction to Intelligence (IntroTel). These courses provide immediate and ongoing support to the integration of intelligence into traditionally operational units, teams, and departments. OPE will develop three additional Intelligence Leadership courses in conjunction with the training division to offer leadership training for Intelligence Commanders in the Field and within OPE's cadre of state and local LE partners agencies.

Operations supported by actionable, relative intelligence helps the FBI and its state and local LE partners mitigate both current and future threats, thus enhancing national security and protecting the U.S. domestic terrorism, mass casualty attacks, and other significant crimes against the American people. OPE's ability to continually meet the demand for these intelligence training courses for LE partners will be directly influenced by budget allocations and any necessary enhancements, if and when supported by DOJ.

Performance Measure: Number of Intelligence Training Courses Offered to SLTT Partners

FY19 Target: 15
FY19 Actual: 15
FY20 Target: 20
FY20 Actual: 2
FY21 Target: 30
FY22 Target: 40

Discussion
OPE manages the intelligence training for Fusion Center personnel and SLTT LE partner agency Intel Commanders. The training is a set of intelligence-centric courses, designed by OPE, to educate LE intelligence commanders and personnel on a common set of practices and production methods in writing, producing, and disseminating intelligence products within their respective departments and communities. To bolster the intelligence production, OPE will complement the training with an intelligence leadership training to provide leadership skills to up-and-coming Intel Commanders and intelligence professionals. Additionally, the trainings provide a venue to teach common intelligence practice and lexicon constructs between federal, state, and local LE, and to create a more common operating language when it comes to intelligence practices.

b. Strategies to Accomplish Outcomes
OPE's strategy for intelligence and leadership training helps the FBI strengthen its relationships with TFOs and state and local LE intelligence personnel while enhancing collaboration with these key partners. The goal of this strategy is to bring federal, state, and local LE agencies together in methodologies, practices, and lexicon to achieve commonalities in procedural execution of critical intelligence support to operational investigations. Unifying intelligence collection, production, and dissemination practices will render a more communicative, collaborative, and agile intelligence sharing LE environment. OPE's efforts will enhance the ability of the FBI and its partners to identify threats and share intelligence analysis faster with more actionable collection methods. Appropriated funding directly supports these training courses and, without it, OPE could not offer these opportunities to strengthen partnerships for protecting the American people. In FY 2022 OPE will ensure current training classes are maintained and will continue to meet the increasing needs of our LE partners.

The FBI missed its FY 2020 target Number of Intelligence Training Courses Offered to SLTT Partners by 18 courses. Eight (8) courses scheduled for FY 2020 were set to commence in March and run through September. Due to COVID-19 challenges, all eight courses required cancellation. In response to these challenges, OPE developed and transitioned the in-person Introduction to Intelligence for Law Enforcement Analysts course to a blended online format entitled Introduction to Intelligence for Partners (FSLTT). This course runs for 10 weeks and is comprised of online instruction and offline assignments. Two courses were offered in FY 2020, with great success.

Terrorist Screening Center

a. Performance Plan and Report for Outcomes

TSC is dedicated to ensuring watchlisting and screening activities are conducted in a manner consistent with protecting privacy and civil liberties by tracking strategic measures pertaining to both the accuracy and efficiency of TSC's work. The measures provided are an indicator of the TSC's commitment to maintaining the highest level of quality while ensuring the most up-to-date Known or Suspected Terrorist (KST) identity information is provided to its partners. TSC will continue to use these measures as a tool to improve organizational agility and refine information sharing processes for watchlisting, screening, encounter management, and identity resolution. These stringent measures reflect TSC's resolve to disseminate up-to-date KST identity information to our partners and highlight TSC's commitment to being the USG's authority in watchlisting and identity resolution. By quickly and accurately processing nominations, TSC is able to rapidly forward this vital data downstream to our partners, ensuring that any new threats are mitigated upon encounter.

Performance Measure: Percent of net analyst-edits rejected by NCTC for inaccuracy

FY19 Target: 7%
FY19 Actual: 1.4%
FY20 Target: 5%
FY20 Actual: 0.9%
FY21 Target: 5%
FY22 Target: 5%

Performance Measure: Percent of TSDB addition and deletion nominations processed within 24 hours of receipt

FY19 Target: 95%
FY19 Actual: 99%
FY20 Target: 97%
FY20 Actual: 99.6%
FY21 Target: 97%
FY22 Target: 98%

Discussion

TSC receives nominations for international KSTs from the USIC via the NCTC and nominations for domestic terrorists directly from the FBI. To provide the most accurate and up-to-date information possible to its partners, TSC analysts strive to process all nominations for addition or removal from the TSDB within 24 hours of receipt. In addition, if edits are made to the nominations submitted to the TSC by NCTC, those records are referred to NCTC for verification and concurrence. NCTC's review of TSC analyst edits represents a quality control mechanism that helps ensure the thoroughness and accuracy of the information contained in the TSDB. The TSC will strive to ensure that 5% or less of these edits submitted to NCTC are rejected, as an indicator of TSC's commitment to maintaining the highest level of quality while balancing its complex watchlisting mission.

b. Strategies to Accomplish Outcomes

The TSC will stay ahead of the threat by advancing strategic objectives, intiatives, and measures. One of the TSC’s strategic measures includes regularly conducting comprehensive and case-specific quality assurance reviews of data in the Terrorist Screening DatabaseSDB to ensure the U.S. Government’s substantive criteria for watchlisting is met and to ensure the records maintained in the watchlist are current, accurate, and thorough. Monitoring the timeliness and quality of additions, deletions, and edits to the TSDB through a monthly dashboard allows TSC management to maintain situational awareness and respond quickly to changes. TSC management is then able to reallocate resources as appropriate and determine when procedural or policy changes are necessary to ensure the accuracy and thoroughness of the TSDB. By maintaining situational awareness of the measures as well as the flexibility to reallocate resources as necessary, TSC management will be able to ensure its ability to refine information sharing operations to improve organizational agility in support of the FBI as well as the broader USIC.

B. Counterterrorism/Counterintelligence Decision Unit

Counterterrorism/Counterintelligence Decision Unit Total	Direct Pos.	Estimate FTE	Amount ($000)
2020 Enacted	13,608	12,932	$3,823,856
2021 Enacted	13,713	13,060	$3,924,373
Adjustments to Base and Technical Adjustments	16	86	$153,201
2022 Current Services	13,729	13,146	$4,077,574
2022 Program Increases	183	92	$67,483
2022 Request	13,912	13,238	$4,145,057
Total Change 2021-2022	**199**	**178**	**$220,684**

1. Program Description

The FBI's Counterterrorism/Counterintelligence (CT/CI) Decision Unit comprises the counterterrorism (CT) program, the WMDD, the counterintelligence (CI) program, a portion of the computer intrusion (cyber) program (CIP), a portion of the CIRG, and the portion of the legat program that supports the FBI's CT and CI missions. Additionally, to capture all resources that support these programs, a prorated share of resources from the FBI's operational support divisions (including the Training, Laboratory, and Security Divisions; the administrative and information technology divisions; and staff offices) are calculated and scored to the decision unit.

Counterterrorism Program

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

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

The FBI aims to eliminate the risk of international and domestic terrorism. The FBI accomplishes this by gathering intelligence from all sources and using analysis to enhance preventive efforts and exploit links between terrorist groups and their support networks. Threat information is shared with all affected agencies and personnel to create and maintain efficient threat mitigation response procedures and provide timely and accurate analysis to the USIC and senior policy makers.

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

The FBI aims to protect the U.S. from terrorist attacks by disrupting terrorists' ability to perpetrate harm. Training, finances, recruiting, logistical support, pre-attack planning, and

preparation are all required components of terrorist operations. These requirements create vulnerabilities, and the FBI focuses on building a comprehensive intelligence base to exploit these vulnerabilities.

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

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

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

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

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

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

Weapons of Mass Destruction Directorate

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

Preparing, assessing, and responding to WMD threats and incidents is challenging because WMD events and its responses are unique. To accomplish its mission, the WMDD integrates the necessary counterterrorism, intelligence, counterintelligence, and scientific and technological components in direct WMD cases and in support of its partners (CTD, CD, DI, CID, and CyD).

The WMDD coordinates the FBI's WMD program through a multifaceted approach that addresses all areas of the WMD incident spectrum, from prevention through response. This approach includes:

Preparedness	The WMDD incorporates the development of comprehensive plans and policies into its preparedness activities. The WMDD implements planning, training, and practice exercises to ensure that the FBI and its USG partners are ready to respond to WMD threats in a highly cohesive and efficient manner.
Countermeasures	The WMDD takes proactive measures to actively and passively prevent, prepare, and mitigate chemical, biological, radiological, nuclear, and explosive WMD-related threats. WMDD works with its partners via outreach activities and establishes tripwires to address "existing" threats and collaboratively develops specialized countermeasures to address "over the horizon" threats. The implementation of each countermeasure reduces the ability of bad actors to obtain, create, and use a WMD.
Investigations and Operations	The WMDD investigates the threatened, attempted, and actual use of a WMD, as well as the attempted or actual transfer of materials, knowledge, and technology needed to create a WMD. The WMDD coordinates the FBI's efforts to ensure a robust capability that can collect evidence in contaminated areas, disarm hazardous devices, and provide direct command and control (C2) support in on-scene situations.
Intelligence	The WMDD proactively leverages timely, relevant, and actionable intelligence to collaborate with key stakeholders – other FBI divisions, and USIC, LE, foreign, and private sector partners – to identify, understand, and mitigate priority current and emerging WMD threats and vulnerabilities.

The FBI combined the operational activities of the CD's counterproliferation (CP) programs with the subject matter expertise of the WMDD, and the analytical capabilities of the DI, to create specialized counterproliferation (CP) units to detect, deter, and defeat the threat posed by state-sponsored groups, individuals, and/or organizations as they attempt to obtain WMD or other sensitive technologies. The hybrid nature of CP operations incorporates aggressive counterintelligence and criminal investigative techniques, to prevent the acquisition of WMDs and dismantle the transfer of the most sensitive technologies. The FBI's CP program works closely with the National Counterproliferation Center (NCPC) to manage these high impact investigations and collection platforms, which if not fully mitigated, pose the highest threat to US national security.

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

Counterintelligence Program

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

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

Computer Intrusion Program (Cyber)

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

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

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

The FBI also leads the National Defense Cyber Alliance, where experts from the government and cleared defense contractors share threat intelligence in real time, and is co-located with

partners in industry, academia, and the financial sector as part of the National Cyber-Forensics and Training Alliance in Pittsburgh and New York City.

Critical Incident Response Program

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

CIRG encompasses the Hostage Rescue Team (HRT), a full-time national tactical counterterrorism team, and manages the SWAT program in all FBI field offices. CIRG also manages the FBI's mobile surveillance programs – the Special Operations Group (SOG) and the Special Surveillance Group (SSG) – and its aviation surveillance program, including the unmanned aircraft systems (UAS) program. SOGs are comprised of armed agents who perform surveillances of targets that might have the propensity for violence; SSGs are comprised of unarmed investigative specialists who perform surveillances of targets who are unlikely to be violent. SOGs, SSGs, and aviation surveillance provide critical support to all programs. CIRG is responsible for managing the FBI's counter-unmanned aircraft systems (C-UAS) program, performing both detect, track, locate, and identify (DTLI) and mitigation missions. CIRG operates the Strategic Information and Operations Center (SIOC) to maintain 24/7/365 enterprise-wide situational awareness. In addition, CIRG oversees the National Center for the Analysis of Violent Crime (NCAVC) Program and provides behavioral analysis and assessments for complex and time-sensitive investigations across multiple programs.

CIRG's readiness posture provides the USG with deployment capabilities to counter a myriad of CT/CI and criminal threats – from incidents involving WMDs to a mass hostage taking. The FBI's crisis response protocols are built upon lessons learned from past incidents, resulting in a tiered response, streamlined command and control, standardized training, equipment, and operating procedures, and collaboration and coordination with other partners. To counter the range of potential crises, an integrated response package that brings command and control, aviation, and technical and tactical assets under a unified structure is essential, and CIRG encompasses all of these elements.

Legal Attaché Program

Legats are the forward element of the FBI's international LE effort and often provide the first response to crimes against the U.S. and its citizens that have an international nexus. The counterterrorism component of the legat program is comprised of agents stationed overseas who work closely with their foreign counterparts to prevent terrorism from reaching into the U.S., help solve crimes, and assist with the apprehension of international terrorists who violate U.S. laws.

2. Performance and Resource Tables

PERFORMANCE AND RESOURCES TABLE										
Decision Unit: Counterterrorism/Counterintelligence										
RESOURCES	**Target**		**Actual**		**Enacted**		**Changes**		**Requested (Total)**	
	FY 2020		**FY 2020**		**FY 2021**		**Current Services Adjustments & FY 2022 Program Changes**		**FY 2022 Request**	
	FTE	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
Total Costs and FTE	12,932	$3,823,856	12,667	$3,812,856	13,060	$3,924,373	178	$220,684	13,238	$4,145,057

Strategy Performance		FY17		FY18		FY19		FY20		FY21	FY22
		Target	Actual	Target	Actual	Target	Actual	Target	Actual	Target	Target
Measure (DOJ Objective 1.1)	Number of terrorism disruptions (effected through investigations)	200	783	200	641	250	518	400	561	400	500
Measure (DOJ Objective 1.2)	Number of computer intrusion program deters, detects, disruptions, and dismantlements conducted	N/A	9,139	4,000	11,540	8,000	15,897	8,000	15,427	10,000	10,000
Measure (DOJ Objective 1.2)	Percent of private sector losses recovered by the FBI's Internet Crime Complaint Center (IC3)	N/A	30%	N/A	73%	76%	78%	77%	85%	78%	79%
Measure (DOJ Objective 1.3)	Number of National Insider Threat Task Force (NITTF) Insider Threat HUB Operations Courses conducted	N/A	8	6	10	6	8	6	3	6	6
Measure (DOJ Objective 1.3)	Percentage of FBI's Annual Insider Threat Training Compliance	95%	93%	95%	99%	95%	96%	95%	96%	95%	95%
Measure (DOJ Objective 1.3)	Number of CI program disruptions and dismantlements conducted	N/A	454	400	698	400	529	400	365	400	400
Measure (DOJ Objective 1.1)	Number of Counter Unmanned Aircraft Systems (C-UAS)	10	13	10	14	15	20	20	20	20	20

3. Resources and Strategies

Counterterrorism Division (CTD)

a. Performance Plan and Report for Outcomes

The FBI's CTD focuses its strategic efforts on defeating terrorism by advancing multiple strategic objectives through strategic initiatives and measures – such as the number of terrorism disruptions the FBI accomplishes – as evidence of the FBI's capability in achieving DOJ strategic objective 1.1 "disrupting and defeating terrorist operations." Disrupting terrorist operations is a core objective of the FBI in preserving national security and protecting the U.S. from terrorist attacks. The FBI's ability to continually meet this performance goal demonstrates the successful alignment of strategy to budget requests by accomplishing this DOJ objective and measure.

Performance Measure: Number of terrorism disruptions (effected through investigations)

FY19 Target: 250
FY19 Actual: 518
FY20 Target: 400
FY20 Actual: **561**
FY21 Target: 400
FY22 Target: 500

Discussion

A disruption is defined as interrupting or inhibiting a threat actor from engaging in criminal or national security related activity. A disruption is the result of direct actions and may include, but is not limited to, the arrest, seizure of assets, or impairing the operational capabilities of threat actors.

b. Strategies to Accomplish Outcomes

The CTD will advance its strategic objectives for partnerships and information-sharing as well as maximize the FBI's impact on the threat and its ability to achieve terrorism disruptions. As an example of strengthening partnerships, the FBI established the Domestic Terrorism-Hate Crimes Fusion Cell in FY 2019 to ensure seamless coordination across the CID and the CTD, and to advance both domestic terrorism and hate crimes investigations. The formation of this cell enabled the FBI to arrest an individual in November 2019, before bombing a synagogue. The CTD will remain committed to strengthening partnerships with partners such as private sector companies and faith-based leaders to improve the FBI's ability to share and receive information. To increase reporting by the public, which can lead to disruptions of actors before they commit violence, the FBI regularly updates its Homegrown Violent Extremist Mobilization Indicator booklet, published jointly with the National Counterterrorism Center (NCTC) and the Department of Homeland Security (DHS). In September 2020 the FBI was able to arrest two individuals for providing support to ISIS. Their disruption took place on the internet through online recruitment/radicalizations, posting ISIS propaganda, and sharing bomb instructions. During March of 2020, the FBI disrupted the plan of a Domestic Terrorist, who tried bombing a Missouri hospital. Recently, The FBI's Joint Terrorism Task Force (JTTF), stopped a domestic terrorist cell in October of 2020, who plotted to kidnap the Michigan Governor. Additionally,

the CTD will continue to pursue opportunities in data science, analytics, and building capabilities. The FBI's FY 2022 budget request will enable the CTD to better achieve these outcomes, especially in the domestic terrorism program.

Cyber Division (CyD)

a. Performance Plan and Report for Outcomes

The CyD's strategic efforts will focus on imposing risk and consequences on cyber adversaries through the FBI's unique authorities, world-class capabilities, and enduring partnerships. The computer intrusion program (CIP) is a top priority of the FBI. The mission of the CIP is to identify, assess, and neutralize computer intrusion threats emanating from terrorist organizations, state-sponsored threat actors, and criminal groups targeting the national information infrastructure. The CIP is characterized by an "all tools" approach, leveraging the FBI's dual LE and national security authorities. The CyD anticipates the number of detects, deters, disruptions, and dismantlements will continually be claimed in FY 2022 due to significant emphasis placed on FBI field offices to achieve judicial, operational, and preventative outcomes through the annual Field Office Strategic Plan (FOSP) creation and evaluations processes.

The Recovery Asset Team (RAT) was established in February 2018 by the CyD's Internet Crime Complaint Center (IC3). The RAT streamlines communication between field offices and financial institutions in an effort to recover assets for victims of any crime type that transfers funds to fraudulent domestic accounts. Recognizing that private sector partners are indispensable to successfully mitigating cyber threats, the CyD continues its efforts to establish and maintain partnerships with the private sector to ensure timely sharing of information. The CyD's ongoing relationships with private sector entities, including banking institutions, have aided in the CyD's ability to provide robust asset recovery numbers. For example, the CyD is able to maintain a platform of data sharing that is beneficial to both parties and thus, beneficial to victims, by continuing to make contact with new financial institutions, as well as fostering relationships established with current partners.

Performance Measure: Number of computer intrusion program deters, detections, disruptions, and dismantlement's conducted

FY19 Target: 8,000
FY19 Actual: 15,987
FY20 Target: 8,000
FY20 Actual: 15,427
FY21 Target: 10,000
FY22 Target: 10,000

Performance Measure: Percent of private sector losses recovered by the FBI's Internet Crime Complaint Center (IC3)

FY19 Target: 76%
FY19 Actual: 78%
FY20 Target: 77%
FY20 Actual: 85%

FY21 Target: 78%
FY22 Target: 79%

Discussion
Detect is the FBI identification of a threat actor, criminal, or national security-related activity. The detect should be claimed by the FBI case agent when known or suspected personnel, assets, front company/cover organizations, funding, operations, objectives, or tradecraft are detected or identified.

Deter is the FBI prevention of a threat actor from engaging in criminal or national security related activity through defensive countermeasures which are implemented by the FBI or implemented by strategic partners due to FBI engagement. The deterrence should be claimed by an agent when the agent's defensive countermeasures were implemented by the FBI or implemented by strategic partners due to FBI engagement.

Disruption is interrupting or inhibiting a threat actor from engaging in criminal or national security related activity. A disruption is the result of direct actions and may include, but is not limited to, the arrest, seizure of assets, or impairment of the operational capabilities of key threat actors. A disruption should be claimed in conjunction with an affirmative LE action (e.g., arrest, indictment, conviction, seizure) and/or regulatory action that impedes the normal and effective operation of the targeted criminal enterprise as indicated by changes in the organizational leadership or methods of operation (e.g., financing, trafficking partners, communications, drug production). An affirmative LE action resulting in multiple arrests, seizures, indictments, or convictions of an organization's members should be reported as one disruption of that organization. An organization, generally speaking, cannot be disrupted more than once on the same day.

A **dismantlement** occurs when the targeted organization's leadership, financial base, and supply network has been destroyed, such that the organization is incapable of operating and/or reconstituting itself. An organization can only be dismantled once. However, in the case of large organizations, several individual identifiable cells or subgroups may be present. Each of these cells or subgroups maintains and provides a distinct function supporting the entire organization. If properly documented, multiple dismantlement statistical accomplishments can be claimed as they pertain to identifiable cells or subgroups. A dismantlement should be claimed by the case agent who had the greatest role in contributing to the dismantlement when the leadership of the organization has been eliminated and/or the criminal enterprise is no longer able to sustain itself, and the last subject/primary target of the organization, cell, or subgroup has been convicted. The point in which a dismantlement will be claimed is only at the time of conviction of the last subject in the organization and/or the conviction of the primary target of the organization/identifiable cell or subgroups.

The RAT defines a "loss" as funds diverted from a victim's account to a fraudulent recipient account via deception techniques employed by fraud actors. A "**recovered loss**" is defined as funds frozen, or held, at the recipient financial institution and unable to be retrieved by the bad actor.

b. Strategies to Accomplish Outcomes
In order to achieve DOJ strategic objective 1.2 "combat cyber-based threats and attacks," as well as the FBI's strategic and operational objectives, the CyD's strategy addresses the growing criminal and national security threat of unauthorized computer intrusions by conducting investigations, collecting intelligence, and engaging victims, all in pursuit of attribution to unmask the adversary. Imposing risk and consequences on cyber adversaries ultimately leads to disruptions, deterrence, and defeat. Each fiscal year, the CyD communicates cyber threat-level guidance to all FBI field offices in order to direct efforts and drive progress toward achieving these outcomes.

The CyD will continue outreach to the private sector to educate victims on reporting incidents to IC3 in a complete and timely manner, as domestic transfers are quickly dispersed and thus difficult to recover. The CyD will also continue to partner with financial institutions to ensure streamlining of efforts to recover victim funds and will partner with regulators to monitor the effects of legal guidance that influence how the financial sector conducts the recovery of fraudulent funds.

Insider Threat Office (InTO)
a. Performance Plan and Report for Outcomes
In order for the FBI to adequately secure its holdings, it trains its workforce to identify and combat existing internal and external threats. Along with creating hardened targets by maintaining robust physical security and information systems (IS), effective personnel security measures can significantly contribute to the safety of the FBI's integrity and the prevention of insider threats. To achieve this objective for combatting insider threats, the FBI's Insider Threat Office (InTO) will continue to use National Insider Threat Task Force's (NITTF) Insider Threat Hub Operations courses to advance the education and training of its employees. The Hub Operations course is designed for employees who support an executive branch agency insider threat program. Additionally, InTO will continue developing and requiring annual insider threat training to all personnel who have been granted access to FBI systems. The FBI's annual insider threat training is a mandatory training for all personnel with FBI system access. The training contains an assessment to measure the individual's grasp of the material. A score of 80% is required to successfully pass the course.

Performance Measure: Number of National Insider Threat Task Force Threat Hub Operations courses conducted

FY19 Target: 6
FY19 Actual: 8
FY20 Target: 6
FY20 Actual: **3**
FY21 Target: 6
FY22 Target: 6

Performance Measure: Percentage of FBI's annual insider threat training compliance

FY19 Target: 95%
FY19 Actual: 96%
FY20 Target: 95%
FY20 Actual: 96%
FY21 Target: 95%
FY22 Target: 95%

Discussion
The Hub Operations training is a collaborative effort between the FBI and the National Counterintelligence and Security Center (NCSC) conducted through the NITTF. Attendees from across the Executive Branch have completed the course. By teaching program staff from the Department of Defense (DOD), the USIC, and NT-50 agencies, the course facilitates the development of professional networks between insider threat programs, which strengthen collaboration and coordination in addressing insider threats, information sharing, and problem solving. This course provides further awareness to insider threat activities to better prepare programs to deter, detect, and mitigate insider threats.

The FBI's annual insider threat training is in accordance with E.O. 12968 and E.O. 13587, an annual training requirement for all personnel with access to FBI systems. This course contains a post-test which requires a score of 80% or higher. The training incorporates insider risk detection and mitigation. The purpose of this course is to familiarize personnel with the appropriate actions to take in relation to possible insider threats. Upon completion of this course, personnel are able to recognize insider threat concerns and the appropriate actions to take when faced with signs of a possible insider threat. The training is available on both the classified and unclassified enclaves.

b. Strategies to Accomplish Outcomes
The FBI's InTO strategy focuses on protecting U.S. information by detecting and deterring insider threat actors, as well as mitigating risks associated with insider threats. InTO advances DOJ strategic objective 1.3 by strengthening systems and educating the workforce against internal and external threats.

The InTO will continue supporting the Hub Operations courses via formal classroom settings, practical exercises, forums, working groups, and conferences. In support of the Hub Operations courses, InTO will develop additional methods of course delivery and expand its accessibility. During the National Emergency, the Hub Operations course expanded its training platform to a virtual setting.

The InTO will continue requiring and tracking completion of the web-based, annual training to ensure all personnel with access to FBI systems receive insider threat awareness training. In order to complete the course, employees must have a successfully passed assessment. The InTO will also perform internal reviews of the course material to ensure appropriate updates and changes are incorporated.

The FBI missed its FY 2020 Number of National Insider Threat Task Force Threat Hub Operations courses conducted by three courses. A workforce trained in internal and external threats is better able to secure its information, effective personnel security measures can deter and prevent insider threats and robust information systems and physical security can create a hardened target for external actors. Therefore, the FBI's Insider Threat Office (InTO) continues to ensure a well-trained workforce by supporting iterations of the National Insider Threat Task Force's (NITTF) Insider Threat Hub Operations courses. Due to COVID-19, the Hub Operations courses were not conducted in the third and fourth quarter of the fiscal year. In September 2020, the NITTF published a Virtual Hub Operations Course schedule took place in a virtual environment through the remainder of calendar year 2020. Additionally, the InTO continues developing and requiring annual Insider Threat training to all personnel who have been granted access to FBI systems. The FBI's annual Insider Threat training is a mandatory training for all personnel with FBI system access. The training contains an assessment to measure the individual's grasp of the material. A score of 80% is required to successfully pass the course. InTO assigned a Training Coordinator to track and report compliance details to managers. InTO exceeded the target for FY20 at 96% compliance.

Counterintelligence Division (CD)

a. Performance Plan and Report for Outcomes

The CD uses the performance measure "number of counterintelligence program disruptions and dismantlement's" to count the counterintelligence operational outcomes with the greatest impact on threat actors during the fiscal year. Disruptions and dismantlement's are high-impact, low-frequency accomplishments demonstrating the FBI's capacity to interrupt adverse operations and impede threat actors from conducting future operations. This metric directly measures the impact of FBI actions to achieve DOJ strategic goal 1 "enhance national security and counter the threat of terrorism" via DOJ strategic objective 1.3 "combat unauthorized disclosures, insider threats, and hostile intelligence activities." As a direct measure of effectiveness, this performance measure provides an ideal justification for the annual budget, demonstrating the operational outcomes that rely on appropriate resourcing. This performance measure is a key indicator as to how well the federal government is mitigating the negative risks of the insider threat, intellectual property theft, and information access, as well as leveraging the opportunities of globalization and private sector engagement as part of that risk mitigation strategy. Each disruption or dismantlement is the outcome of investigative and analytical efforts by the FBI through a whole-of-government approach, often alongside local, private sector, and foreign partners, to disrupt a hostile intelligence scheme or unauthorized disclosure that would otherwise have harmed U.S. national or economic security.

Performance Measure: Number of counterintelligence program disruptions and dismantlements conducted

FY19 Target: 400
FY19 Actual: 529
FY20 Target: 400
FY20 Actual: 365
FY21 Target: 400
FY22 Target: 400

Discussion
This measure uses the combined score of two types of statistical accomplishments – disruptions and dismantlement's – as documented by the FBI in the counterintelligence program case files of its official, classified recordkeeping system. **Disruption** is interrupting or inhibiting a threat actor from engaging in national security-related activity. A **dismantlement** occurs when the targeted organization's leadership, financial base, and supply network has been destroyed, such that the organization or active cell is incapable of operating and/or reconstituting itself. FBI personnel claim statistical accomplishments for various types of operational activities so the number of occurrences of these activities can be tracked for oversight purposes. By this definition, dismantlement's are relatively rare. Disruptions are the primary accomplishment that demonstrates how the FBI has stopped or mitigated threat activities against U.S. targets, and disruptions vary in size of impact. The target remains stable so that investigators can focus on impact to the threat actor rather than the total number of disruptions each year.

b. Strategies to Accomplish Outcomes
The FBI's counterintelligence strategy focuses on protecting U.S. information, items, and other assets by disrupting hostile foreign actors and by dismantling organizations that further the hostile activities. Preventing the loss of assets and proactively disrupting threat actors are essential parts of a counterintelligence strategy; once a hostile foreign nation has acquired U.S. assets, the damage cannot be undone. In FY 2020, the CD activated a new threat mission center approach to put direct emphasis on combatting the highest priority threats as determined through FBI and USIC analysis and strategic vision. The mission centers leverage the broadest set of lawful tools, including non-prosecutorial methods, and the broadest set of allies, including other U.S. agencies at all levels of government, the private sector, and friendly foreign partners, against the most damaging sponsors of hostile foreign intelligence activity. The FBI has increased coordination with that set of allies through the National Counterintelligence Task Force (NCITF), providing nationwide coordination with federal LE and USIC partners on the model of successful drug and counterterrorism joint task forces. The NCITF supports CI task forces in all 56 field offices, allowing the FBI to leverage additional federal, state, and local LE personnel to bring additional resources to bear on the broad-based counterintelligence threat.

The FBI missed its FY 2020 Number of counterintelligence program disruptions and dismantlements conducted by 35. The public health response to the 2020 COVID-19 pandemic demanded creative ways to achieve the FBI counterintelligence mission while maintaining the safety of all employees, witnesses, victims, and suspects. The FBI Counterintelligence Division met this challenge, continuing to produce high quality outcomes through the height of the pandemic. While the total number of disruptions and dismantlements lagged behind the annual target, the numbers show this was a direct result of COVID-19 protection strategies in quarters 3 and 4. Throughout FY20, the FBI Counterintelligence Division continued its focus on identifying, understanding, and combating foreign activities in order to deter, defeat, and aggressively respond to counterintelligence threats against U.S. national and economic security. Key accomplishments include the August arrests of Alexander Yuk Ching Ma and Peter Rafael Dzibinski Debbins on charges that they provided national security information to the governments of China and Russia, respectively; the July forfeiture filings to seize the ill-gotten gains from North Korean and Iranian violators of international sanctions on their governments; and the February indictment of Chinese technology firm Huawei with conspiracy to violate the

Racketeer Influenced and Corrupt Organizations Act (RICO), marking a novel use of this legal strategy to complete a counterintelligence investigation. In addition, Henry Kyle Frese was sentenced to 30 months in prison for leaking national defense information to journalists in 2018 and 2019, and the Department of Justice achieved the successful extradition of accused international sanctions violators in the custody of Georgia and the United Kingdom. Despite the pandemic, the FBI made historic strides in combatting unauthorized disclosure, insider threat, and hostile intelligence activities.

Critical Incident Response Group (CIRG)

a. Performance Plan and Report for Outcomes

The FBI's counter-unmanned aircraft systems (C-UAS) program remains a priority strategic initiative for the organization in order to better protect the American people and stay ahead of emerging threats. Program management responsibilities have transitioned from the OTD to the CIRG, and the CIRG will continue to enhance the FBI's capabilities in the C-UAS mission space by delivering technology-based C-UAS solutions to enable and enhance the FBI's intelligence, national security, and LE operations.

Performance Measure: Number of C-UAS deployments

FY19 Target: 15
FY19 Actual: 20
FY20 Target: 20
FY20 Actual: 20
FY21 Target: 20
FY22 Target: 20

Discussion

C-UAS measure: Within the past few years, UAS experienced rapid advancements in technology and market growth resulting in highly capable, simple-to-use aircraft which are easily accessible to the general public. As UAS continue to become more complex and integrated into everyday life, so will the exploitation of UAS by individuals with nefarious intent. Recent events involving UAS in the Middle East, the United Kingdom, and in the U.S. have highlighted serious security gaps and emphasized the need for C-UAS capabilities. The FBI established itself as one of the experts on C-UAS matters among its international and domestic LE partners. The C-UAS program has experienced drastic increases in requests to provide both operational support to the field, as well as institutional knowledge to its partners. In order to mitigate the ever-growing threat posed by UAS, the CIRG's C-UAS program is exploring means to expand research and development capabilities, as well as operational capacity.

b. Strategies to Accomplish Outcomes

CIRG's strategy to protect the American people, stay ahead of the threat, and lead in the mission space for the FBI's C-UAS program is a defensive one where the CIRG actively deploys C-UAS technology in support of National Special Security Events (NSSEs) and Special Event Assessment Rating (SEAR) events, as well as for investigative purposes. Current defensive capabilities include detection, tracking, locating, and identification of small UAS devices utilizing an array of technologies to include: radio frequency (RF) direction finding, RF decoding

and demodulation, radar, and infrared/electro-optical camera systems. The CIRG's C-UAS program has various mission profiles which are dependent on field office requests, the level of field office support, and specialized legal authorities. The C-UAS program's core mission is to identify, track, and locate UAS operating within the airspace surrounding an event or location.

The C-UAS program provides UAS operator location information to response personnel who will attempt to intercept and educate the UAS operator. If mitigation authority has been obtained for the event, the C-UAS program will deploy and utilize technologies capable of mitigating a UAS while in flight. UAS mitigation capabilities are categorized as (from least to most destructive) either cyber, RF jamming, or kinetic. Cyber-based mitigation involves a man-in-the-middle style attack, essentially, hijacking the UAS command and control (C2) signal – this allows for the C-UAS operator to take control of the UAS, providing several options. RF jamming overwhelms the UAS command and control link within a given environment. This technique may or may not lead to a predictable outcome. Kinetic mitigation is any method that makes physical contact with the UAS while in operation. The FBI's C-UAS program currently has limited UAS mitigation capabilities and is working to acquire, develop, and integrate additional CONUS appropriate mitigation technologies.

In addition to traditional RF-based tracking capabilities, the CIRG's C-UAS program is exploring means to support research and develop new technological methods which would identify, track, and locate UAS that utilize cellular and/or satellite communication for command and control (C2). The FBI currently utilizes equipment capable of detecting and tracking traditional UAS C2 technologies, which are limited in range and to line-of-site communication. Recent technological developments have provided industry and hobbyists with commercially available and inexpensive equipment which allow for UAS C2 over cellular and satellite communications networks. This advancement is very likely to be adopted by industry and hobbyists in the near future, in part, because it eliminates the range and line-of-site restrictions of traditional UAS C2. Although current cellular based tracking technology is very capable, it is not able to identify and/or distinguish the difference between cellular-based UAS C2 and standard cellular communications traffic.

C. Criminal Enterprises and Federal Crimes Decision Unit

Criminal Enterprises and Federal Crimes Decision Unit Total	Direct Pos.	Estimated FTE	Amount ($000)
2020 Enacted	12,924	12,597	$3,303,519
2021 Enacted	12,924	12,608	$3,416,096
Adjustments to Base and Technical Adjustments	7	(10)	$64,619
2022 Current Services	12,931	12,598	$3,480,715
2022 Program Increases	61	31	$62,943
2022 Request	12,992	12,629	$3,543,658
Total Change 2021-2022	**68**	**21**	**$127,562**

1. Program Description

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

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

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

The structure of the FBI's criminal intelligence program maximizes the effectiveness of resources; improves investigation and intelligence gathering processes; focuses on threats from criminal enterprises; and promotes the collection, exchange, and dissemination of intelligence throughout the FBI and other authorized agencies.

Financial Crimes

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

Violent Crime and Gang Threats

The FBI's violent crime and gang program aims to combat violent criminal threats and to disrupt and dismantle local, regional, national, and transnational cells of criminal enterprises that pose the greatest threat to the economic and national security of the U.S.

The violent crime component combats the most significant violent crime offenders and threats falling within the FBI's investigative jurisdiction. Violent crime continues to threaten communities within the U.S. and its citizens. Major violent crime incidents such as mass killings, school shootings, serial killings, and violent fugitives can paralyze whole communities and stretch state and local LE resources to their limits. Particular emphasis is directed toward matters involving serial violent offenders and significant violence, including bank robberies, armored car robberies, fugitives, kidnappings for ransom, extortions, police killings, and assault on federal officers.

Cyber Program
Included under the purview of the cyber program within the CEFC DU are criminal computer intrusion investigations conducted by the CyD and IC3.

Legal Attaché Program
Crime-fighting in an era of increasing globalization and interconnectivity is a truly international effort, and the people who make up the IOD and legat program work together to lead and direct the FBI’s growing number of operations around the globe.

The FBI’s legats and their staffs work hard to combat crime and strengthen the bonds between LE personnel throughout the world. Agents working in the IOD use their unique skill sets and knowledge to coordinate investigations large and small. Legats partner with the FBI’s criminal and intelligence divisions, foreign LE, and U.S. and foreign intelligence and security services.

The IOD and legat program also includes a major training component, which includes efforts such as supporting international LE academies and teaching LE partners about proper investigation techniques at crime scenes or crisis management.

2. Performance and Resource Tables

PERFORMANCE AND RESOURCES TABLE										
Decision Unit: Criminal Enterprises and Federal Crimes										
RESOURCES	**Target**		**Actual**		**Enacted**		**Changes**		**Requested (Total)**	
	FY 2020		**FY 2020**		**FY 2021**		**Current Services Adjustments & FY 2022 Program Changes**		**FY 2022 Request**	
Total Costs and FTE	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
	12,597	$3,303,519	12,471	$3,280,519	12,608	$3,416,096	21	$127,562	12,629	$3,543,658

Strategy Performance		FY17		FY18		FY19		FY20		FY21	FY22
		Target	Actual	Target	Actual	Target	Actual	Target	Actual	Target	Target
Measure (DOJ Objective 3.1)	Percentage increase of gang/criminal enterprise dismantlements (non-consolidated priority organized target (CPOT)) from prior FY*	160	147	15% (173)	19% (194)	15% (198)	16% (217)	15% (227)	-6.6% (185)	15% (261)	15% (300)
Measure (DOJ Objective 4.1)	Number of Criminal Organizations Engaging in White-Collar Crimes Dismantled	400	389	400	510	400	388	400	205	400	400
Measure (DOJ Objective 3.2)	CPOT-linked drug-trafficking organizations (DTOs) disrupted	50	57	50	50	50	58	50	76	50	50
Measure (DOJ Objective 3.2)	CPOT-linked DTOs dismantled	20	23	20	21	20	14	20	11	20	20
Measure (DOJ Objective 4.1)	Number of investigations opened on Elder Fraud	N/A	N/A	N/A	N/A	60	96	90	176	90	90

3. Resources and Strategies

Criminal Investigative Division (CID)

a. Performance Plan and Report for Outcomes

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

CID's measures, as identified by DOJ and FBI strategic priorities, provide a snapshot of the FBI's work within the criminal program. As such, the measures cannot adequately demonstrate all of the work performed within the CID's budget or resources, which is allocated across all criminal threats, not just those posed by gangs, criminal enterprises/organizations, and drug trafficking organizations. However, gangs, criminal enterprises, criminal organizations engaging in white-collar crime and money laundering, and drug-trafficking organizations are some of the highest priority threats, as identified by DOJ and FBI. As disruptions and dismantlements of these criminal groups hinders or eliminates their ability to commit crimes, these performance measures demonstrate the most impactful work performed by the FBI against these threats.

DOJ maintains a national list of the most prolific major international drug trafficking and money laundering organizations threatening the U.S. known as the Consolidated Priority Organization Target (CPOT) list, which reflects the most significant international narcotic manufacturers, poly-drug traffickers, suppliers, transporters, and money laundering organizations.

The intent of the performance measures are as follows:

CPOT-linked drug trafficking organizations (DTOs) disrupted:
Increase the number of CPOT-linked cases, thereby leading to increased disruptions linked to CPOTs.

CPOT-linked DTOs dismantled:
Increase the number of CPOT-linked cases, thereby leading to increased dismantlements linked to CPOTs.

Percentage of gang/criminal enterprise dismantlements (non-CPOT):
Increase the percentage of gang/criminal enterprise dismantlements (non-CPOT).

Number of criminal organizations engaging in white collar crimes dismantled:
Increase the number of criminal enterprises engaging in white-collar crimes dismantled.

Number of investigations opened on elder fraud:
Count the number of investigations targeting elder fraud, a priority for DOJ prosecution.

CID is committed to vigorous enforcement efforts against these violent transnational criminal organizations and gangs, and uses all available tools, to include developing relationships with foreign LE partners and targeting the most egregious criminal acts, to disrupt and dismantle the most violent gangs and criminal organizations. CID is also committed to vigorous enforcement of the wide range of financial criminal violations within its purview. Major areas of focus include money laundering, health care fraud, corporate fraud, securities and commodities fraud, fraud targeting the elderly, and intellectual property rights crimes (e.g., theft of trade secrets and counterfeiting). To combat those crimes, the FBI

focuses heavily on maintaining and enhancing relationships with foreign, state, local, and private industry partners; developing advanced analytical capabilities to identify criminal activity; and targeting the most egregious criminal actors to disrupt and dismantle schemes and organizations.

CID anticipates the number of disruptions, dismantlements, and case initiations will continually be claimed in FY 2022 because of emphasis to achieve judicial and preventative outcomes. These quantitative outcomes will largely reflect the work performed and progress toward meeting and exceeding the relevant performance measure, targets, or goals. Leveraging future resources and focusing efforts against addressing the outlined DOJ/FBI objectives can ultimately ensure increased public safety.

Performance Measure: Percentage increase of gang/criminal enterprise dismantlement's (non-CPOT) from prior FY

FY19 Target: 15% (198)
FY19 Actual: 16% (217)
FY20 Target: 15% (227)
FY20 Actual: -6.6% (185)
FY21 Target: 15% (261)
FY22 Target: 15% (300)

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

FY19 Target: 400
FY19 Actual: 388
FY20 Target: 400
FY20 Actual: 205
FY21 Target: 400
FY22 Target: 400

Performance Measure: CPOT-linked DTOs disrupted

FY19 Target: 50
FY19 Actual: 58
FY20 Target: 50
FY20 Actual: 76
FY21 Target: 50
FY22 Target: 50

Performance Measure: CPOT-linked DTOs dismantled

FY19 Target: 20
FY19 Actual: 14
FY20 Target: 20
FY20 Actual: 11
FY21 Target: 20
FY22 Target: 20

Performance Measure: Number of investigations opened on Elder Fraud

FY19 Target: 60
FY19 Actual: 96
FY20 Target: 90
FY20 Actual: 176
FY21 Target: 90
FY22 Target: 90

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

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

b. Strategies to Accomplish Outcomes
The CID's strategy focuses on strategic objectives and efforts to fulfill the FBI's vision to stay ahead of the threat. CID has developed, implemented, and prioritized strategies as part of DOJ's strategic goal 3 "reduce violent crime and promote public safety," objectives 3.1 "combat violent crime, promote safe communities, and uphold the rights of victims of crime," and 3.2 "disrupt and dismantle drug trafficking organizations to curb opioid and other illicit drug use in our nation," and DOJ's goal 4 "promote integrity, good government, and the rule of law," objective 4.1 "uphold the rule of law and integrity in the proper administration of justice."

The FBI uses the Enterprise Theory of Investigation (ETI), which focuses on disrupting and dismantling the entire criminal organization through intelligence-based targeting and execution of coordinated investigations against the high value subjects.

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

enterprises and dark web vendors importing, distributing, and selling fentanyl and illegal opioids, as well as sources of illegitimate prescription opioids. The Prescription Drug Initiative targets health care providers and pharmaceutical companies involved with illegal marketing and distribution practices, as well as fraudulent prescriptions. The FBI and DOJ are partnered together on the Appalachian Regional Prescription Opioid Strike Force, which has dedicated investigators and prosecutors to address the problem in the region.

The FBI also uses ETI to reduce the threat of violent crime and promote safe neighborhoods and is committed to vigorous enforcement efforts against violent transnational criminal organizations and gangs. The FBI will continue to strive for the goals set forth of non-CPOT gangs and criminal enterprise dismantlements in order to be accountable and committed to reduce violent crime through partnerships.

As part of overall efforts to reduce criminal activity, the FBI is engaged with DOJ priority initiatives, such as the growing threat of fraud targeting elderly victims. DOJ and the FBI initiated the Transnational Elder Fraud Strike Force to investigate and prosecute these cases across the country, and the FBI increased resources, intelligence gathering, and investigations to facilitate prosecution in cooperation with DOJ.

To advance strategic objectives for the rule of law, the FBI's white collar crime program will integrate intelligence analysis with its investigations of criminal activities such as public corruption, money laundering, corporate fraud, securities and commodities fraud, mortgage fraud, financial institution fraud, bank fraud and embezzlement, fraud against the government, election law violations, mass marketing fraud, and health care fraud. The FBI generally focuses on complex investigations – often with a nexus to organized crime activities – that are international, national, or regional in scope and where the FBI can bring to bear unique expertise or capabilities that increase the likelihood of successful investigations.

CID will work closely with partner LE and regulatory agencies such as the Securities and Exchange Commission, the Internal Revenue Service, the U.S. Postal Inspection Service, the Commodity Futures Trading Commission, and the Treasury Department's Financial Crimes Enforcement Network, among others, targeting sophisticated, multi-layered fraud cases that harm the American people and the U.S. economy.

The FBI missed its FY 2020 Percentage increase of gang/criminal enterprise dismantlement's (non-CPOT) from prior FY by 6.6 percentage points. During the FY20 reporting period, the FBI had significant gang/non-CPOT dismantlements, including Operation Only Family. The Operation Only Family investigation was initiated by the FBI Chicago Field Office (CG) to target The Black Disciples (BD), a violent gang operating in the Greater Chicago area. The BDs were involved in the distribution of street level and wholesale amounts of narcotics, gang-related homicides, credit card fraud, assaults, armed robberies, and aggravated batteries. The investigation progressed to a large-scale, multi-state endeavor involving federal, state, and local law enforcement partners. CG's CHS operations, 16 Title III intercepts, and multiple search warrants led to CG's arrest of 27 individuals and seizure of 20 firearms, over 14 kilograms of cocaine, and 2.5 kilograms of heroin in July 2020. In a spin-off case, FBI Milwaukee initiated an investigation into the BD based on intelligence gained from the CG operation. Gang members were subsequently indicted on narcotics and firearms violations. These investigations and dismantlements had a significant impact on the operations of the Black Disciples in the Mid-West.

The FBI missed its FY 2020 Number of criminal organizations engaging in white collar crimes dismantled by 195. The FBI's CID operational challenges were compounded by other COVID-19 challenges, such as FBI personnel exposures/quarantines, the inability to conduct sensitive case analysis from remote environments ("telework"), and the lack of private industry responsiveness (specifically to federal grand jury (FGJ) subpoenas for business records). Additionally, there was an increase in COVID-19 crime, specifically in schemes/complaints related to Price Gouging/Hoarding, Procurement Fraud, Investment Fraud, Counterfeit Public Health Products, and Unemployment Insurance. The FBI needed to reallocate investigative resources to mitigate the financial losses from these crimes.

The FBI missed its FY 2020 Number of CPOT-linked DTOs dismantled by nine. The COVID-19 Pandemic affected all target measures and severely impacted investigative accomplishments for FY 2020. Numerous planned operations did not occur and were postponed until FY 2021. The widespread shutdown also affected the U.S. Attorney's Offices and courts (including FGJ procedures), which are responsible for the prosecution, trial, and sentencing of subjects. The FBI defines a dismantlement as when a criminal organization (e.g., leadership, financial infrastructure) is incapable of operating or reconstituting itself, so the FBI does not claim these statistics until the last subject in the organization is sentenced. This extended period in which there were limited court proceedings (e.g., indictments, trials, proffers) greatly affected the FBI's ability to fully dismantle criminal enterprises and claim statistics under DOJ strategic objectives 3.1 and 3.2.

D. Criminal Justice Services Decision Unit

Criminal Justice Services Decision Unit Total	Pos.	FTE	Amount ($000)
2020 Enacted	2,323	2,276	$575,965
2021 Enacted	2,461	2,363	$590,876
Adjustments to Base and Technical Adjustments	0	89	$29,628
2022 Current Services	2,461	2,452	$620,504
2022 Program Increases	27	13	$4,085
2022 Request	2,488	2,465	$624,589
Total Change 2021-2022	**27**	**102**	**$33,713**

1. Program Description

The Criminal Justice Services (CJS) Decision Unit comprises the following:

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

Criminal Justice Information Services Division

The mission of CJIS is to equip LE, national security, and intelligence community (IC) partners with the criminal justice information needed to protect the U.S. while preserving civil liberties. CJIS includes several major program activities that support this mission, all of which are described below.

Next Generation Identification (NGI): NGI provides timely and accurate identification services in a paperless environment 24 hours a day, 7 days a week. The NGI system, which expanded and significantly enhanced the FBI’s biometric identification capabilities, became fully operational in September 2014, providing the criminal justice community with the world’s largest and most efficient electronic repository of biometric and identity history information.

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

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

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

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

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

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

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

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

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

The NGI system also expanded cascade or reverse search services to include newly submitted criminal, select civil, and other investigative biometric events to produce new investigative leads after initial search and retention of latent prints within the Unsolved Latent File (ULF). The ULF contains latent finger and palm prints from criminal and terrorist subjects that have searched against the legacy IAFIS and/or the NGI system but remain unidentified. As of July 31, 2020, the

ULF consisted of 945,031 unidentified latent prints contributed by local, state, federal, and international LE agencies, as well as LD and members of the USIC from evidence within both criminal and terrorism investigations.

National Palm Print System (NPPS) and Interstate Photo System (IPS) - In FY 2013, NGI added the NPPS, containing over 20 million biometric images, and the IPS, as well as new services, such as rapid mobile searches, facial recognition, and Rap Back, a service which is designed to assist federal, state, and local agencies in the continuous vetting of individuals in a position of trust. The IPS, through facial recognition, now provides a method to search over 43 million booking photos of criminals – data the FBI has collected for decades – and generates a list of ranked candidates to be used as potential investigative leads by authorized agencies, adding another way biometrics can be used as an investigative tool.

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

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

The NGI CJ RBS is designed to provide immediate notifications to LE on an NGI Identity of subscribed individuals currently under an active criminal investigation, active probation, or parole (custody and supervision).

Currently, three of the largest submitting agencies include the State of Utah, the State of Texas, and the Transportation Security Administration (TSA). Utah has enrolled 337,720 active Rap Back subscriptions, and Texas has enrolled 2,249,873 Rap Back subscriptions, to include teachers, nurses, and EMS workers. The TSA has enrolled 625,195 Rap Back subscriptions from numerous airports and airlines throughout the U.S.

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

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

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

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

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

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

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

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

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

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

National Instant Criminal Background Check System: The NICS is a national system established to enforce the provisions of the Brady Handgun Violence Prevention Act of 1993. Federal Firearms Licensees (FFL) utilize the NICS to determine whether receipt of a firearm by a prospective purchaser would violate state or federal law. The system ensures the timely transfer of firearms to individuals who are not specifically prohibited and denies transfer to prohibited persons.

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

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

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

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

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

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

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

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

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

Law Enforcement Enterprise Portal: The FBI's LEEP is a gateway for thousands of users in the criminal justice, intelligence, and military communities to gain access to critical data protected at the Controlled Unclassified Information level in one centralized location. With one click, users can securely access national security, public safety, and terrorism information contained within dozens of federal information systems. Consistent with the National Strategy for Information Sharing and Safeguarding, LEEP also connects users to other federations serving the USIC, the criminal intelligence community, and the homeland security community. LEEP gives users the ability to transfer and use information efficiently and effectively in a consistent manner across multiple organizations and systems to accomplish operational goals.

National Data Exchange: The FBI's N-DEx System is an unclassified national strategic investigative information-sharing system, which enables criminal justice agencies to search, link, analyze, and share local, state, tribal, and federal records across jurisdictional boundaries. The N-DEx System contains incident, arrest, and booking reports; pretrial investigations; supervised release reports; calls for service; photos; and field contact/identification records.

By using the N-DEx System as a pointer system and for data discovery, users can uncover relationships between people, crime characteristics, property, and locations; generate integrated biographies of subjects; eliminate information gaps by linking information across jurisdictions; discover relationships between non-obvious and seemingly unrelated data; and obtain collaboration among agencies by allowing its users to coordinate efforts in a secure online environment.

The N-DEx System connects many regional and local information-sharing systems and leverages their collective power to provide access to millions of records. The N-DEx System complements existing state and regional systems and is positioned to fill in gaps in the many areas of the country where no information sharing system or program currently exists. The N-DEx System contains over 538 million searchable records from over 7,500 criminal justice agencies and provides access to an additional 336 million records from DHS, the Interstate Identification Index, NCIC, and INTERPOL.

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

Center, the IC3, the WMD tip line, and all FBI electronic information submissions (E-Tips). The NTOC's threat intake examiners (TIEs) receive threat information from individuals around the globe, completing preliminary research and analysis on the information received and documenting all relevant information in the Threat Intake Processing Systems (TIPS) database. The TIEs make a determination on the threat level associated with the information provided, determine if the information needs immediate action (such as TTLs), and refer the information to the appropriate FBI entity or other appropriate LE agency for action. NTOC works 24/7/365 to provide reliable, actionable, and high-value information to the field and other partner agencies.

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

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

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

Laboratory Division

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

Training Division

In addition to training FBI agents, the FBI provides instruction for state and local LE partners, both at the FBI Academy and throughout the U.S. at state, regional, and local training facilities; the principal course for state and local LE officers is the 10-week multi-disciplinary course at the FBI National Academy. These training sessions cover the full range of LE training topics, such as hostage negotiation, computer-related crimes, and arson.

Due to the ongoing pandemic, Training Division has not held a National Academy session in FY21. The next session of NA is currently scheduled to begin in September of 2021, comprised of 100 students (no foreign nationals due to travel restrictions). TD is watching closely and will revise the start date if necessary, to accommodate ongoing pandemic concerns.

International Operations Division

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

2. Performance and Resources Tables

PERFORMANCE AND RESOURCES TABLE										
Decision Unit: Criminal Justice Services										
RESOURCES	**Target**		**Actual**		**Enacted**		**Changes**		**Requested (Total)**	
	FY 2020		**FY 2020**		**FY 2021**		**Current Services Adjustments & FY 2022 Program Changes**		**FY 2022 Request**	
Total Costs and FTE	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
	2,276	$575,965	2,235	$581,965	2,363	$590,876	102	$33,713	2,465	$624,589

Strategy Performance		FY17		FY18		FY19		FY20		FY21	FY 22
		Target	Actual	Target	Actual	Target	Actual	Target	Actual	Target	Target
Measure (DOJ Objective 4.4)	Percent of Next Generation Identification (NGI) system availability	N/A	N/A	99.5%	99.66%	99.5%	99.90%	99.5%	99.81%	99.5%	99.5%
Measure (DOJ Objective 4.4)	Percent of National Crime Information Center (NCIC) system availability	99.5%	99.73%	99.5%	99.86%	99.5%	99.82%	99.5%	99.71%	99.5%	99.5%
Measure (DOJ Objective 4.4)	Percent of National Instant Criminal Background Check System (NICS) system availability for any user of the NICS	98%	98.98%	98%	99.64%	98%	99.80%	98%	99.81%	98%	98%
Measure (DOJ Objective 4.4)	Number of DNA profiles in profiles in the National DNA Index System (NDIS) changed	950,000	938,006	950,000	1,017,843	950,000	1,024,489	950,000	833,140	700,000	700,000
Measure (DOJ Objective 4.4)	Percent of multi-band radios distributed supporting multi-agency interoperability	2%	2%	8%	7%	8%	10%	8%	10.6%	9%	9%

3. Resources and Strategies

Criminal Justice Information Services

a. Performance Plan and Report for Outcomes

CJIS division will improve information technology management, infrastructure, and services by deploying innovative solutions in collaboration with the STB, the ITB, and the OCIO. CJIS will architect, engineer, develop, deliver, operate, and maintain secure networks and computing environments which enable the efficient delivery and hosting of information and technical services to protect the American people and LE partners. The following measures will be utilized to drive toward a high degree of system availability to ensure CJIS continues to progress towards achieving DOJ strategic objective 4.4.

CJIS intends to provide percentages quarterly to demonstrate system availability for NGI. The outcome for this measure is 99.5 percent system availability to ensure operational efficiencies.

CJIS intends to provide target percentages quarterly to demonstrate system availability for the NCIC. The outcome for this measure is 99.5 percent system availability to ensure operations efficiencies.

CJIS intends to provide target percentages quarterly to demonstrate system availability for the National Instant Criminal Background Check System (NICS). The outcome for this measure is 98 percent system availability to ensure operations efficiencies.

Performance Measure: Percent of NGI system availability

FY19 Target: 99.5%
FY19 Actual: 99.90%
FY20 Target: 99.5%
FY20 Actual: 99.81%
FY21 Target: 99.5%
FY22 Target: 99.5%

Performance Measure: Percent of NCIC system availability

FY19 Target: 99.5%
FY19 Actual: 99.82%
FY20 Target: 99.5%
FY20 Actual: 99.71%
FY21 Target: 99.5%
FY22 Target: 99.5%

Performance Measure: Percent of NICS system availability for any user of the NICS

FY19 Target: 98%
FY19 Actual: 99.80%
FY20 Target: 98%
FY20 Actual: 99.81%
FY21 Target: 98%
FY22 Target: 98%

Discussion
NGI (99.5%) - Provide exemplary system availability to ensure the most complete and up-to-date records possible for criminal and noncriminal justice purposes.

NCIC (99.5%) - Provide real-time, accurate, and complete criminal justice information to support LE and criminal justice communities.

NICS (98%) - Provide reliable availability of the NICS to save lives and protect people from harm by ensuring the timely transfer of firearms or firearm and explosive-related permits to eligible persons.

The system availability for NGI, NCIC, and NICS measures the probability that these major information sharing systems are functioning when needed, under normal operating conditions.

b. Strategies to Accomplish Outcomes
CJIS will collect daily statistics for the three system availabilities during the quarter and report outcomes as necessary. The daily updates will ensure consistent management of the systems to ensure achievement of the measure targets set forth for FY 2022. Additionally, STB will monitor and manage quarterly strategic goals and objectives set by branch executive management to maintain oversight management of the CJIS systems. STB's fiscal, strategic, and intelligence program managers will work collaboratively with CJIS counterparts and CJIS systems subject matter experts in meeting DOJ strategic objective 4.4 "achieve management excellence" and the FBI's strategic objective "improve information technology."

Laboratory Division
a. Performance Plan and Report for Outcomes
LD will measure the change in the number of profiles in the National DNA Index System (NDIS) with the aim of demonstrating the overall impact of the National DNA Database. DNA profiles in NDIS support the exchange and comparison of forensic DNA evidence from violent crime investigations. NDIS submissions, the highest level of the Combined DNA Index System (CODIS) hierarchy, enable the exchange and comparison of DNA profiles on a national level from partner laboratories. An increase in the volume of profiles provides insight into the potential for providing aid to investigations and obtaining hits. An increase in this number impacts LD budget and resourcing requirements.

DNA legislation has had two recent legislation updates, which involve federal DNA collection agencies submitting samples to the FBI Laboratory for analysis and commercially available Rapid DNA equipment being connected to the national DNA database. Successfully meeting these requirements in DNA processing will lead to significant benefits to public safety by increasing the size of the national DNA database and leveraging the latest technology to enhance the speed of DNA analysis.

Performance Measure: Number of DNA profiles in the NDIS changed

FY19 Target: 950,000
FY19 Actual: 1,024,489
FY20 Target: 950,000
FY20 Actual: 833,140
FY21 Target: *700,000*
FY22 Target: *700,000*

Discussion
The greater the number of DNA profiles in NDIS, the greater the ability to obtain forensic and offender hits, which link two or more cases or link a forensic sample to a sample that falls under the "offender" category of profiles in NDIS, as well as aid investigations by adding value to the investigative process in a case.

b. Strategies to Accomplish Outcomes
LD strategy will introduce novel techniques that can be applied to laboratory services to better serve its stakeholders and customers. LD will enhance forensic capabilities by ensuring research is relevant, well-managed, and aligned to DOJ and FBI gaps and strategic priorities. LD will support this strategic direction through communication and collaboration with CODIS partners and stakeholders (conferences, Advisory Policy Board (APB) working groups, etc.), implementation of Rapid DNA capability and booking stations, and the processing of DNA samples from federal arrestees and convicted offenders by entering the samples into CODIS. LD will also participate in the development of relevant policies that impact the submission of DNA samples.

The FBI missed its FY 2020 target number of DNA profiles in the NDIS changed by 116,860. NDIS is a system of DNA profile records input by criminal justice agencies, including state and local law enforcement agencies beyond the FBI. Many of these state and local agencies experienced the effects of COVID-19 related restrictions (such as less frequent sample collection and reduced staffing), contributing to fewer DNA profiled uploaded to NDIS during FY 2020. Additionally, several NDIS-participating laboratories were unable to submit CODIS metric updates or were only able to submit limited information, negatively affecting the change in the number of DNA profiles in NDIS for FY 2020.

<u>Operational Technology Division</u>
a. Performance Plan and Report for Outcomes
The intent of the OTD's strategy and strategic measure is for the OTD to deploy innovative solutions in a consistently changing communications environment where there is still a serious need for federal secure radio communications. By replacing single-band radios with multi-band radios, the FBI will be able to inter-operate more regularly and with more fluidity amongst federal, state, and local partners. The FBI relies on radio communications to conduct a vast array of investigations to include those that support DOJ's strategic objectives of disrupting terrorist planning and hostile intelligence activities in the U.S. Additionally, the FBI is currently supporting DOJ objectives along the southwest border of the U.S. Multi-band radios are a necessity for FBI agents, as the radios allow them to use relevant, current, and secure radio technological advancements to communicate on a vast array of networks, which are required to uphold the task force model present in field offices around the country.

Performance Measure: Percent of multi-band radios distributed supporting multi-agency interoperability

FY19 Target: 8%
FY19 Actual: 10%
FY20 Target: 8%
FY20 Actual: 10.6%
FY21 Target: 9%

FY22 Target: 9%

Discussion
An OTD strategic goal is to deploy innovative solutions in a consistently changing communications environment and this is being met by replacing single band radios with multi-band radios.

b. Strategies to Accomplish Outcomes
OTD's strategy is to use yearly allocated funding to gradually refresh approximately 30 percent of the FBI's aging fleet of radios utilizing a regional approach. The OTD will continue to strive to meet its goals and support the needs of agents in the field. Increasing the number of multi-band radios in the FBI will enhance the agency's ability to communicate with other DOJ components and with other federal, state, and local LE partners to support DOJ objectives.

V. PROGRAM INCREASES BY ITEM

Item Name: **Countering Domestic Terrorism**

Strategic Goals: 1, 3, 4
Strategic Objectives: 1.1, 3.1, 3.2, 4.1
Organizational Programs: Criminal Justice Information Services, Counterterrorism, Terrorist Screening Center, Information Technology

Program Increase: Positions 179 Agt 80 FTE 90 Dollars $45,000,000 ($8,968,000 non-personnel)

Description of Item

The FBI requests 179 positions (80 Special Agents) and $45,000,000 ($8,968,000 non-personnel) to effectively counter terrorism and the increasing acts of domestic terrorism occurring across the United States. The FBI must be able to identify, assess, and respond to potential threats. Specifically, the requested resources will be used to enhance the following areas:

- **Combating Domestic Terrorism:** The FBI requests 147 positions (80 Special Agents) and $39,650,000 ($6,363,000 non-personnel) to detect and disrupt domestic terrorism (DT) threats nationwide.
- **National Security Threat Program:** The FBI requests 7 positions and $2,025,000 ($1,105,000 non-personnel) to maintain public safety and effectively address the emerging requirements associated with the National Security Threat Program (NSTP).
- **The National Threat Operations Center:** The FBI requests 25 positions and $1,825,000 (all personnel) to increase capacity to support the receipt, prioritization, and processing of actionable tips in support of threat intake, operational requirements, and resilience.
- **Enterprise Voice over Internet Protocol:** The FBI requests $1,500,000 (all non-personnel) to enhance Enterprise Voice over Internet Protocol (EVoIP) capabilities in support of threat intake, operational requirements, and resiliency.

Justification

For more than a century, the FBI has occupied a critical role in protecting the U.S. from threats to American public safety, borders, economy, and way of life. To do so, the FBI has developed advanced methods to detect, prevent, and disrupt threats using human resources, information, and technology. Investment in these methods is critical to address emerging threats. Investing in NTOC and domestic terrorism personnel will help mission-critical information reach investigators, analysts and partners and allow them to complete holistic strategic analysis and take action to prevent acts of violence and terror.

Combating Domestic Terrorism (DT): 147 positions (80 Special Agents) and $39,650,000 ($6,363,000 non-personnel)

Large-scale DT incidents have increased significantly over the last year. Civil unrest and riots are specifically addressed by the DT program within the FBI and do not have coverage or investigative responsibility by any other U.S. Government (USG) entity. Most notably, the siege on the U.S. Capitol on January 6, 2021 was determined to be a DT incident and has resulted in a two-fold increase in DT cases across the FBI. Every FBI field office has been impacted by this singular incident and has had to divert resources from other programs to effectively address increased case load. Other examples of DTs utilizing civil unrest and riots over the last year are highlighted by events in Minneapolis, MN; Portland,

OR; Kenosha, WI; Louisville, KY and various other U.S. cities in 2020 and 2021. Each of these incidents required a surge in resources to address the DT threat as well as the deployment of FBIHQ assets to assist in the management of these incidents. The tactics, techniques and procedures used by DTs in these incidents have proven to be effective and similar activities will likely continue in the future, requiring significant FBI resources to address DT threats.

DT shootings throughout the U.S., including those occurring in Poway and Gilroy, California; El Paso, Texas; and Jersey City, New Jersey have also increased significantly in the past few years. 2019 saw more DT activity in the U.S. than the previous 24 years – since the 1995 Oklahoma City bombing – combined. Analysis of these incidents has revealed new trends such as DTs traveling overseas, increased DT prevalence in the military, and an increase in involuntary celibate actors. The emergence of DT has been recognized at the highest levels of the USG, as evidenced by the inclusion of DT threats for the first time in the October 2018 National Strategy for Counterterrorism and the April 2020 designation of the Russian Imperial Movement, which promotes racially motivated domestic terrorist (RMDT) ideology as a Specially Designated Global Terrorist Group.

To mitigate violent criminal activity, the FBI's DT program took tangible actions over the past year, such as branding RMVE as a National Threat Priority, expanding the use of advanced investigative techniques, and collaborating more consistently with partners (e.g., state/local LE, the National Counterterrorism Center, and DHS). These measures directly contributed to key disruptions of RMVEs associated with Neo-Nazi groups (The Base and Atomwaffen Division) and of individuals who sought to commit violence in furtherance of their anti-government/anti-authority extremist ideology. The additional 147 positions (80 Special Agents) will enhance the FBI’s ability to effectively manage and combat domestic terrorism threats, including investigations, targeting, threat analysis, and source reporting. The 147 additional positions will be split between Headquarters (HQ) and the Field Offices (FOs). A current example of that collaboration was evident during the 2020 WOLVERINE WATCHMEN investigation into the plot against the Governor of Michigan, as it was another resource intensive endeavor that involved multiple subjects across multiple Field Offices.

In FY 2020, the FBI's DT program has had to employ more advanced investigative techniques than in years past, including more long-running undercover operations and online exploitation efforts due to the increased sophistication of actors and their advanced use of technology. Additionally, given the constant virulence of the DT threat, the DT program has been forced to increase its surveillance coverage of subjects. In the past, only a small portion of DT actors may have had a high propensity for imminent violence. The FBI is now seeing a more widespread predisposition to violent criminal activity, which necessitates more extensive surveillance coverage. As such, the FBI seeks to enhance domestic terrorism efforts by requesting $4,478,000 in non-personnel resources for case and other operational expenses, training, and information technology maintenance and enhancement.

As a result of the attack on the U.S. Capitol the FBI is also requesting $1,885,000 to address the increase in data collection volume and complexity necessitates for data storage, analysis, and sharing. Handling large amounts of data is common to many prosecutions and is critical for meeting discovery obligations and this funding will help facilitate that process.

NSTP All Threats Screening: 7 positions and $2,025,000 ($1,105,000 non-personnel)

The FBI requests 7 positions and $2,025,000 ($1,105,000 non-personnel) to effectively address the emerging requirements associated with the NSTP to maintain public safety.

The Terrorist Screening Center (TSC) must have technical tools and personnel in place to address grave threats to national and public safety, from initial information or tip intake, through analysis, sharing, and investigation. With enhanced capabilities, the TSC and FBI will be able to better address national security threats in part by reducing its response time to partners, completing mandated checks in the required time, illuminating trends, identifying new targets, and increasing information sharing. The TSC will also be able to expand the infrastructure within the USIC's I2 cloud architecture to address intelligence gaps and provide a common operating picture of how threats converge.

NTOC: 25 positions and $1,825,000 (all personnel)

NTOC operates 24/7/365, providing the public with an effective avenue to submit tips to the FBI concerning suspected criminal and terrorist activity. NTOC is responsible for processing all telephonic and E-Tips from the public and currently serves all FBI field offices. After evaluating information received, NTOC provides the information to the field offices and headquarters entities as appropriate. NTOC also operates the Major Case Contact Center, which fields calls for high-profile investigations and initiatives. NTOC examiners are supervised by support supervisors and supervisory special agents (SSAs) trained to respond to national security and emergency situations such as bomb threats, active shooter incidents, hostage situations, threats to life (TTL), and cyber threats. NTOC has helped reduce the administrative burden on the FBI's 56 field offices by creating a central intake point for the FBI. This has also allowed for incoming information to be tracked and analyzed more efficiently.

NTOC has been successful in bringing fugitives to justice. Below are a few examples:

- November 2019: An anonymous individual submitted an E-Tip to NTOC to report an unidentified YouTube user who posted a video depicting himself in a hotel room with large amounts of ammunition and several weapons. The NTOC examiner processed the tip and information was provided to the FBI's San Diego Field Office, which opened a preliminary investigation. The individual was arrested by the FBI and the San Diego Joint Terrorism Task Force for possession of an assault weapon, possession of a high-capacity magazine, and child endangerment.
- April 2020: NTOC received a call from a Bank Secrecy Act Office Senior Vice President (SVP) for Stifel Bank and Trust in St. Louis, Missouri. The SVP informed the NTOC examiner of a fraudulent $300,000 wire transfer to a bank in Canada. The NTOC examiner forwarded the information to the St. Louis field office, and the entire $300,000 was recovered as a result of a multiple-day effort between the FBI, Stifel Bank and Trust, and individuals at other banks.
- December 2020: NTOC received a call from the former girlfriend of Anthony Quinn Warner, the individual responsible for the Christmas Day 2020 recreational vehicle (RV) bombing in Nashville, Tennessee, which damaged 41 downtown buildings and crippled telecommunication systems throughout the Southeast. The threat intake examiner (TIE) gathered enough information from the caller to create a Guardian lead and forwarded it to the Memphis Field Office. The TIE continued to gather information from the caller and other sources to confirm Warner's address. The next day, members of the FBI's Laboratory Division, using DNA samples, confirmed Warner's death in the explosion. The Guardian lead and the vital information the TIE forwarded to special agents in the Memphis Field Office was crucial to the investigation.

In January 2020, NTOC experienced unprecedented call-volumes resulting from the U.S. Capitol unrest. NTOC witnessed nine out of the top ten record breaking days for tips/calls in the Center's

history. To mitigate the volumes, several resources were surged to NTOC to meet the increased demand and mandatory overtime was implemented.

Despite successes, NTOC has identified gaps in providing this mission-critical service. The volume of calls and E-Tips exceeds NTOC's capacity to properly respond to each submission. The inability to properly address each submission results in long wait times and contribute to a 28 percent abandoned call rate. Abandoned calls that go unanswered, or delays processing of E-Tips could result in a TTL and information loss.

The NTOC experienced an increase of 98 percent (388,995) as of January 31, 2021 over the same time in FY 2020. This increase was primarily the result of the U.S. Capitol unrest which occurred on January 6, 2021. NTOC anticipates an overall increase in calls of about 459 per day, increasing the average daily submissions to 6,224. Peak times, crises, events, and major cases result in more tips, leading to more dropped calls due to wait times, and delays processing E-Tips. In addition, NTOC also experienced an increase in Internet Crime Complaint Center (IC3) and social media tip submissions in FY 2021, up to 20,709 per day.

In mitigation, the FBI is executing the strategies listed below.

- Using an operations center to monitor incoming work and handle call spikes by moving TIEs from working E-Tips to the phone lines.
- Requiring all non-operational personnel assigned to NTOC to take E-Tip training to handle incoming information during periods of high volume.
- Requiring mandatory overtime for all National Threat Operations Section (NTOS) staff.
- Requiring non-NTOS Criminal Justice Information Services (CJIS) Division staff to maintain NTOC proficiency standards to assist during times of high volumes, pulling them from their home team functions.
- Establishing a program Assisting NTOC to Help Operational Resources (ANCHOR) for volunteers across the Division to support during times of crisis.
- Using contractor staff to assist with E-Tip processing.
- Establishing efficiencies such as a screening tool that diverts callers who have made numerous non-value reports.
- Using algorithm technology that minimizes a TIE's time devoted to non-serious or non-valuable online tips, identifies important or high-risk tips, and prioritizes tip for action.
- Developing a social media bucket which allows for efficient and expedient processing of low scoring social media threats.
- Developing the SSA Triage bucket for SSAs to review all complaints to ensure significant threats are immediately processed.

The additional positions are requested to ensure that the FBI effectively handles all incoming tips, especially those containing critical TTL tips.

EVoIP: $1,500,000 (all non-personnel)

The FBI requests an additional $1,500,000 of non-personnel funding to enhance EVoIP capabilities in support of threat intake, operational requirements, and resiliency. This funding will provide the FBI with enhanced capabilities in terms of call accounting and call trace capabilities. The new architecture (EVoIP) will provide the ability to fully trace calls coming into the FBI from any point to the

destination. The FBI will also transition circuits to SIP (Session Initiation Protocol), which will provide the FBI with detailed information about the calls it receives.

The FBI intends to upgrade its standalone telecommunications infrastructure into a dual-core, geo-redundant, centralized, and private cloud-based solution that will support operations, improve resiliency, and establish an additional method of communication during a crisis event. Currently, the FBI has isolated, locally managed telecommunication systems which are nearing obsolescence and fail often. The FBI is establishing a western telecommunication enterprise core at its Pocatello Datacenter. This enhancement will establish a permanent eastern core at the FBI's Clarksburg Data center providing geo-redundancy for centralized telecommunication voice services, such as call recording, accounting, voicemail services, active domain, and systems management.

Impact on Performance

The FBI considers the attack on the U.S. Capitol Building on January 6, 2021 to be a "DT event" and therefore is managed by the Domestic Terrorism Operations Section (DTOS). As such, DTOS tracked an increase in investigations of approximately 57 percent from January 2021 to April 2021. It is estimated that approximately 2000 individuals are believed to have been involved with the siege and nearly all field offices have an active investigation stemming from this DT event. Given the complexities of this singular event, the increase in funding and personnel is crucial to the success of the FBI to provide appropriate oversight in these investigations to ensure consistency, compliance, and appropriate use of resources.

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

Funding

Base Funding

FY 2020 Enacted				FY 2021 Enacted				FY 2022 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
1,067	569	1,072	$196,338	1,384	730	1,446	$292,450	1,384	730	1,523	$298,639

Personnel Increase Cost Summary

Type of Position/Series	Positions Requested	Annual Costs per Position ($000)			FY 2022 Request ($000)	Annualizations ($000)	
		1st Year Adjusted Cost	2nd Year Adjusted Cost	3rd Year Full Cost (Modular)		FY 2023 (net change from 2022)	FY 2024 (net change from 2023)
Special Agent, Field	80	$296	$237	$401	$23,680	($4,720)	$8,400
Intelligence Analyst	43	$172	$178	$236	$7,396	$258	$2,752
Clerical	25	$73	$110	$92	$1,825	$925	$475
Professional Support	5	$101	$140	$178	$505	$195	$385
Staff Operations Specialists	26	$101	$140	$178	$2,626	$1,014	$2,002
Total Personnel	**179**	**$743**	**$805**	**$1,085**	**$36,032**	**($2,328)**	**$14,014**

Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	FY 2022 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2023 (net change from 2022)	FY 2024 (net change from 2023)
Contract-Management	$2,803	N/A	N/A	$0	$0
Contract-Training	$500			$0	$0
Equipment	$838			($838)	$0
IT Service	$31			$0	$0
Supplies	$2,796			($1,845)	$0
Telecommunication	$1,500			$0	$0
Travel-Training	$500			$0	$00
Total Non-Personnel	**$8,968**	**N/A**	**N/A**	**($2,683)**	**$0**

Justification for Non-Personnel Annualizations

The FBI will recur $6,825,000 annually to support IT services, telecommunication, training, travel, and contractor support to address emerging threats to national and public safety. Outyear expenditures for equipment and supplies will be reduced after the initial investment.

Total Request for this Item

Category	Positions	Amount Requested ($000)	Annualizations ($000)

	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2023 (net change from 2022)	FY 2024 (net change from 2023)
Current Services	1,384	730	1,523	$293,0148	$5,625	$298,639	N/A	N/A
Increases	179	80	90	$36,032	$8,968	$45,000	($5,011)	$14,014
Grand Total	**1,563**	**810**	**1,613**	**$329,046**	**14,593**	**$343,639**	**($5,011)**	**$14,014**

Item Name: **McGirt Resources**

Strategic Goals: 3, 4
Strategic Objectives: 3.1, 3.2, 4.1
Budget Decision Unit: Counterintelligence and Criminal Enterprise/Federal Crimes
Organizational Programs: Support for Indian Country

Program Increase: Positions 0 Agt 0 FTE 0 Dollars $25,500,000 ($13,597,000 non-personnel)

Description of Item

The FBI requests $25,500,000 ($13,597,000 non-personnel) to effectively address the increased operational need in the state of Oklahoma following the Supreme Court decision in *McGirt v. Oklahoma.* This ruling significantly expanded federal jurisdiction for crimes committed on the tribal lands of five Native American reservations in Oklahoma. Specifically, the requested resources will be used to temporarily enhance the FBI's capacity to address the significantly increased number of investigations now falling under FBI jurisdiction in Oklahoma while Federal, state, and tribal authorities identify a longer term solution.

Justification

The Major Crimes Act (MCA) and the General Crimes Act (GCA) combine to provide federal jurisdiction over most serious criminal acts committed by or victimizing a Native American in Indian Country (IC) territory. These acts establish the FBI as having primary jurisdiction over a wide range of criminal acts in IC which typically fall under state or local jurisdiction.

On July 9, 2020, the Supreme Court's ruling in *McGirt v. Oklahoma* determined the territorial boundaries of the Muscogee Creek Nation (MCN) fall under federal IC jurisdiction, making the FBI the responsible LE agency under the MCA for offenses committed by or victimizing a tribal member. The territorial boundaries of the MCN now under FBI jurisdiction encompass most of the city of Tulsa and approximately one million residents, including approximately 60,000 MCN tribal members.

The principles of the McGirt decision also apply to the status of the Cherokee, Chickasaw, Choctaw and Seminole tribal territories. The Cherokee and Chickasaw reservations were reaffirmed as falling under federal jurisdiction on March 11, 2021 and the Choctaw and Seminole reservations were reaffirmed on April 1, 2021. Combined, all five reservation territories encompass approximately 32,000 square miles, or 45 percent of the state of Oklahoma. The total population within the combined borders is roughly 1.9 million, of which approximately 420,000 are enrolled tribal members.

This drastic increase in FBI jurisdiction poses significant and long-term operational and public safety risks given the challenges associated with the increased number of violent criminal cases now under federal jurisdiction within Oklahoma's IC territory. Since this decision, the FBI's Oklahoma City Field Office (OC) now has the FBI's largest IC investigative responsibility. FBI OC has seen a drastic increase in the total number of IC investigations. From July 9, 2020 to March 23, 2021, FBI OC opened nearly 1,000 IC investigations, prioritizing cases involving the most violent offenders who pose the most serious risk to the public. As a point of comparison, the FBI's other 55 Field Offices opened a combined total of 1,255 IC investigations during the same period, with FBI Minneapolis, the next largest IC office behind FBI OC, opening over 300 cases.

The FBI's workload data described above primarily represents the cases from the MCN reservation alone. Workloads are expected to increase substantially given the additions of the Cherokee and Chickasaw reservations in mid-March and the Choctaw and Seminole reservations in April. As all five tribal territories were reaffirmed as being under federal jurisdiction, current projections indicate FBI OC could open over 7,500 IC investigations over the course of one year. Approximately 2,500 of these cases would be new and approximately 5,000 would be adopted from cases previously adjudicated in Oklahoma state courts which were overturned by the *McGirt* decision. Without an increase in investigative personnel, the permanently allocated Special Agents working IC matters in FBI OC would be opening two new cases and four adopted cases per week, nearly eight times the national average of FBI agent caseloads across all investigative areas.

The vast majority of FBI OC IC cases are death investigations and investigations of child sexual abuse, violent assaults, and domestic violence. These investigations are key components of DOJ's strategic goal to *Reduce Violent Crime and Promote Public Safety* and objective to *Combat violent crime, promote safe communities, and uphold the rights of victims of crime*, as well as meeting the goals of *Operation Lady Justice*, the Presidential Task Force on Missing and Murdered American Indians and Alaska Natives established by Executive Order 13898 in November 2019. FBI OC's new area of IC responsibility presents unique investigative challenges which hinder the ability to achieve these objectives, including a large metropolitan area with high-population density, overwhelmed tribal police departments, and the FBI's unique responsibility to investigate crimes perpetrated by non-tribal members on tribal members, regardless of the crime.

To effectively conduct these investigations, the FBI has conducted temporary duty (TDY) rotations of an approximate total of 140 Special Agents to the Muskogee and Tulsa RAs, the offices most impacted by the decision. Additionally, Investigative Analysts, Victim Specialists, and other professional staff from FBI Field Offices and other FBI OC programs and locations were provided. FBI OC has also expanded state, local, and tribal participation on task forces to 230 Task Force Officers from 32 agencies to assist with initial response and investigative efforts. As of March 19, 2021, the U.S. Attorney's Offices in the Eastern District of Oklahoma and the Northern District of Oklahoma also increased its staffing. In order to support the U.S. Attorney's effective prosecution of these crimes, the FBI must have the capability to sustain an enhanced presence in FBI OC.

Based on the increased operation needs created by the *McGirt* decision as described above, the FBI requests funding in the amount of $11,903,000 to account for a portion of the personnel expenses incurred by the FBI's staffing increase in FBI OC. This includes compensation and benefits for FBI Special Agents and Professional Staff temporarily re-assigned to work IC matters within FBI OC as well as TDY personnel to FBI OC from other field offices. In addition to the surge in personnel, the FBI requires non-personnel funding, including approximately $1,699,000 in transfer costs and relocation incentives and approximately $6,080,000 in travel expenses for TDY personnel. To accommodate this increase in staffing, the FBI requires approximately $4,885,000 in additional funding for physical space (e.g., rent, construction, furniture), IT infrastructure (e.g., network equipment, computers), vehicles, and other equipment/supplies. Lastly, to adequately address the significant increase in investigations, the FBI is requesting approximately $933,000 in training and case funds.

Impact on Performance

The FBI's current footprint in Oklahoma draws personnel from other Field Offices and from programs within FBI OC, effectively reducing resources available to investigate other criminal activity, both within Oklahoma and across the nation. Furthermore, reducing violence and protecting American communities through vigorous investigation of violent crimes is a key DOJ priority, as is DOJ's commitment to enhance the operation of the criminal justice system to address the concerns of tribal communities. To keep Oklahoman's safe, and to fully respond to these priority missions while maintaining operational posture against other threats, the FBI requires an additional $25.5 million allocated to FBI OC and the Indian Country program while Federal, state, and tribal authorities identify a longer-term solution.

Funding

Base Funding

FY 2020 Enacted				FY 2021 Enacted				FY 2022 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

The base funding for McGirt Resources was based off previous fiscal years, Indian Country figures.

Personnel Increase Cost Summary

Type of Position/Series	Positions Requested	Annual Costs per Position ($000)			FY 2022 Request ($000)	Annualizations ($000)	
		1st Year Adjusted Cost	2nd Year Adjusted Cost	3rd Year Full Cost (Modular)		FY 2023 (net change from 2022)	FY 2024 (net change from 2023)
Special Agent, Field	N/A	N/A	N/A	N/A		N/A	N/A
Intelligence Analyst							
Computer Scientist							
Data Analyst							
Digital Operations Specialist							
Staff Operations Specialist							
Total Personnel	**N/A**	**N/A**	**N/A**	**N/A**	**$11,903**	**N/A**	**N/A**

Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	FY 2022 Request	Unit Cost ($000)	Quantity	Annualizations ($000)

	($000)			FY 2023 (net change from 2022)	FY 2024 (net change from 2023)
Travel	$6,080	N/A	N/A	-$6,080	$0
Vehicles	$1,060			-$1,060	$0
Space Rental-Non GSA	$2,675			-$2,675	$0
IT Hardware	$610			-$610	$0
Travel-Training	$85			-$85	$0
PCS-Other	$1,699			-$1,699	$0
Case Funds	$848			-$848	$0
Supplies	$115			-$115	$0
Furniture	$425			-$425	$0
Total Non-Personnel	**$13,597**	**N/A**	**N/A**	**-$13,597**	**$0**

Justification for Non-Personnel Annualizations

FBI is not recurring this program enhancement.

Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2023 (net change from 2022)	FY 2024 (net change from 2023)
Current Services	0	0	0	$0	$0	$0	N/A	N/A
Increases	0	0	0	$11,903	$13,597	$25,500	$0	$0
Grand Total	**0**	**0**	**0**	**$11,903**	**$13,597**	**$25,500**	**$0**	**$0**

Item Name: **Cyber**

Strategic Goal: 1
Strategic Objective: 1.2
Budget Decision Units: Counterterrorism/Counterintelligence and Criminal Enterprises/Federal Crimes
Organizational Program: Cyber

Program Increase: Positions 155 Agt 52 FTE 78 Dollars $40,000,000 ($7,103,000 non-personnel)

Description of Item

The FBI requests 155 positions (52 Special Agents) and $40,000,000 ($7,103,000 non-personnel) to address the rapidly evolving cyber threats facing the nation.

The requested resources will strengthen the foundation the FBI needs to remain the world's premier cyber investigative agency equipped to work with United States allies and partners to impose risk and consequences on cyber adversaries through joint, enabled, and sequenced operations. This request focuses on the development of three critical areas:

- Cyber threat identification, analysis, and attribution;
- Synchronized interagency operations; and
- Cyber workforce development.

Justification

A principal component of the FBI's cyber strategy, announced by the FBI Director in September 2020, is to impose risk and consequences on cyber adversaries using the FBI's capabilities to further its operations and those of its partners. The FBI leverages its authorities as a LE agency and as the lead for domestic intelligence collection to conduct investigations, collect intelligence, and engage with victims in pursuit of attribution. Attribution allows the United States Government (USG) to deter and respond to malicious cyber activity through such actions as infrastructure disruptions, indictments, arrests, demarches, sanctions, and operations coordinated and sequenced with foreign and domestic partners.

As a member of the LE community and the IC, the FBI uses an array of tools and supports partners responsible for the spectrum of network defense and offensive operations. More specifically, the FBI uses industry partnerships, criminal legal process, and national security tools to:

- Warn of adversary plans and intentions;
- Obtain unique insight into adversary activity on domestic infrastructure and victim networks;
- Engage foreign partners to obtain evidence stored overseas; and
- Share information to inform network defense, attribution, and response.

This request is for resources to position the FBI to meet threats from criminal and nation-state cyber actors and continue the critical support the FBI provides to public, private, and government partners.

Recent legislation, independent studies, and Presidential directives underscore the need to resource the FBI to deter and combat cyber threats.

The 2020 Cyberspace Solarium Commission report recommends strengthening the FBI's cyber program, noting that "understanding the cyber threat requires domestic intelligence gathering, evidence collection, technical and human operations, and the cooperation of victims and third-party providers to support investigative efforts," which the FBI is uniquely positioned to provide. It also recommends strengthening the National Cyber Investigative Joint Task Force (NCIJTF) to coordinate whole-of-government counter-threat campaigns and enable other agencies' missions in support of National Strategic Objectives.

The 2018 National Cyber Strategy asserts that LE actions to combat malicious cyber actors serve as an instrument of national power by deterring malicious cyber activity.

Presidential Policy Directive-41 designated the FBI as the USG's lead agency for threat response to significant cyber incidents.

Executive Order (EO) 13870 on America's Cybersecurity Workforce directs departments and agencies to grow, strengthen, and develop their cyber workforces. The FBI must have a workforce trained and equipped to meet the next generation of cyber threats.

Cyber Threat Identification, Analysis, and Attribution: 10 Positions and $7,657,000 ($5,937,000 non-personnel)

Intelligence Gathering and Analysis: 10 Positions and $1,720,000 (all personnel)

Timely action on cyber threats requires the FBI to analyze and assess disparate data and act on its findings, but current and projected growth in the volume, speed, and complexity of malicious cyber activity and its associated data outstrips the FBI's current capacity to address the cyber threat.

The requested enhancement will support the following:
- Increase capacity to identify and analyze cyber activity by known actors with intent and capability to harm the United States;
- Create a new capability to attribute malicious cyber activity to individuals or state actors;
- Increase capacity to share unique information from FBI collections and public-private partnerships through Intelligence Information Reports (IIRs);
- Increase capacity to share intelligence with and from foreign partners by placing cyber intelligence analysts in key FBI legal attaches.

Cyber Threat Actor Program (CTAP): $3,750,000 (all non-personnel)

The CTAP, established in the FBI in FY 2020, is required to fulfill DOJ's commitments outlined in National Security Presidential Memorandum (NSPM)-7. Those commitments include strengthening the ability of the USG to effectively integrate, correlate, analyze, evaluate, and share information concerning National Security Threat Actors (NSTAs) and their networks, and using that information in support of national security missions and activities as an essential component of United States national security. NSTA information comprises identity attributes and associated information about individuals, organizations, groups, or networks assessed to be a threat to the safety, security, or national interests of

the United States that fall into one or more of five NSTA defined categories in NSPM-7: Cyber, foreign intelligence, military, transnational criminal, and weapons proliferators.

To meet the requirements of NSPM-7, the NCIJTF formed an interagency governance model encouraging agencies to identify and contribute cyber threat actor information from within their holdings. It also created the Malicious Cyber Actor System (MCAS) to curate, exchange, and enrich this information flow between stakeholder agencies.

This request will provide the FBI with the hardware, software, development services, and facilities needed to adhere to its NSPM-7 executive agent responsibilities for cyber threat actors. It will also provide the FBI with additional capabilities to:

Gather and maintain the first USG collection of evaluated cyber threat actor identity intelligence information;
- Enable interoperability with agencies' existing holdings;
- Improve efficiencies for sharing knowledge between agencies; and
- Increase opportunities for detecting, attributing, interdicting, disrupting, and deterring cyber threats.

CyNERGY: $2,187,000 (all non-personnel)

EO 13636 on "Improving Critical Infrastructure Cybersecurity" directed the Attorney General and Secretary of the Department of Homeland Security (DHS), in coordination with the Director of National Intelligence, to establish a system for tracking the production, dissemination, disposition, and sharing of unclassified threat reports to entities targeted by malicious cyber activity.

The FBI developed CyNERGY to be this system. CyNERGY enables rapid, transparent, and coordinated contact by the FBI and Sector Risk Management Agencies against specific incidents, addressing a key request from private industry for coordinated engagement by the federal government. As cyber criminals and nation-state actors increasingly target US critical infrastructure networks and other private sector entities, these funds will enable CyNERGY's development and maintenance to evolve to meet the volume of targeted entities as well as interagency partner requirements.

Synchronized Interagency Operations: 145 Positions (52 Special Agents) and $31,177,000 (all personnel)

Model Field Office Cyber Squad: 145 Positions (52 Special Agents) and $31,177,000 (all personnel)

Frequent, significant, and complex cyber threats from criminals and nation-state actors require response through synchronized offensive and defensive actions by multiple USG agencies. The FBI's cyber operational resources have remained relatively flat as the IC, Department of Defense (DOD), and DHS have continued to grow their cyber capabilities and capacities. These partner agencies' missions depend on the FBI, requiring the FBI's cyber program to be sufficiently resourced. The FBI has internally reprioritized resources to cover these requirements, but additional resources are needed to address the significant current and projected nation-state and criminal threats.

This request will ensure each FBI field office is equipped at the minimum necessary investigative, analytical, technical, and administrative level to address cyber threats under a model field office cyber squad. These resources will enhance cyber investigations, cyber intelligence production, and cyber-

related engagement targeting Russian, Chinese, North Korean, Iranian, and criminal cyber threats, and increase the FBI's capacity for joint, enabled, and sequenced operations.

Cyber Workforce Development: $1,166,000 (all non-personnel)

Accelerated Cyber Training Program (ACTP): $1,166,000 (all non-personnel)

The ACTP will help ensure the FBI continues to be the world's premier cyber investigative agency by pairing world-class training facilities with a world-class training program, strengthened by Huntsville's proximity to government and academic partners.

The FBI's expansion to Huntsville will bolster its technology, training, talent, and analytics and includes construction of a state-of-the-art Innovation Center. This facility will include advanced cyber training elements, including advanced classroom space, a kinetic cyber range, and a virtual reality range. To complement the state-of-the-art training facility and ensure the FBI cyber workforce keeps pace with the threat, the FBI seeks to enhance the capabilities of its cyber training programs. As new positions are added to the FBI's cyber intrusion program, the FBI must be able to rapidly develop students' skills through the ACTP, which includes topics such as cyber investigative techniques, technical training, cybersecurity, cyber incident response, and Industrial Control Systems/Supervisory Control and Data Acquisition (ICS/SCADA) basics.

The accelerated nature of the program requires significant initial investment to reduce typical baseline training times. The ACTP will address skill shortages and allow the FBI to build a workforce capable of combating emerging cyber threats while ensuring the best cyber talent is deployed against the most significant threats.

Impact on Performance

The investments in the FBI's cyber program will help position the FBI to meet the increasing demands of the cyber threat and the synchronized, innovative, interagency operations needed to impose a real and lasting impact on United States adversaries.

With additional resources for cyber threat identification, analysis, and attribution, the FBI will more quickly organize and analyze data to identify and act on adversary activity, enabling quicker responses throughout the USG.

Investing in synchronized interagency operations will extend the capabilities of the FBI's computer intrusion program nationwide by equipping every FBI field office with at least one model cyber squad. This will increase the FBI's capacity for joint, enabled, and sequenced operations with other federal agencies, international partners, and state and local partners through FBI cyber task forces, as well as the FBI's local engagement with private sector targets of malicious activity.

Investments in accelerated cyber training undergird all the FBI's efforts to change the cost-benefit calculus of cyber adversaries. The requested resources will help create a highly capable FBI cyber workforce trained in the latest technical tools and adversary techniques.

Funding

Base Funding

FY 2020 Enacted				FY 2021 Enacted				FY 2022 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
2,083	978	1,950	$440,496	2,124	1,006	2,016	$435,371	2,124	1,006	2,038	$458,413

Personnel Increase Cost Summary

Type of Position/Series	Positions Requested	Annual Costs per Position ($000)			FY 2022 Request ($000)	Annualizations ($000)	
		1st Year Adjusted Cost	2nd Year Adjusted Cost	3rd Year Full Cost (Modular)		FY 2023 (net change from 2022)	FY 2024 (net change from 2023)
Special Agent, Field	52	$296	$237	$401	$15,392	($3,068)	$5,460
Intelligence Analyst	57	$172	$178	$236	$9,804	$342	$3,648
Computer Scientist	1	$334	$401	$350	$334	$67	$16
Data Analyst	34	$184	$219	$206	$6,256	$1,190	$748
Staff Operations Specialist	11	$101	$140	$178	$1,111	$429	$847
Total Personnel	**155**	**$1,087**	**$1,175**	**$1,371**	**$32,897**	**($1,040)**	**$10,719**

Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	FY 2022 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2023 (net change from 2022)	FY 2024 (net change from 2023)
Contract Services	$4,761	N/A	N/A	$0	$0
Cloud Services	$500			$0	$0
IT Hardware	$250			$0	$0
IT Software	$350			$0	$0
IT Maintenance	$110			$0	$0
GSA Space Rental	$370			$0	$0
Travel	$37			$0	$0
Training	$500			$0	$0
Travel-Training	$225			$0	$0
Total Non-Personnel	**$7,103**	**N/A**	**N/A**	**$0**	**$0**

Justification for Non-Personnel Annualizations

The FBI will maintain the effort at current or increased levels in the outyears. Contract and cloud services will be sustained to continue mission support. Specifically, the FBI anticipates maintaining 19 contract FTE to support the continued development and O&M of these systems. MCAS and other tools will require routine IT support through the use of systems administrators, log analysis specialists, and technical writers to provide reliable systems operations, ad-hoc reporting, change management, documentation, performance monitoring, contingency planning, user management and user support throughout the life of the MCAS system. The FBI anticipates using virtual interfaces to maintain travel and training costs at FY 2022 levels. Software and hardware funding are fully recurred to leverage emerging technologies in the outyears. Annualizations are requested pursuant to the FBI's outyear mission requirements.

Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2023 (net change from 2022)	FY 2024 (net change from 2023)
Current Services	2,142	1,006	2,016	$378,719	$79,694	$458,413	N/A	N/A
Increases	155	52	78	$32,897	7,103	$40,000	($1,040)	$10,719
Grand Total	**2,279**	**1,058**	**2,094**	**$411,616**	**$86,797**	**$498,413**	**($1,040)**	**$10,719**

Item Name: **Counterintelligence**

Strategic Goals: 1, 3, 4
Strategic Objectives: 1.1, 1.2, 1.3, 3.1, 4.1, 4.2
Budget Decision Units: All
Organizational Programs: Counterintelligence, Operational Technology

Program Increase: Positions 28 Agt 0 FTE 14 Dollars $18,792,000 ($12,369,000 non-personnel)

Description of Item

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

Item Name: **TFO Body Worn Cameras (BWC)**

Strategic Goals: 3
Strategic Objectives: 3.1, 4.1
Budget Decision Unit: Criminal Enterprise/Federal Crimes
Organizational Programs: TFO Body Worn Cameras (BWC)

Program Increase: Positions 0 Agt 0 FTE 0 Dollars $6,208,000 (all non-personnel)

Description of Item

The FBI requests $6,208,000 annually to provide software and video storage to store data and video from the body worn cameras (BWCs) of Federally deputized Task Force Officers (TFOs). This funding will allow the FBI to support storage of BWC video for TFOs whose parent agency mandates the use of BWCs while they serve on Federal task forces.

Justification

The Department announced in October 2020 that DOJ "will permit state, local, territorial, and tribal task force officers to use body worn cameras on Federal task forces around the nation. The Department's policy will permit Federally-deputized officers to activate a body worn camera while serving arrest warrants, or during other planned arrest operations, and during the execution of search warrants." The policy is the result of a pilot program launched by the Department in October 2019 and applies to the extent that a TFO's parent agency requires BWC use by its officers during Federal task force operations.

Funding will allow the FBI to support the TFO and the TFO's parent agency by providing data and video storage software and capacity for some of the TFO's BWC video while the TFO is serving on a Federal task force directed by the FBI. Video storage is one of the costliest aspects of a BWC program, and Federal support for these storage requirements will allow the FBI to maintain and increase partner agency participation in the Department's task forces.

The Department's policy on Use of Body Worn Cameras by Federally Deputized Task Force Officers applies to the extent that a TFO's parent agency requires BWC use by its officers during Federal task force operations. This funding will not be used to purchase camera hardware, as the hardware will be provided by the parent agency.

As outlined in the Department's policy, "all TFO BWC recordings made during Federal task force operations, including such recordings retained by the TFO's parent agency and/or in the possession of any third party engaged by the parent agency to store or process BWC recordings, shall be deemed Federal records of the Department and the Federal agency sponsoring the task force pursuant to the Federal Records Act." Furthermore, the policy directs that "TFO BWC recordings are controlled by, and the property of, the Department and will be retained and managed by the Federal agency sponsoring the task force. The Federal agency sponsoring the task force is responsible for considering requests to release TFO BWC recordings."

Data storage as it relates to the retention of BWC video for FBI TFO operations requires infrastructure improvements to meet mission needs and legal requirements. The FBI intends to use the enhancement improvements to accommodate technical and contractor support.

The FBI will use the funding enhancement on the following items:

Cloud Storage: The FBI requests $1,760,000 for Cloud Storage. The cost for cloud storage is divided into four elements that include hot storage, archive storage, compute, and bandwidth to support immediate and long-term requirements.

Software: The FBI requests $953,000 for the purchase of software to accommodate the tracking of service tickets for those involved in the TFO pilot program, audio/video enhancing software to respond to discovery and FOIA requests, compliance, cybersecurity and licenses to integrate with FBI enterprise systems.

Field Bandwidth Enhancement: The FBI requests $270,000 to support increased bandwidth to field office sites participating in the TFO BWC pilot program.

Contractor Labor Costs: The FBI requests $3,225,000 for contractor support to achieve accreditation for the storage of BWC footage. The FBI will rely on contractor labor support providing Information System Security Officer expertise. Additionally, the FBI will utilize funding for multiple software developers, system administrators, and forensic audio/visual personnel to manage the storage environment, integration into FBI enterprise systems and redaction services.

Impact on Performance

The FBI maintains over 750 task forces across its criminal, counterterrorism, counterintelligence, and cyber programs, composed of federal, state, local, and tribal partners. These partners provide critical intelligence and serve as an operational force-multiplier in support of the FBI's highest investigative priorities – keeping the American public safe. The FBI's criminal task forces (e.g., Safe Streets, Child Exploitation, Public Corruption, Organized Crime) alone account for over 550 task forces, comprised of over 3,200 full-time TFOs and nearly 1,200 task force participants from over 1,400 state, local, and tribal agencies. As more state and local jurisdictions implemented legislative requirements for their LE agencies to use BWCs, FBI TFOs were placed in a difficult position in which they could be out of compliance with their home agency policies by not wearing BWCs when conducting federal operations. The FBI successfully participated in the Department's pilot program launched in October 2019 and continues to work with state and local partners to fully implement the Department's formal TFO BWC policy issued in October 2020. The Department's TFO BWC policy allows the flexibility to accommodate partners and ensure participation, regardless of current or future state and local mandates. Development of storage and software for TFO BWC footage will assist the FBI in implementing the Department's TFO BWC policy and ensure proper management of and access to data collected.

Furthermore, the Department has provided numerous grants and support for state and local LE agency use of BWCs as part of the Department's *Strategic Goal 4: Uphold the rule of law and integrity in the proper administration of justice*. This additional funding for storage of BWC footage will enable the FBI to better implement the Department's TFO BWC policy; maintain flexibility with state, local, and tribal partners, and assist partners with consistent application of BWC policies. The FBI is committed to supporting our state, local, and tribal partners to increase transparency and accountability of LE in their local communities.

Funding

Base Funding

FY 2020 Enacted				FY 2021 Enacted				FY 2022 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

Personnel Increase Cost Summary

Type of Position/Series	Positions Requested	Annual Costs per Position ($000)			FY 2022 Request ($000)	Annualizations ($000)	
		1st Year Adjusted Cost	2nd Year Adjusted Cost	3rd Year Full Cost (Modular)		FY 2023 (net change from 2022)	FY 2024 (net change from 2023)
Special Agent, Field							
Intelligence Analyst							
Computer Scientist							
Data Analyst							
Digital Operations Specialist							
Staff Operations Specialist							
Total Personnel	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**

Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	FY 2022 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2023 (net change from 2022)	FY 2024 (net change from 2023)
Cloud Storage	$1,760			$0	$0
Software	$953			$0	$0
Field Enhancement	$270			$0	$0
Contract Support	$3,225			$0	$0
Total Non-Personnel	**$6,208**	**N/A**	**N/A**	**$0**	**$0**

Justification for Non-Personnel Annualizations

The organization maintains funding levels to preserve operational readiness and support emergent initiatives. Infrastructure requirements to implement and maintain a Body Worn Camera (BWC)

program will continue. As such, the FBI's $6,208,000 non-personnel increases for IT software, services, and network bandwidth improvements are expected to recur in FY 2023 and FY 2024. These services will be essential to retain BWC video, manage the service ticket system, comply with discovery and FOIA requests, and ensure appropriate security, accreditation, and functionality to support the BWC program. Recurred funding also will ensure the FBI can leverage emerging technologies.

Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2023 (net change from 2022)	FY 2024 (net change from 2023)
Current Services	0	0	0	$0	0	0	N/A	N/A
Increases	0	0	0	$0	$6,208	$6,208	$0	$00
Grand Total	**0**	**0**	**0**	**$0**	**$6,208**	**$6,208**	**$0**	**$0**

Item Name: **Cybersecurity**

Strategic Goals: 1, 3, 4
Strategic Objectives: 1.1, 1.2, 1.3, 3.1, 3.2, 4.1, 4.2
Budget Decision Units: All
Organizational Programs: Information Technology

Program Increase: Positions 22 Agt 0 FTE 11 Dollars $15,230,000 ($12,832,000 non-personnel)

Description of Item

The President's FY 2022 discretionary request identified a cyber reserve of $750 million. The FY 2022 President's Budget allocates these resources to nine agencies that were significantly impacted by the SolarWinds incident, one of which is the Department of Justice. The purpose of the funding is to address immediate response needs and does not focus on wholesale replacement of IT systems at this time. The funding request targets critical cybersecurity needs at these nine agencies which prioritizes basic cybersecurity enhancements, including: cloud security, Security Operations Center (SOC) enhancements, encryption, Multi-Factor Authentication (MFA), increased logging functions, and enhanced monitoring tools. Each agency's maturation levels were reviewed in these areas to determine the most critical gaps that require additional funding.

The FBI requests 22 positions and $15,230,000 ($12,832,000 non-personnel) to enhance its cybersecurity posture and cybersecurity threat assessment program. FBI data, including national security data, is vulnerable to external cyber and insider threat attacks. Current tools are not capable of fully monitoring the FBI's numerous enterprise systems, and are not prepared for the ever-changing technological landscape, including increased use of cloud computing and mobile platforms. The FBI must invest in people and tools to enhance its cybersecurity posture to meet federal mandates for a secure IT enterprise.

The requested resources will be used to enhance the following areas:

- **Cybersecurity Posture:** The FBI requests 20 positions and $14,012,000 ($11,832,000 non-personnel) to ensure robust cybersecurity through targeted investments in engineering, operations, risk management, and modernization.
- **Cybersecurity Threat Assessment Program:** The FBI requests two positions and $1,218,000 ($1,000,000 non-personnel) to proactively address cybersecurity vulnerabilities and the growing cyber threat posed by groups exploiting technology to breach the FBI's technical systems and networks, with the intent to cause harm to the FBI mission and reputation.

Justification

Threat Summary: To keep pace with today's emerging threats, the FBI must make cybersecurity improvements to ensure a more secure infrastructure and limit vulnerabilities posing a threat to the FBI mission.

Asset Management: Industry reports that 60 percent of breaches in 2019 involved unpatched vulnerabilities. The FBI maintains over 800 systems with a vast number of interconnections and interdependencies and such breaches constitute a high risk to the FBI's cybersecurity posture. The FBI

must use reporting and server ownership information to identify, communicate and address non-compliance for remediation. The FBI assesses, based on its current cybersecurity posture, that it must invest additional resources in efforts to combat potential breaches and vulnerabilities.

Security & Compliance: There are currently more than 75 FBI IT systems requiring security assessments. The FBI has over 115 cloud services that require security review to ensure they are configured in accordance with cloud service providers best security practices. Without an automated means of validating these settings and services, the FBI risks possible data compromise as it migrates IT systems into cloud environments.

Agility: With the number of cyber-attacks against the FBI increasing every year, sophisticated identification and prevention are required to differentiate threats from benign network noise. Cyber threats constantly evolve, and the FBI's cybersecurity defense must evolve with it. The FBI must keep up with the new technologies threatening its IT infrastructure and must deploy new defensive tools to keep pace with innovation and technological advances in the cyber environment.

Cybersecurity Posture: 20 positions and $14,012,000 ($11,832,000 non-personnel)

The FBI is requesting enhancements to protect IT assets from cyberattacks and insider threats. The cyber defense landscape is constantly changing, and new threat technologies and techniques are constantly emerging. Better systems are required to address the current gaps in monitoring, incident response, and vulnerability mitigation. The FBI is requesting 20 positions to monitor, develop, and create compliance procedures.

Engineering: $6,332,000 (all non-personnel)

The FBI requests $6,332,000 (all non-personnel) to address foundational IT infrastructure re-engineering requirements to keep pace with cybersecurity technologies. This IT engineering program will deploy technologies across enterprise computer networks and mobile device platforms to defend against cyber and insider threats. It will also provide technologies for the FBI's cyber defenders to prevent and respond to attacks against the FBI's infrastructure. Additionally, this funding will support the FBI's patching program to prevent the exploitation of outdated systems.

Specifically, the requested resources will be used to enhance the following areas:

- $4,332,000 for expanded monitoring of FBI IT assets to deploy technologies to support increased visibility into the FBI's existing information technology assets and emerging technologies such as cloud and mobility platforms.
- $2,000,000 for an asset management system to provide expanded insight into, accountability over, and centralized vulnerability management coverage over FBI IT assets.

Information Security Workforce: 13 positions and $1,417,000 (all personnel)

The FBI requests 13 Information Security professional positions to effectively address the FBI's growing inability to effectively respond to critical Information System (IS) security incidents. The creation of government Information Security positions will be cost-effective and will create a consolidated and streamlined information systems program management framework to support FBI operations.

The IS professionals will serve in three primary functional areas:

- **Information Systems Security Operations (ISSO):** The FBI requests four positions to ensure the day-to-day implementation, oversight, continuous monitoring, and maintenance of the security configuration, practices, and procedures for each IS. The staff will ensure that selected security controls are implemented and operating as intended during all phases of the IS lifecycle, conduct required IS vulnerability scans according to risk assessment parameters and develop Plans of Actions and Milestones (POA&Ms) in response to reported security vulnerabilities.

- **Information Systems Security Management (ISSM):** The FBI requests five positions to ensure that FBI ISs are operated, maintained, and disposed of in accordance with the internal security policies and practices outlined in the approved Security Assessment and Authorization (SAA) package, and provide baseline security controls to system owners. The staff will initiate, coordinate, and recommend (to the FBI Authorizing Official) all Interconnection Security Agreements (ISAs), Memoranda of Understanding (MOUs), and Memoranda of Agreement (MOAs) that permit the interconnection of an FBI IS with any non-FBI or joint-use IS.

- **Information System Security Engineering (ISSE):** The FBI requests four positions to enhance the organization's ability to identify information protection needs for an IS and Network Environment, develop and implement security designs for new or existing network systems, ensure the design of hardware and operating systems are appropriate, develop and implement security designs for new or existing network system(s) and software applications, and adequately address cybersecurity requirements for the IS and Network Environment. The staff will provide the expertise to ensure that network systems design supports the incorporation of FBI directed cybersecurity vulnerability solutions.

Cybersecurity Incident Response Program Management: 4 positions and $1,436,000 ($1,000,000 non-personnel)

The FBI requests four positions and $1,436,000 ($1,000,000 non-personnel) to enhance the FBI's program management over its incident response functions under the FBI's Chief Information Security Officer (CISO). While the FBI's Enterprise Security Operations Center (ESOC) is primarily responsible for cybersecurity incident response, the FBI's CISO is responsible for managing that function and reporting the FBI's compliance with reporting requirements from the US Department of Justice and the Office of the Director of National Intelligence. The enhancement will strengthen the FBI's ability to manage its cybersecurity program without having to remove ESOC personnel from their core critical incident response mission.

Operations and Forensic Analysis: 3 positions and $2,827,000 ($2,500,000 non-personnel)

The FBI requests three positions and $2,827,000 ($2,500,000 non-personnel) to enhance the ESOC. ESOC is required to protect FBI IS by monitoring for, detecting, responding to, mitigating, and reporting on cybersecurity threats that could potentially compromise FBI IS, data, and personnel. Cybersecurity threats are evolving and growing therefore tools are needed to ensure FBI systems are protected from external, internal, and foreign threats. The enhancement would allow ESOC to address mission-critical gaps to protect FBI systems and data. This request will provide substantial improvements to all areas of the FBI's cybersecurity posture.

This will support mission-critical workflows by providing ESOC with support to meet federally mandated objectives, namely the government employee oversight over ESOC's enhanced operations and digital forensic analysis teams. The FBI requests 3 Information Technology (IT) Specialists to fulfill this requirement.

The FBI requests $2,500,000 (all non-personnel) to provide additional support for ESOC's daily operations and post-incident digital forensic analysis functions and modern tools for both ESOC operations and endpoint detection.

EDR and SOC Tool Modernization: $2,000,000 (all non-personnel)

The FBI requests $2,000,000 (all non-personnel) to provide industry standard hardware and services needed to protect FBI endpoints (including mobile devices used by FBI personnel), perform remote analysis, collect data from potentially compromised systems, process and analyze investigative data, disassemble potentially compromised systems and transfer the unit's mobile activity data into a GovCloud.

Cybersecurity Threat Assessment Program: 2 positions and $1,218,000 ($1,000,000 non-personnel)

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

The program is comprised of two teams that serve different functions to collaboratively address enterprise vulnerabilities.

Advanced Security Assessment Team: The FBI requests two Information Technology Specialists (ITS) positions and $1,218,000 ($1,000,000 non-personnel) to continuously assess and enhance the security posture of the FBI through threat-driven, cybersecurity technical operations based on adversarial tools, techniques, and procedures (TTP) that are realistic, relevant, and identify true risk to FBI missions.

The primary purpose of the Advanced Security Assessment Team (Blue and Red) is to proactively assess the overall information security and cybersecurity management of an organization or system beyond vulnerability scans. The Blue Team assessments focus on a collaborative approach intended to determine the overall effectiveness of the personnel and processes used to secure information technology assets, while the Red Team operations focus on an approach based on employing potential tools, techniques, and processes used by adversaries to identify the risks to the organization's most mission-critical and mission-essential elements. This request will provide substantial improvements to all areas of the FBI's cybersecurity posture.

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

Impact on Performance

With this enhancement to its cybersecurity program, the FBI will gain a clearer view of the current state of its cybersecurity, increasing its understanding of cyber risk and allowing for the prioritization of mitigation efforts, while also validating the effectiveness of current security controls. Investing in transformative technologies will allow the FBI to identify high-risk vulnerabilities and gaps in security that may otherwise go unidentified using less advanced methods. Further, the FBI will be able to proactively identify a compromise from insider threats or external adversaries in coordination with the ESOC and the Insider Threat Office.

Without the necessary enhancements to address engineering requirements for the many assets that the FBI maintains, monitoring and analysis to maintain and protect sensitive data on all FBI asset inventory will be limited. Further, for the FBI to adhere to the federally mandated Federal Information Security Modernization Act (FISMA) security requirements for its assets, it must automate and standardize the full lifecycle development process for systems and applications by migrating towards a mature Security Development Operations (SecDevOPS) model and employing state of the art tools, such as IRM and Mobile Application Security Vetting, to support the Security Assessment and Authorization process.

Funding

Base Funding

FY 2020 Enacted				FY 2021 Enacted				FY 2022 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
29	1	27	$57,944	45	2	43	$77,758	45	2	43	$79,446

Personnel Increase Cost Summary

Type of Position/Series	Positions Requested	Annual Costs per Position ($000)			FY 2022 Request ($000)	Annualizations ($000)	
		1st Year Adjusted Cost	2nd Year Adjusted Cost	3rd Year Full Cost (Modular)		FY 2023 (net change from 2022)	FY 2024 (net change from 2023)
Information Technology Specialists	22	$109	$92	$146	$2,398	$2,024	$814
Total Personnel	**22**	**$109**	**$92**	**$146**	**$2,398**	**$2,024**	**$814**

Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	FY 2022 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2023 (net change from 2022)	FY 2024 (net change from 2023)
Cybersecurity Posture	$11,832			($1,000)	$0
Cybersecurity Threat Assessment Program	$1,000			$0	$0
Total Non-Personnel	**$12,832**	**N/A**	**N/A**	**($1,000)**	**$0**

Justification for Non-Personnel Annualizations

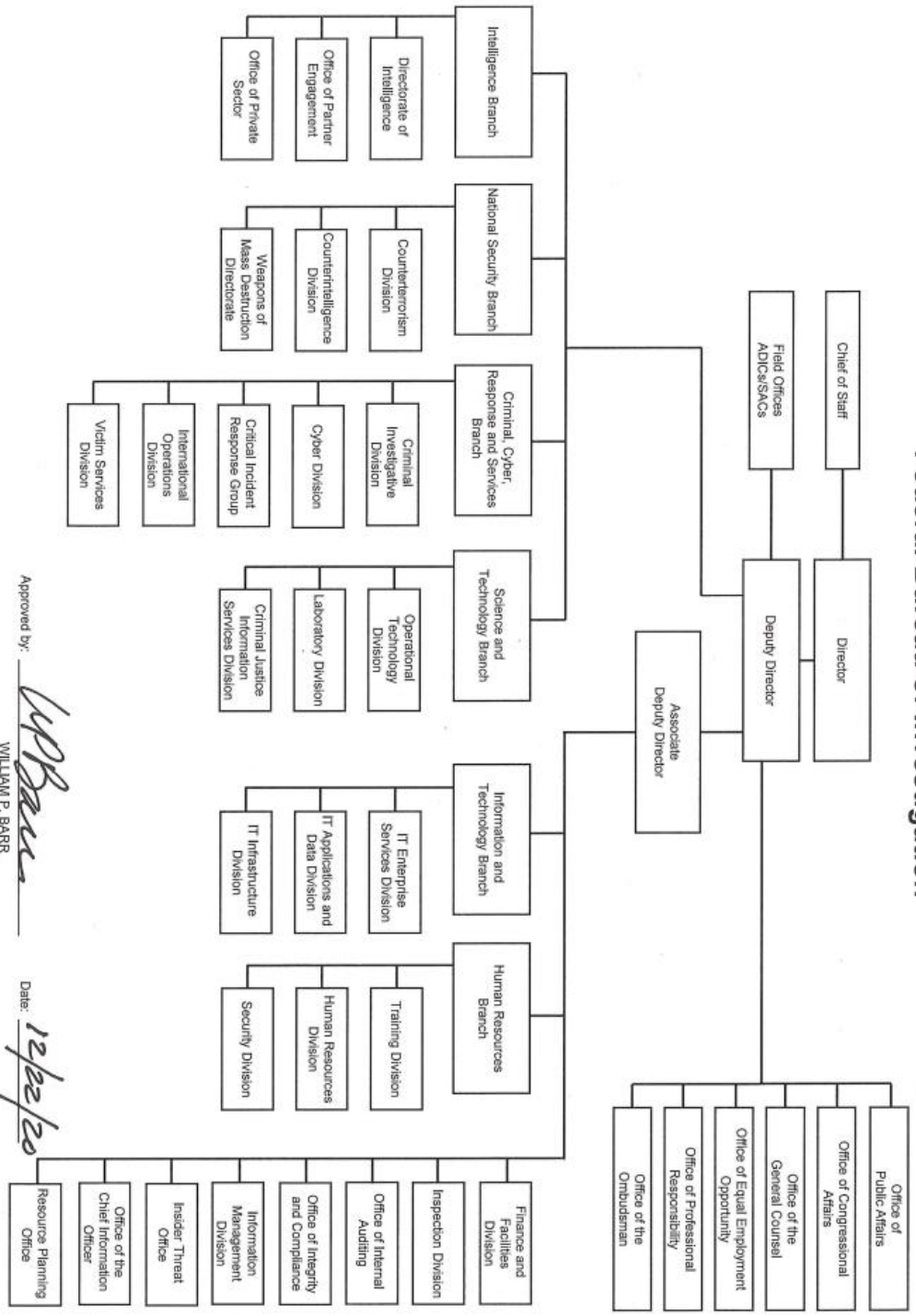
The FBI will recur $11,832,000 annually to support IT software, contract services, and IT maintenance to meet federal mandates for a secure IT enterprise. Contract services, software, and IT maintenance costs will be maintained to continue mission support. Initial hardware investments will not be repeated in the outyears, reducing the annualized costs by $1,000,000.

Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2023 (net change from 2022)	FY 2024 (net change from 2023)
Current Services	45	2	43	$11,354	$60,092	$79,446	N/A	N/A
Increases	22	0	11	$2,398	$12,832	$15,230	$1,024	$814
Grand Total	**67**	**2**	**54**	**$13,752**	**$80,924**	**$94,676**	**$1,024**	**$814**

VI. Exhibits

A. Organizational Chart



K. Status of Congressionally Requested Studies, Reports, and Evaluations

Status of Congressionally Requested Studies, Reports, and Evaluations
Federal Bureau of Investigation
Salaries and Expenses

1. The FY 2021 Conference Report directs the FBI to submit a report on field offices' capacity to investigate all crimes of slavery and human trafficking in their jurisdiction. The report should further detail any additional resources that have been provided to those field offices for these efforts.

2. The FY 2021 Conference Report directs the FBI to report on efforts to investigate and support DOJ criminal prosecution of serious human rights crimes, including genocide, torture, use or recruitment of child soldiers, war crimes, and other crimes committed by serious human rights violators, and continue to comply with direction in the explanatory statement accompanying Public Law 116-93, regarding the International Human Rights Unit, the Human Rights Violators and War Crimes Center, and FBI field office training.

3. The FY 2021 Conference Report directs the FBI to prepare an updated report on security advisory opinion (SAO) processing, as required by the explanatory statement accompanying Public Law 116-93, to include any classified data.

4. The FY 2021 Conference Report directs the FBI to provide a report on which databases, including N-DEx, are used for point-of-contact (POC) initiated firearm background checks; what barriers, if any, prevent incorporating N-DEx into POC background check processes, and how to overcome them; and how to raise State and local awareness of N-DEx.

5. The FY 2021 Conference Report directs the FBI to describing how the FBI is addressing each recommendation in the OIG report "Audit of the Handling of Firearms Purchase Denials Through the National Instant Criminal Background Check System" (Audit Division 16-32). If the FBI is not implementing a recommendation, the report shall indicate whether the FBI intends to do so, and if not, the justification for not pursuing the recommended course of action. The report shall also identify any changes made to the Standard Operating Procedures to better process NICS inquiries within the three-day time period. All unclassified data shall be publicly released by the FBI.

6. The FY 2021 House Senate Report directs the FBI to report on efforts to work with LE agencies in the five U.S. territories to provide training, technical assistance, and NIBRS subject matter expertise to ensure it can collect and publish crime statistics from these jurisdictions.

7. The FY 2021 House Report directs the FBI to report on efforts to train all Field Offices on how to detect and investigate crimes committed by serious human rights violators, and to report on efforts to increase the number of human rights investigations.

8. The FY 2021 Conference Report directs the FBI to report on the number of racially-motivated violent extremist incidents in fiscal years 2016 through 2020 that required surveillance, investigation, and prosecution of white supremacist activity or racially motivated domestic

terrorism associated with white supremacist ideology, and include, if available, incidents in which the FBI deferred to State or local authorities.

9. The FY 2021 Senate Report directs the FBI to provide a report describing its methods for collecting National Use of Force data, suggestions for increasing participation by LE agencies, and any associated resources needs.

10. The FY 2021 Senate Report directs the FBI to report on efforts of the Human Rights Unit, participation in the Human Rights Violators and War Crimes Center, and training to all field offices.

11. The FY 2021 Senate Report directs the FBI to update the FY 2020 report on Security Advisory Opinion (SAO) processing, including the publication of unclassified data.

12. The FY 2021 Senate Report directs the FBI to provide a report, with detailed explanations, of how the FBI is addressing each of the recommendations included in the OIG report entitled 'Audit of the Handling of Firearms Purchase Denials Through the National Instant Criminal Background Check System'' (Audit Division 16–32). If the FBI is not implementing a specific recommendation from the report, the FBI shall explain whether it intends to implement the specific recommendation, and if not, the justification for not pursuing the recommended course of action. The report shall also identify any changes to the Standard Operating Procedures the FBI has made to better process NICS inquiries within the three-day time period.

13. The FY 2021 Senate Report directs the FBI to develop plans for and report on a pilot C–UAS training program for State and local LE personnel from both urban and rural areas.

L. Senior Executive Service Reporting

	Staffing (as of 12/31/20)		Awards (as of 12/31/20)		SES Removals (as of 12/31/20)		
SES Pay Band	**Established Positions**	**Onboard Personnel**	**Number of Awards**	**Amount of Awards**	**Less Than Fully Successful Performance**	**Reduction in Force**	**Other Reasons**
$131,239 - $197,300	328	294	209	$4,083	1	0	N/A

NOTE: Note: OPM no longer sets basic rates of pay for members of the SES. Basic SES pay for an agency with a certified performance management system, which DOJ has, is between $131,239 and $197,300 for 2020.

VII. CONSTRUCTION

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

The FBI requests $61,895,000 in the Construction account for the SWE program and safety and strategic improvements to the Quantico Campus. The FBI and DOJ also look forward to working with OMB and Congress to secure the funding required for a new FBI Headquarters building.

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

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

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

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

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

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

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

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

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

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

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

FBI Headquarters: Built in 1975 to support 2,000 personnel, the FBI HQ infrastructure, including mechanical, electrical, and life safety systems, require critical repairs or replacement to safely support the current capacity of 5,500 FBI personnel. The FBI continues to plan and innovate within the J. Edgar Hoover (JEH) Building to find efficiencies that sustain its critical operations despite the building's failing infrastructure as the FBI awaits further discussion on the potential for a new HQ location.

Appropriations Language and Analysis of Appropriations Language

Appropriations Language for Construction

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

Analysis of Appropriations Language

No substantive change.

Item Name: **Safety and Strategic Improvements to the Quantico Campus**

Strategic Goals: 1, 3, 4
Strategic Objectives: 1.1, 1.2, 1.3, 3.1, 4.4
Budget Decision Units: All
Organizational Program: Facilities and Logistics Services

Program Increase: Positions 0 Agt 0 FTE 0 Dollars $10,000,000 (all non-personnel)

Description of Item

The FBI requests $10,000,000 (all non-personnel) for strategic construction at its Quantico campus in support of the FBI's evolving mission and the resulting training needs. This request supports the replacement of critical operational support facilities that will increase the safety of students and employees and will be used to support FBI operations and those of its LE partners now and into the future.

Justification

The FBI's 49-year-old Quantico campus is home to five major FBI Headquarters divisions encompassing 78 facilities across approximately 2,500,000 square feet of administrative, laboratory, training, industrial, and support facilities. Over the years, the Quantico campus has grown from supporting a single FBI entity and mission – the Training Division – to a multi-tenant/multi-mission venue. In addition to housing the FBI Academy and serving as a national training asset, Quantico also houses key operational entities, including the Hostage Rescue Team, the FBI Laboratory Division, and the FBI's operational technology program. Today, the Quantico campus supports approximately 3,200 personnel and accommodates about 13,500 students and 20,000 visitors annually.

As the mission and work of the FBI have evolved to keep up with new technologies and shifts in domestic and international criminal and terrorist activities, its approach to training and mission support has followed. The FBI's foremost training offering, the Basic Field Training Course (BFTC) for new agents and intelligence analysts, was expanded to allow for an increase in the training of new personnel, placing a strain on Quantico's aging facilities. For Quantico to remain the crown jewel of LE training, the FBI must revitalize aging and failing infrastructure, and make continual and sustained investments in master-planned capital improvements.

Safety and Maintenance Improvements to Critical Mission Support Space: $10,000,000 (all non-personnel)

The FBI requests $10,000,000 of recurring construction funds to replace numerous dilapidated facilities that have exceeded their useful life.

As the FBI has expanded its footprint at Quantico, many temporary structures have been incorporated into the FBI's campus master plan to provide critical mission support space for expanding operations. These temporary buildings were constructed with materials and support equipment that typically have a lifespan of 10 to 20 years, and many of these buildings are now over 30 years old. Several modular trailers are falling apart, some do not have fire systems, and some do not possess adequate fresh air to

inhibit mold and mildew growth. This creates an unhealthy and unsafe work and training environment that is not conducive to maintaining a world-class training academy.

The FBI requests recurring funding of $10,000,000 to address ongoing, phased permanent replacement of numerous worn-out facilities. The facilities to be replaced are modular trailers, large fabric "tent" buildings, and relocatable masonry buildings put in place from the 1980s to the 2000s to quickly support the FBI's expanding operational requirements, and that have remained well past their useful (and safe) lives. For example, the cost to replace the air conditioning in one of these temporary buildings exceeds the value of the building itself. As a result, when failures occur, high-cost emergency system replacements that cause major interruptions to FBI operations are required.

By having an additional dedicated $10,000,000 to replace numerous antiquated Quantico facilities, the FBI will not be limited to the existing $2,000,000 in the construction account. The current funding level discourages preventative planning and can result in interrupted operations when critical failures inevitably occur. With additional funding, the FBI can deploy a long-term plan for Quantico end-of-life facility replacements.

HRT Modular Trailer: Deteriorated classroom

Modular Trailer: Rotting from the floor up

Precast Concrete Building: Structural Failure

Effects of Degradation: Moisture penetration and Black Mold

Impact on Performance

Quantico is the world's premier LE research and learning center and as such requires an investment of resources for its sustainment and enhancement. Without this investment, Quantico will not be able to adequately host training classes and other scenarios that prepare FBI agents, analysts, and global partners to counter the evolving criminal and national security threats of the 21st century, while keeping students and workers safe.

The FBI's Quantico complex has an immediate and urgent need for projects that require security-related improvements such as relocating the central shipping and receiving facility from the middle of new agent training to outside the security perimeter of the FBI Quantico complex. Other projects include life and safety improvements that would move a firearms range support (gunsmithing) function from below the cafeteria to the firearms ranges. The replacement of temporary buildings with permanent facilities will ensure the required safety systems and mission support amenities will be available to support operational requirements and ensures the FBI remains in compliance with current building code.

Funding

Base Funding

FY 2020 Enacted				FY 2021 Enacted				FY 2022 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
0	0	0	$2,000	0	0	0	$2,586	0	0	0	$2,000

Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	FY 2022 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2023 (net change from 2022)	FY 2024 (net change from 2023)
Construction	$10,000	N/A	N/A	$10,000	$10,000
Total Non-Personnel	**$10,000**	**N/A**	**N/A**	**$10,000**	**$10,000**

Justification for Non-Personnel Annualizations

The $10,000,000 will recur annually to address the ongoing, phased permanent replacement of numerous worn-out facilities on the FBI's Quantico campus.

Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2023 (net change from 2022)	FY 2024 (net change from 2023)
Current Services	0	0	0	$0	$2,000	$2,000	N/A	N/A
Increases	0	0	0	$0	$10,000	$10,000	$0	$0
Grand Total	**0**	**0**	**0**	**$0**	**$12,000**	**$12,000**	**$0**	**$0**

VIII. GLOSSARY

ACTP	Accelerated Cyber Training Program
ADIC	Assistant Director in Charge
Agt	Special Agent
AOR	Area of Responsibility
APB	Advisory Policy Board
ATB	Adjustments to Base
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
AWFC	Analytic Writing for Fusion Centers
BRF	Ballistics Research Facility
BTC	Biometric Technology Center
BWC	Body Worn Camera
C2	Command and Control
CAR	Criminal Answer Required
CARD	Child Abduction Rapid Deployment Team
CARES	Coronavirus Aid, Relief and Economic Security Act
CCRSB	Criminal, Cyber, Response, and Services Branch
CD	Counterintelligence Division
CEFC	Criminal Enterprises and Federal Crimes
CHRI	Criminal History Record Information
CHS	Confidential Human Source
CI	Counterintelligence
CIA	Central Intelligence Agency
CID	Criminal Investigative Division
CIP	Computer Intrusion Program
CIRG	Critical Incident Response Group
CISO	Chief Information Security Officer
CJ	Criminal Justice
CJIS	Criminal Justice Information Services
CJS	Criminal Justice Services
CODIS	Combined DNA Index System
COL	Color of Law
CONUS	Continental United States
COOP	Continuity of Operations
CP	Counterproliferation
CPOT	Consolidated Priority Organization Target
CRC	Central Records Complex
CST	Child Sex Tourism
CT	Counterterrorism
CTAP	Cyber Threat Actor Program
CT/CI	Counterterrorism/Counterintelligence
CTD	Counterterrorism Division
C-UAS	Counter-Unmanned Aircraft Systems
CyD	Cyber Division
DHS	Department of Homeland Security
DI	Directorate of Intelligence

DIA	Defense Intelligence Agency
DNA	Deoxyribonucleic Acid
DOD	Department of Defense
DOJ	Department of Justice
DSAC	Domestic Security Alliance Council
DT	Domestic Terrorism
DTLI	Detect, Track, Locate, and Identify
DTO	Drug-trafficking Organizations
DTOS	Domestic Terrorism Operations Section
DU	Decision Unit
EAD	Executive Assistant Director
eDO	Electronic Departmental Order
EO	Executive Order
ESOC	Enterprise Security Operations Center
ETI	Enterprise Theory of Investigation
E-Tips	Electronic Tips
EUROPOL	European Union Agency for Law Enforcement Cooperation
EVoIP	Enterprise Voice over Internet Protocol
FACE	Freedom of Access to Clinic Entrance
FBI	Federal Bureau of Investigation
FFD	Facilities and Finance Division
FFL	Federal Firearms Licensee
FLP	Foreign Language Program
FO	Field Office
FOSP	Field Office Strategic Plan
FTE	Full-time Equivalent
FTTTF	Foreign Terrorist Tracking Task Force
FY	Fiscal Year
GCA	General Crimes Act
GPS	Global Positioning System
HDS	Hazardous Devices School
HIG	High-Value Detainee Interrogation Group
HQ	Headquarters
HRB	Human Resources Branch
HRD	Human Resources Division
HRT	Hostage Rescue Team
HRVWCC	Human Rights Violators and War Crimes Center
HUMINT	Human Intelligence
HVE	Homegrown Violent Extremists
IA	Intelligence Analyst
IAFIS	Integrated Automated Fingerprint Identification System
IB	Intelligence Branch
IC	Indian Country
IC	Intelligence Community
IC3	Internet Crime Complaint Center
ICS	Industrial Control Systems
ICSJU	Indian Country and Special Jurisdiction Unit

IDU	Intelligence Decision Unit
IHR	International Human Rights
IHRU	International Human Rights Unit
III/Triple I	Interstate Identification Index
IIR	Intelligence Information Reports
IINI	Innocent Images National Initiative
ILNI	Innocence Lost National Initiative
IMD	Information Management Division
INSD	Inspection Division
IntelSup	Intelligence for Supervisors
InTO	Insider Threat Office
IntroTel	Introduction to Intelligence
IOD	International Operations Division
IPM	Integrated Program Management
IPS	Interstate Photo System
IS	Information System
ISIS	Islamic State of Iraq and ash-Sham
ISSE	Information Systems Security Engineering
ISSM	Information Systems Security Management
ISSO	Information Systems Security Operation
IT	Information Technology
ITADD	IT Applications and Data Division
ITB	Information and Technology Branch
ITESD	IT Enterprise Services Division
ITID	IT Infrastructure Division
JCODE	Joint Criminal Opioid and Darknet Enforcement
JEH	J. Edgar Hoover Building
JTTF	Joint Terrorism Task Force
JWICS	Joint Worldwide Intelligence Communication System
KST	Known or Suspected Terrorist
LD	Laboratory Division
LE	Law Enforcement
LEEP	Law Enforcement Enterprise Portal
MCA	Major Crimes Act
MCAS	Malicious Cyber Actor System
MCN	Muscogee Creek Nation
MENACE	Mobile Encrypted Networks and Communications Exploitation
MLF	Money Laundering Facilitator
NCAVC	National Center for the Analysis of Violent Crime
NCIC	National Crime Information Center
NCIJTF	National Cyber Investigative Joint Task Force
NCITF	National Counterintelligence Task Force
NCJ	Non-Criminal Justice
NCMEC	National Center for Missing and Exploited Children
NCPC	National Counterproliferation Center
NCSC	National Counterintelligence and Security Center
NCTC	National Counterterrorism Center

N3G	NCIC 3rd Generation
N-DEx	National Data Exchange
NDIS	National DNA Index System
NGI	Next Generation Identification
NIBRS	National Incident-Based Reporting System
NICS	National Instant Criminal Background Check System
NIP	National Intelligence Program
NIPF	National Intelligence Priorities Framework
NITTF	National Insider Threat Task Force
NPPS	National Palm Print System
NSB	National Security Branch
NSPM	National Security Presidential Memorandum
NSSE	National Special Security Event
NSTA	National Security Threat Actor
NSTP	National Security Threat Program
NTOC	National Threat Operations Center
NTOS	National Threat Operations Section
NTP	National Threat Priority
NVTC	National Virtual Translation Center
OC	Oklahoma City
OCA	Office of Congressional Affairs
OCIO	Office of the Chief Information Officer
ODNI	Office of the Director of National Intelligence
OEEOA	Office of Equal Employment Opportunity Affairs
OGC	Office of the General Counsel
OIC	Office of Integrity and Compliance
OMB	Office of Management and Budget
OPA	Office of Public Affairs
OPE	Office of Partner Engagement
OPR	Office of Professional Responsibility
OPS	Office of Private Sector
OTD	Operational Technology Division
POC	Point of Contact
PPP	Paycheck Protection Program
PS	Professional Staff
PSC	Private Sector Coordinator
RA	Resident Agency
RAT	Recovery Asset Team
RBS	Rap Back Services
RF	Radio Frequency
RMDT	Racially Motivated Domestic Terrorism
RPO	Resource Planning Office
RV	Recreational Vehicle
S&E	Salaries and Expenses
SA	Special Agent
SAC	Special Agent in Charge
SAO	Security Advisory Opinion

SCADA	Supervisory Control and Data Acquisition
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCINet	Sensitive Compartmented Information Network
SEAR	Special Event Assessment Rating
SecD	Security Division
SecDevOPS	Security Development Operations
SID	State Identification Number
SIIG	Strategic Intelligence Issues Group
SIOC	Strategic Information Operations Center
SIP	Session Initiation Protocol
SLTT	State, Local, Tribal, and Territorial
SME	Subject Matter Expert
SOG	Special Operations Group
SRS	Summary Reporting System
SSA	Supervisory Special Agent
SSG	Special Surveillance Group
STB	Science and Technology Branch
SVP	Senior Vice President
SWE	Secure Work Environment
TAG	Transnational Anti-Gang Task Force
TCO	Transnational Criminal Organization
TD	Training Division
TDI	Technology and Data Innovation
TDY	Temporary Duty
TEDAC	Terrorist Explosive Device Analytical Center
TFO	Task Force Operator
TIE	Threat Intake Examiner
TIPS	Threat Intake Processing System
TOC	Transnational Organized Crime
TRP	Threat Review and Prioritization
TRPS	Ten Print Rap Sheet
TS	Top Secret
TSA	Transportation Security Administration
TSC	Terrorist Screening Center
TSDB	Terrorist Screening Data Base
TTL	Threat to Life
UAS	Unmanned Aircraft System
UCE	Undercover Employee
UCN	Universal Control Number
UCR	Uniform Crime Reporting
ULF	Unsolved Latent File
UNet	Unclassified Network
US	United States
USG	United States Government
USIC	United States Intelligence Community
VGSSTF	Violent Crime and Safe Streets Gang Task Forces

VSD	Victim Services Division
WCC	White Collar Crime
WMD	Weapons of Mass Destruction
WMDD	Weapons of Mass Destruction Directorate