Department of Justice

STATEMENT OF

CHRISTOPHER A. WRAY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
SUBCOMMITTEE ON COMMERCE, JUSTICE, SCIENCE AND RELATED AGENCIES
COMMITTEE ON APPROPRIATIONS
UNITED STATES SENATE

AT A HEARING ENTITLED
"FEDERAL BUREAU OF INVESTIGATION BUDGET REQUEST FOR FISCAL YEAR 2024"

PRESENTED
MAY 10, 2023

STATEMENT OF
CHRISTOPHER A. WRAY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
SUBCOMMITTEE ON COMMERCE, JUSTICE, SCIENCE AND RELATED AGENCIES
COMMITTEE ON APPROPRIATIONS
UNITED STATES SENATE

AT A HEARING ENTITLED
"FEDERAL BUREAU OF INVESTIGATION BUDGET REQUEST FOR FISCAL YEAR 2024"

PRESENTED
MAY 10, 2023

Good afternoon, Chairwoman Shaheen, Ranking Member Moran, and Members of the Subcommittee. Thank you for inviting me to appear before you today. I do so on behalf of the men and women of the Federal Bureau of Investigation ("FBI"), who tackle some of the most complex national security and criminal threats every day with perseverance, professionalism, and integrity – sometimes at the greatest of costs. I am extremely proud of their service and commitment to the FBI's mission and to ensuring the safety and security of communities throughout our nation. On their behalf, I would like to express my appreciation for the support you have given them in the past, ask for your continued support in the future, and pledge to be the best possible stewards of the resources you provide. I would like to begin by providing a brief overview of the FBI's FY 2024 budget request, and then follow with a short discussion of key threats and challenges that we face, both as a nation and as an organization.

FY 2024 Budget Overview

The FY 2024 budget request proposes a total of $11.4 billion in direct budget authority to carry out the FBI's national security, intelligence, criminal law enforcement, and criminal justice services missions. The request includes a total of $11.3 billion for Salaries and Expenses, which will support 37,312 positions (13,662 Special Agents, 3,215 Intelligence Analysts, and 20,435 professional staff), and $61.9 million for Construction. The request includes nine program enhancements under Salaries and Expenses totaling $196.0 million. These enhancements are proposed to meet critical requirements and close gaps in operational capabilities, including $63.4 million to enhance cyber investigative capabilities, $13.0 million to address escalating counterterrorism threats, $4.5 million to mitigate threats from foreign intelligence services, $27.2 million to enhance the FBI's cybersecurity posture and protect

internal networks, $14.9 million to combat violent crime, $53.1 million to address the increase in DNA collection and processing, $3.1 million to sustain secure communications platforms, $2.8 million to support infrastructure needs related to the use of Body Worn Cameras, and $14.1 million to begin to address executive order requirements for zero emission vehicles.

Key Threats and Challenges

Our nation continues to face a multitude of serious and evolving threats ranging from homegrown violent extremists to hostile foreign intelligence services and operatives, from sophisticated cyber-based attacks to internet facilitated sexual exploitation of children, from violent gangs and criminal organizations to public corruption and corporate fraud. Keeping pace with these threats is a significant challenge for the FBI. As an organization, we must be able to stay current with constantly evolving technologies. Our adversaries — terrorists, foreign intelligence services, and criminals — take advantage of technology, including the Internet and social media, to facilitate illegal activities, recruit followers, encourage terrorist attacks and other illicit actions, to spread misinformation, and to disperse information on building improvised explosive devices and other means to attack the U.S. The breadth of these threats and challenges are as complex as any time in our history. And the consequences of not responding to and countering threats and challenges have never been greater.

The support of this Committee in helping the FBI do its part in thwarting these threats and facing these challenges is greatly appreciated. That support is allowing us to establish strong capabilities and capacities to assess threats, share intelligence, leverage key technologies, and — in some respects, most importantly — hire some of the best to serve as Special Agents, Intelligence Analysts, and professional staff. We have built, and are continuously enhancing, a workforce that possesses the skills and knowledge to deal with the complex threats and challenges we face today — and tomorrow. We are building a leadership cadre that views change and transformation as a positive tool for keeping the FBI focused on the key threats facing our nation.

Today's FBI is a national security and law enforcement organization that uses, collects, and shares intelligence in everything we do. Each FBI employee understands that, to defeat the key threats facing our nation, we must constantly strive to be more efficient and more effective. Just as our adversaries continue to evolve, so, too, must the FBI. We live in a time of acute and persistent terrorist and criminal threats to our national security, our economy, and indeed our communities. These diverse threats underscore the complexity and breadth of the FBI's mission: to protect the American people and uphold the Constitution of the United States.

National Security

Top Terrorism Threats

Protecting the American people from terrorism—both international and domestic—remains the FBI's number one priority. The threat from terrorism is as persistent and complex as ever. The threats from international terrorism (IT), domestic terrorism (DT), and state-sponsored terrorism all remain at elevated levels, necessitating the need for continued investment and vigilance.

The greatest terrorism threat to our Homeland is posed by lone actors or small cells who typically radicalize online and look to attack soft targets with easily accessible weapons. We see these threats manifested within both Domestic Violent Extremists ("DVEs") and Homegrown Violent Extremists ("HVEs"), two distinct threats, both of which are located primarily in the United States and typically radicalize and mobilize to violence on their own. Individuals who commit violent criminal acts in furtherance of social or political goals stemming from domestic influences – some of which include racial or ethnic bias, or anti-government or anti-authority sentiments – are described as DVEs, whereas HVEs are individuals who are inspired primarily by global jihad but are not receiving individualized direction from Foreign Terrorist Organizations ("FTOs").

Domestic and Homegrown Violent Extremists are often motivated and inspired by a mix of social or political, ideological, and personal grievances against their targets, and more recently have focused on accessible targets to include civilians, law enforcement and the military, symbols or members of the U.S. government, houses of worship, retail locations, and mass public gatherings. Lone actors present a particular challenge to law enforcement and intelligence agencies. These actors are difficult to identify, investigate, and disrupt before they take violent action, especially because of the insular nature of their radicalization and mobilization to violence and limited discussions with others regarding their plans.

The top domestic terrorism threat we face continues to be from DVEs we categorize as Racially or Ethnically Motivated Violent Extremists ("RMVEs") and Anti-Government or Anti-Authority Violent Extremists ("AGAAVEs"). In May 2022, a RMVE in the United States conducted an attack in Buffalo, NY that resulted in the deaths of 10 innocent individuals. The number of FBI domestic terrorism investigations has more than doubled since the spring of 2020, and as of the end of fiscal year 2022, the FBI was conducting approximately 2,700 investigations within the domestic terrorism program. In addition to the cases conducted within the domestic terrorism program, the FBI was also conducting approximately 4,000 investigations within its international terrorism program in fiscal year 2022.

The FBI uses all tools available at its disposal to combat domestic terrorism. These efforts represent a critical part of the National Strategy for Countering Domestic Terrorism, which was released in June 2021, and which sets forth a comprehensive, whole of government approach to address the many facets of the domestic terrorism threat.

The FBI assesses HVEs are the greatest, most immediate international terrorism threat to the homeland. HVEs are people located and radicalized to violence primarily in the United States, who are not receiving individualized direction from FTOs but are inspired by FTOs, including the self-proclaimed Islamic State of Iraq and ash-Sham ("ISIS") and al-Qa'ida and their affiliates, to commit violence. An HVE's lack of a direct connection with an FTO, ability to rapidly mobilize without detection, and use of encrypted communications pose significant challenges to our ability to proactively identify and disrupt potential violent attacks. Recently, an HVE attacked three New York Police Department Officers using an edged weapon in New York City on New Year's Eve 2022.

The FBI remains concerned about the Taliban takeover of Afghanistan and the intent of FTOs, such as ISIS and al-Qa'ida and their affiliates, to carry out or inspire large-scale attacks in the United States. Despite its loss of physical territory in Iraq and Syria, ISIS remains relentless in its campaign of violence against the United States and our partners—both here at home and overseas. ISIS and its supporters continue to aggressively promote its hate-fueled rhetoric and attract like-minded violent extremists with a willingness to conduct attacks against the United States and our interests abroad. ISIS's successful use of social media and messaging applications to attract individuals is of continued concern to us. Like other foreign terrorist groups, ISIS advocates for lone offender attacks in the United States and Western countries via videos and other English language propaganda that have, at times, specifically advocated for attacks against civilians, the military, law enforcement and intelligence community personnel.

Al-Qa'ida maintains its desire to both conduct and inspire large-scale, spectacular attacks. Because continued pressure has degraded some of the group's senior leadership, we assess that, in the near term, al-Qa'ida is more likely to continue to focus on cultivating its international affiliates and supporting small-scale, readily achievable attacks in regions such as East and West Africa. Over the past year, propaganda from al-Qa'ida leaders continued to seek to inspire individuals to conduct their own attacks in the United States and other Western nations.

Iran and its global proxies and partners, including Iraqi Shia militant groups, continue to attack and plot against the United States and our allies throughout the Middle East. Iran's Islamic Revolutionary Guard Corps-Qods Force ("IRGC-QF") continues to provide support to militant resistance groups and terrorist organizations. Iran also continues to support Lebanese Hizballah and other terrorist groups. Hizballah has sent operatives to build terrorist infrastructures worldwide. The arrests of individuals in the United States allegedly linked to Hizballah's main overseas terrorist arm, and their intelligence collection and procurement efforts, demonstrate Hizballah's interest in long-term contingency planning activities here in the Homeland. Hizballah Secretary-General Hassan Nasrallah also has threatened retaliation for the

death of IRGC-QF Commander Qassem Soleimani. The willingness to seek retaliation exemplified in 2022, when the Department charged an Iranian national and member of the IRGC, working on behalf of the Qods Force, with a plot to murder a former national security advisor.

The terrorism threat continues to evolve, but the FBI resolve to counter that threat remains constant. As an organization, we continually adapt and rely heavily on the strength of our Federal, state, local, Tribal, territorial, and international partnerships to combat all terrorist threats to the United States and our interests. To that end, we use all available lawful investigative techniques and methods to combat these threats while continuing to collect, analyze, and share intelligence concerning the threat posed by violent extremists, in all their forms, who desire to harm Americans and U.S. interests. We will continue to share information and encourage the sharing of information among our numerous partners via our Joint Terrorism Task Forces across the country, and our Legal Attaché offices around the world. The FY 2024 Request includes an additional 43 positions (including 20 Special Agents and 23 professional staff) and $13.0 million to counter the increasing acts of domestic terrorism across the United States.

Additionally, countering the proliferation of weapons of mass destruction materials, technologies, and expertise, preventing their use by any actor, and securing nuclear and radioactive materials of concern also are top national security priority missions for the FBI. The FBI considers preventing, mitigating, investigating, and responding to WMD terrorism a "no-fail" mission because a WMD attack could result in substantial injuries, illness, or loss of lives, with significant social, economic, political and other national security consequences. The FBI employs a full range of capabilities, in collaboration with its Federal, state, local, tribal, territorial, and other partners, and synchronizes its efforts to leverage resources efficiently and to integrate complementary efforts in countering WMD terrorism.

Cyber

Throughout these last two years, the FBI has seen a wider-than-ever range of cyber actors threaten Americans' safety, security, and confidence in our digitally connected world. Cyber-criminal syndicates and nation-states continue to innovate and use unique techniques to compromise our networks and maximize the reach and impact of their operations, such as by selling malware as a service or by targeting vendors as a way to access scores of victims by hacking just one provider.

These criminals and nation-states believe that they can compromise our networks, steal our property, extort us, and hold our critical infrastructure at risk without incurring any risk themselves. In the last few years, we have seen—and have publicly called out—the People's Republic of China ("PRC"), the Democratic People's Republic of Korea ("DPRK"), and Russia for using cyber operations to target U.S. COVID-19 vaccines and research. We have seen the far-reaching disruptive impact a serious supply-chain compromise can have through the

SolarWinds-related intrusions, conducted by the Russian SVR. We have seen the PRC working to obtain controlled dual-use technology and developing an arsenal of advanced cyber capabilities that could be used against other countries in the event of a real-world conflict. As these adversaries become more sophisticated, we are increasingly concerned about our ability to detect and warn about specific cyber operations against U.S. organizations. One of the most worrisome facets is their focus on compromising U.S. critical infrastructure, especially during a crisis.

What makes things more difficult is that there is no bright line that separates where nation-state activity ends and cybercriminal activity begins. Some cybercriminals contract or sell services to nation-states; some nation-state actors moonlight as cybercriminals to fund personal activities; and nation-states are increasingly using tools typically used by criminal actors, such as ransomware.

So, as dangerous as nation-states are, we do not have the luxury of focusing on them alone. In the past year, we also have seen cybercriminals target hospitals, medical centers, educational institutions, and other critical infrastructure for theft or ransomware, causing massive disruption to our daily lives. Such incidents affecting medical centers in particular have led to the interruption of computer networks and systems that put patients' lives at an increased risk, at a time when America faces its most dire public health crisis in generations.

We have also seen the rise of an ecosystem of services dedicated to supporting cybercrime in exchange for cryptocurrency. The effect is that what were once unsophisticated criminals now have the tools to engage in destructive behavior—for example, deploying ransomware to paralyze entire hospitals, police departments, and businesses—and the means to better conceal their tracks. It is not that individual malicious cyber actors have become much more sophisticated, but they can more easily rent sophisticated capabilities.

We must make it harder and more painful for malicious cyber actors and criminals to carry on their malicious activities. The FBI, using its role as the lead Federal agency for threat response, with its law enforcement and intelligence responsibilities, works seamlessly with domestic and international partners to defend their networks, attribute malicious activity, sanction bad behavior, and take the fight to our adversaries overseas. We must impose consequences on cyber adversaries and use our collective law enforcement and intelligence capabilities to do so through joint and enabled operations sequenced for maximum impact. And we must continue to work with the Department of State and other key agencies to ensure that our foreign partners are able and willing to cooperate in our efforts to bring the perpetrators of cybercrime to justice or otherwise disrupt such perpetrators' activities.

An example of this approach is the coordinated international operation announced in April 2023 against Genesis Market, a criminal online marketplace offering access to data stolen from over 1.5 million compromised computers around the world containing over 80 million account access credentials. Genesis Market was also a prolific initial access broker (IAB) in the cyber crime world, providing criminals a user-friendly database to search for stolen credentials

so they could easily infiltrate a victim's computer. As part of this operation, law enforcement seized 11 domain names used to support Genesis Market's infrastructure pursuant to a warrant authorized by the US District Court for the Eastern District of Wisconsin. A total of 22 international agencies and 44 FBI field offices provided assistance to the FBI Milwaukee Field Office investigating the case. And on April 5, the US Department of the Treasury announced sanctions against Genesis Market.

In January 2023, the DOJ and FBI heralded the success of an FBI investigation against Hive ransomware. This impactful action spotlighted an operation that truly characterized how the FBI can assist during ransomware attacks and why timely reporting is key. Through unique access to decryption keys, the FBI was able to prevent $130 million in ransoms being paid to cyber criminals. This access allowed us to really gauge the amount of reporting to law enforcement from a single ransomware variant, which is rather dire: approximately 20-25% of Hive victims reported to some law enforcement entity. There are many more actions we can take and there's much more intelligence to be gleaned, but we need to know about it. We can put these actors out of business, but it requires everyone's help.

In total, we took over 1,000 actions against cyber adversaries in 2022, to include arrests, criminal charges, convictions, dismantlements, and disruptions, and enabled many more actions through our dedicated partnerships with the private sector, foreign partners, and with Federal, state, and local entities. We also provided thousands of individualized threat warnings and disseminated 70 public threat advisories by way of Joint Cybersecurity Advisories, FBI Liaison Alert System ("FLASH") reports, Private Industry Notifications ("PINs"), and Public Service Announcements ("PSAs")—many of which were jointly authored with other U.S. agencies and international partners.

With our partners in the interagency, we have been putting a lot of energy and resources into all those partnerships, especially with the private sector. We are working hard to push important threat information to network defenders, but we have also been making it as easy as possible for the private sector to share important information with us. For example, we are emphasizing to the private sector how we keep our presence unobtrusive in the wake of an incident; how we protect information that the private sector shares with us, including their identities. We are also committed to providing useful feedback and improving coordination with our government partners so that we are speaking with one voice. But we need the private sector to do its part, too. We need the private sector to come forward to warn us and our partners—and warn us quickly—when they see malicious cyber activity. We also need the private sector to work with us when we warn them that they are being targeted. The recent examples of significant cyber incidents—SolarWinds, Cyclops Blink, the Colonial pipeline incident—only emphasize what I have been saying for a long time: The government cannot protect against cyber threats on its own. We need a whole-of-society approach that matches the scope of the danger. There is no other option for defending a country where nearly all of our critical infrastructure, personal data, intellectual property, and network infrastructure sits in private hands.

In summary, the FBI is engaged in a myriad of efforts to combat cyber threats, from improving threat identification and information sharing inside and outside of the government to developing and retaining new talent, to examining the way we operate to disrupt and defeat these threats. We take all potential threats to public and private sector systems seriously and will continue to investigate and hold accountable those who pose a threat in cyberspace. The FY 2024 Request includes an additional 192 positions (including 31 Special Agents, 8 Intelligence Analysts, and 153 Professional Staff) and $63.4 million to enhance cyber information-sharing abilities and increase cyber tools and capacities. The Request also includes 4 positions and $27.2 million to help protect internal FBI networks.

Foreign Intelligence Threats

We see nations such as China, Russia, and Iran becoming more aggressive and more capable in their nefarious activity than ever before. These nations seek to undermine our core democratic, economic, and scientific institutions. They employ a growing range of tactics to advance their interests and to harm the United States. Defending American institutions and values against these threats is a national security imperative and a priority for the FBI.

With that, the greatest long-term threat to our nation's ideas, innovation, and economic security is the foreign intelligence and economic espionage threat from China. It's a threat to our economic security—and by extension—to our national security. The Chinese government aspires to reshape the international rules-based system to its benefit, with little regard for the democratic ideals that underpin it. The pursuit of these goals is often with little regard for international norms and laws.

When it comes to economic espionage, the PRC uses every means at its disposal against us, blending cyber, human intelligence, diplomacy, corporate transactions, and pressure on U.S. companies operating in China, to achieve its strategic goals to steal our companies' innovations. These efforts are consistent with China's expressed goal to become a national power, modernizing its military and creating innovative-driven economic growth.

To pursue this goal, China uses not only human intelligence officers, co-optees, and corrupt corporate insiders, but also sophisticated cyber intrusions, pressure on U.S. companies in China, shell-game corporate transactions, and joint-venture "partnerships" that are anything but a true partnership. There's also nothing traditional about the scale of their theft—it's unprecedented in the history of the FBI. American workers and companies are facing a greater, more complex danger than they've ever dealt with before. Stolen innovation means stolen jobs, stolen opportunities for American workers, stolen national power, and stolen leadership in the industries.

As the lead U.S. counterintelligence agency, the FBI is responsible for detecting and lawfully countering the actions of foreign intelligence services and organizations as they seek to adversely affect U.S. national interests. The FBI recognized the need to coordinate similar

efforts across all agencies, and therefore established the National Counterintelligence Task Force ("NCITF") in 2019 to create a whole-of-government approach to counterintelligence. The FBI established the national-level task force, or NCITF, in the National Capital Region to coordinate, facilitate, and focus these multi-agency counterintelligence operations, and to programmatically support local Counterintelligence Task Force ("CITF") operations. Combining the authorities and operational capabilities of the U.S. Intelligence Community; Federal, state, and local law enforcement; and local CITFs in each FBI field office, the NCITF coordinates and leads whole-of-government efforts to defeat hostile intelligence activities targeting the United States.

The Department of Defense has been a key partner in the NCITF since its founding. While the FBI has had long-term collaborative relationships with DoD entities such as the Air Force Office of Special Investigations, Naval Criminal Investigative Service, and Army Counterintelligence, the NCITF has allowed us to enhance our collaboration with each other for greater impact. We plan to emphasize this whole-of-government approach moving forward as a powerful formula to mitigate the modern counterintelligence threat.

In recent years, we have seen a rise in efforts by authoritarian regimes to interfere with freedom of expression and punish dissidents abroad. These acts of repression cross national borders, often reaching into the United States. It's important to note countries like China, Russia, and Iran stalk, intimidate, and harass certain people in the U.S. This is called transnational repression. It's illegal, and the FBI is investigating it.

Transnational repression can occur in different forms, including assaults and attempted kidnapping. Governments use transnational repression tactics to silence the voices of their citizens, U.S. residents, or non-citizens connected to the home country. This sort of repressive behavior is antithetical to our values as Americans. People from all over the world are drawn to the United States by the promise of living in a free and open society—one that adheres to the rule of law. To ensure that this promise remains a reality, we must continue to use all of our tools to block authoritarian regimes that seek to extend their tactics of repression beyond their shores.

Our nation is confronting multifaceted foreign threats seeking to both influence our national policies and public opinion, and cause harm to our national dialogue and debate. The FBI and our interagency partners remain concerned about, and focused on, foreign malign influence operations—which include subversive, undeclared, coercive, and criminal actions used by foreign governments in their attempts to sway U.S. voters' preferences and perspectives, shift U.S. policies, increase discord in the United States, and undermine the American people's confidence in our democratic institutions and processes.

Foreign malign influence is not a new problem, but the interconnectedness of the modern world, combined with the anonymity of the Internet, have changed the nature of the threat and how the FBI and its partners must address it. Foreign malign influence operations have taken many forms and used many tactics over the years. Most widely reported these days

are attempts by adversaries—hoping to reach a wide swath of Americans covertly from outside the United States—to amplify existing stories on social media in an attempt to discredit U.S. individuals and institutions.

The FBI is the lead Federal agency responsible for investigating foreign malign influence threats. Several years ago, we established the Foreign Influence Task Force ("FITF") to identify and counteract foreign malign influence operations targeting the United States. The FITF is led by the Counterintelligence Division and comprises agents, analysts, and professional staff from the Counterintelligence, Cyber, Counterterrorism, and Criminal Investigative Divisions. It is specifically charged with identifying and combating foreign malign influence operations targeting democratic institutions and values inside the United States. In all instances, the FITF strives to protect democratic institutions, develop a common operating picture, raise adversaries' costs, and reduce their overall asymmetric advantage.

The FITF brings the FBI's national security and traditional criminal investigative expertise under one umbrella to prevent foreign malign influence in our elections. This better enables us to frame the threat, to identify connections across programs, to aggressively investigate as appropriate, and—importantly—to be more agile. Coordinating closely with our partners and leveraging relationships we have developed in the technology sector, we had several instances where we were able to quickly relay threat indicators that those companies used to take swift action, blocking budding abuse of their platforms.

After previous midterm elections, we reviewed the threat and the effectiveness of our coordination and outreach. As a result of this review, we further expanded the scope of the FITF. Previously, our efforts to combat foreign malign influence focused solely on the threat posed by Russia. Utilizing lessons learned, the FITF widened its aperture to confront malign foreign operations of the PRC, Iran, and other global adversaries. To address this expanding focus and wider set of adversaries and influence efforts, we have also added resources to maintain permanent "surge" capability on foreign malign influence threats to elections.

In addition, the domestic counterintelligence environment is more complex than ever. This nation faces a persistent and pervasive national security threat from foreign adversaries, particularly Russia and China, conducting sophisticated intelligence operations using coercion, subversion, malign influence, disinformation, cyber and economic espionage, traditional spying and non-traditional human intelligence collection. Together, they pose a continuous threat to U.S. national security and its economy by targeting strategic technologies, industries, sectors, and critical infrastructures. Historically, these asymmetric national security threats involved foreign intelligence service officers seeking U.S. government and U.S. Intelligence Community 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.

The FY 2024 Request includes an additional 30 positions (all Professional Staff) and $4.5 million to help combat the threats posed by foreign, and potentially hostile, intelligence services and other foreign government actors.

Criminal Threats

The U.S. faces many criminal threats, including financial and health care fraud, transnational and regional organized criminal enterprises, crimes against children and human trafficking, and public corruption. Criminal organizations — domestic and international — and individual criminal activity represent a significant threat to security and safety in communities across the nation.

A critical tool in protecting the Nation from those who wish to do us harm is the National Instant Criminal Background Check System, or NICS. The goal of NICS is to ensure that guns don't fall into the wrong hands, and ensure the timely transfer of firearms to eligible gun buyers. Mandated by the Brady Handgun Violence Prevention Act of 1993 and launched by the FBI on November 30, 1998, NICS is used by Federal Firearms Licensees (FFLs) to determine whether a prospective buyer is eligible to buy firearms. NICS receives information from tens of thousands of FFLs and checks to ensure that applicants do not have a criminal record and aren't otherwise prohibited and therefore ineligible to purchase a firearm. In the first complete month of operation in 1998, a total of 892,840 firearm background checks were processed; in 2022, approximately 2.6 million checks were processed per month, for a total of 31.6 million processed in 2022.

While most checks are completed within minutes by electronic searches of the NICS database, a small number of checks require examiners to review records and resolve missing or incomplete information before an application can be approved or rejected. Ensuring the timely processing of these inquiries is important to ensure law abiding citizens can exercise their right to purchase a firearm and to protect communities from prohibited and therefore ineligible individuals attempting to acquire a firearm. To ensure the FBI maintains this capability, the FY 2024 Request includes an additional 27 positions (including 1 Special Agent and 26 Professional Staff) and $8.4 million.

In 2022, Congress demonstrated its united faith in the role NICS plays in our country's public safety and a desire to make it even stronger with passage of the Bipartisan Safer Communities Act. This legislation added dating relationships as a disqualifying consideration for misdemeanor crimes of domestic violence prohibitions; enhanced checks on persons under the age of 21 by requiring additional outreach to state and local agencies where the person resides to inquire about the existence of any possibly disqualifying juvenile records; allows certain FFLs to receive information from the NCIC gun file necessary to verify if a firearm had been reported stolen before buying it second hand; and allows FFLs to access NICS for the purposes of voluntary background checks on current and prospective employees to help combat illegal firearms trafficking. The FBI has implemented all aspects of the BSCA with the

exception of the two latter parts as they require the promulgation of regulations. Those proposed regulatory changes are in process and are a priority to complete. Since the passage of the BSCA, the FBI has conducted over 86,400 expanded background checks on persons under the age of 21. The vast majority are proceeded quickly. However, a total of 750 checks have been denied under the new process. As a result of the expanded outreach enabling NICS to issue denials based solely on information it obtains, NICS issued 151 denials.

Violent Crime

Violent crimes and gang activities exact a high toll on individuals and communities. Many of today's gangs are sophisticated and are well organized. They use violence to control neighborhoods and boost their illegal money-making activities, which include robbery, drug and gun trafficking, fraud, extortion, and prostitution rings. These gangs do not limit their illegal activities to single jurisdictions or communities. The FBI is able to work across such lines, which is vital to the fight against violent crime in big cities and small towns across the Nation. Every day, FBI special agents work in partnership with Federal, state, local, and Tribal officers and deputies on joint task forces and individual investigations.

FBI joint task forces—Violent Crime Safe Streets, Violent Gang Safe Streets, and Safe Trails—focus on identifying and targeting major groups operating as criminal enterprises. Much of the FBI criminal intelligence is derived from our state, local, and tribal law enforcement partners, who know their communities inside and out. Joint task forces benefit from FBI surveillance assets, and our sources track these gangs to identify emerging trends. Through these multi-subject and multi-jurisdictional investigations, the FBI concentrates its efforts on high-level groups engaged in patterns of racketeering. This investigative model enables us to target senior gang leadership and to develop enterprise-based prosecutions.

By way of example, the FBI has dedicated tremendous resources to combat the threat of violence posed by MS-13. The atypical nature of this gang has required a multi-pronged approach—we work through our task forces here in the U.S. while simultaneously gathering intelligence and aiding our international law enforcement partners. We do this through the FBI's Transnational Anti-Gang Task Forces (TAGs). Established in El Salvador in 2007 through the FBI's National Gang Task Force, Legal Attaché San Salvador, and the United States Department of State, each TAG is a fully operational unit responsible for the investigation of MS-13 operating in the northern triangle of Central America and threatening the United States. This program combines the expertise, resources, and jurisdiction of participating agencies involved in investigating and countering transnational criminal gang activity in the United States and Central America. There are now TAGs in El Salvador, Guatemala, and Honduras. Through these combined efforts, the FBI has achieved substantial success in countering the MS-13 threat across the United States and Central America.

We are committed to working with our Federal, state, local, and tribal partners in a coordinated effort to reduce violent crime in the United States.

Transnational Organized Crime ("TOC")

More than a decade ago, organized crime was characterized by hierarchical organizations, or families, that exerted influence over criminal activities in neighborhoods, cities, or states. But organized crime has changed dramatically. Today, international criminal enterprises run multi-national, multi-billion-dollar schemes from start to finish. Modern-day criminal enterprises are flat, fluid networks with global reach. While still engaged in many of the "traditional" organized crime activities of loan-sharking, extortion, and murder, modern criminal enterprises are also involved in trafficking counterfeit prescription drugs containing deadly fentanyl, targeting stock market fraud and manipulation, cyber-facilitated bank fraud and embezzlement, illicit drug trafficking, identity theft, human trafficking, money laundering, alien smuggling, public corruption, weapons trafficking, kidnapping, and other illegal activities. TOC networks exploit legitimate institutions for critical financial and business services that enable the storage or transfer of illicit proceeds. Preventing and combating transnational organized crime demands a concentrated effort by the FBI and Federal, state, local, tribal, and international partners.

As part of our efforts to combat the TOC threat, the FBI is focused on the cartels trafficking dangerous narcotics, like fentanyl, across our border. The FBI has over 380 cases linked to cartel leadership and actively participates in 6 OCDETF Strike Forces along the border, investigating major drug trafficking, money laundering, and other high priority transnational organized crime networks. On top of that, we are pursuing healthcare fraud investigations against medical professionals and pill mills through our prescription drug initiative, investigating the gangs and criminal groups responsible for distributing dangerous substances like fentanyl through our Safe Streets Task Forces, and disrupting and dismantling DarkNet marketplaces for prescription opioids and drugs like fentanyl through our Joint Criminal Opioid Darknet Enforcement team.

While the FBI continues to share intelligence about criminal groups with our partners and combines resources and expertise to gain a full understanding of each group, the threat of transnational crime remains a significant and growing threat to national and international security with implications for public safety, public health, democratic institutions, and economic stability across the globe. TOC groups increasingly exploit jurisdictional boundaries to conduct their criminal activities overseas. Furthermore, they are expanding their use of the Darknet to engage in illegal activity while exploiting emerging technology to traffic illicit drugs and contraband across international borders and into the U.S.

Crimes Against Children and Human Trafficking

It is unthinkable, but every year, thousands of children become victims of crimes, whether it is through kidnappings, violent attacks, sexual abuse, human trafficking, or online predators. The FBI is uniquely positioned to provide a rapid, proactive, and comprehensive response; identify, locate, and recover child victims; and strengthen relationships between the

FBI and Federal, state, local, tribal, and international law enforcement partners to identify, prioritize, investigate, and deter individuals and criminal networks from exploiting children.

But the FBI's ability to learn about and investigate child sexual exploitation is being threatened by the proliferation of sites online on the Darknet. For example, currently, there are at least 30 child sexual abuse material (CSAM) sites operating openly and notoriously on the Darknet, including the Tor network. Some of these CSAM sites are exclusively dedicated to the sexual abuse of infants and toddlers. The sites often expand rapidly, with one site obtaining 200,000 new members within its first four weeks of operation.

The FBI combats this pernicious crime problem through investigations such as Operation Cross Country. Over a two-week period in 2022, the FBI, along with other Federal, state, and local partners, executed approximately 400 operations. These operations identified and located 84 minor victims of child sex trafficking and child sexual exploitation offenses and located 37 actively missing children. Furthermore, the FBI and its partners located 141 adult victims of human trafficking, and identified or arrested 85 suspects with child sexual exploitation and human trafficking offenses.

The FBI has several programs in place to arrest child predators and to recover missing and endangered children. To this end, the FBI funds or participates in a variety of endeavors, including our Innocence Lost National Initiative, Innocent Images National Initiative, Operation Cross Country, Child Abduction Rapid Deployment Team, Victim Services, over 80 Child Exploitation and Human Trafficking Task Forces, over 50 International Violent Crimes Against Children Task Force Officers, as well as numerous community outreach programs to educate parents and children about safety measures they can follow. Through improved communications, the FBI also has the ability to quickly collaborate with partners throughout the world, which plays an integral role in crime prevention.

The Child Abduction Rapid Deployment Team is a rapid response team comprised of experienced investigators strategically located across the country to quickly respond to child abductions. Investigators are able to provide a full array of investigative and technical resources during the most critical time period following the abduction of a child, such as the collection and analysis of DNA, impression, and trace evidence, and the processing of digital forensic evidence.

In addition to programs combating child exploitation, the FBI also focuses efforts to stop human trafficking. The FBI works collaboratively with law enforcement partners to combat all forms of human trafficking through Human Trafficking Task Forces nationwide.

The majority of human trafficking victims recovered during FBI investigations are United States citizens, but traffickers are opportunists who will exploit any victim with a vulnerability, including foreign nationals and victims of all ages, by subjecting them to forced labor or sex trafficking. We take a victim-centered, trauma-informed approach to investigating these cases and strive to ensure the needs of victims are fully addressed at all stages. To

accomplish this, the FBI works in conjunction with other law enforcement agencies and victim specialists on the local, state, tribal, and Federal levels, as well as with a variety of vetted non-governmental organizations. Even after the arrest and conviction of human traffickers, the FBI often continues to work with partner agencies and organizations to assist victims and survivors in moving beyond their exploitation.

The FBI commends the committee's dedication to these efforts and appreciates the resources provided to combat these horrific acts. The FY 2024 Request includes an additional 17 positions (14 Special Agents and 3 professional staff) and $6.4 million to expand the Crimes Against Children and Human Trafficking programs.

Key Cross-Cutting Capabilities and Capacities

Operational Technologies

As criminal and terrorist threats become more diverse and dangerous, the role of technology becomes increasingly important to our efforts. We are using technology to improve the way we collect, analyze, and share information. We have seen significant improvement in capabilities and capacities over the past decade; but keeping pace with technology remains a key concern for the future.

The FBI Laboratory is one of the largest and most comprehensive forensic laboratories in the world. Operating out of a state-of-the-art facility in Quantico, Virginia, laboratory personnel travel the world on assignment, using science and technology to protect the nation and support law enforcement, intelligence, military, and forensic science partners. The Lab's many services include providing expert testimony, mapping crime scenes, and conducting forensic exams of physical and hazardous evidence. Lab personnel possess expertise in many areas of forensics supporting law enforcement and intelligence purposes, including explosives, trace evidence, documents, chemistry, cryptography, DNA, facial reconstruction, fingerprints, firearms, digital forensics and weapons of mass destruction (WMD).

One example of the Lab's key services and programs is the Combined DNA Index System (CODIS), software the FBI develops and administers, which allows 200 law enforcement laboratories throughout the United States to compare over 20 million DNA profiles. In the last 20 years, CODIS has aided over 600,000 investigations, while maintaining its sterling reputation and the confidence of the American public. The latest version of the system, however, is 10 years old, and requires transition to a more stable, reliable, efficient and secured platform.

In addition, statutory requirements and recent regulatory changes have significantly expanded the DNA processing requirements of the FBI. For instance, enacted in 2005, the DNA Fingerprint Act (in 34 U.S.C. § 40702(a)(1)(A) and (B)) authorized the Attorney General

(AG) to collect DNA samples from individuals who are arrested, facing charges, or convicted, and from non-U.S. persons detained under U.S. authority. The law mandates Federal DNA collection agencies submit their arrestee collections to the FBI Laboratory for analysis and entry into CODIS. In April 2020, the Department of Justice (DOJ) amended the DNA Fingerprint Act's implementing rule that now precludes the Department of Homeland Security (DHS) from waiving DNA collections on over 700,000 individuals per year. As a result, during the past 12 months, the FBI has received an average of 92,000 DNA samples per month (over 10 times the historical sample volume). When Title 42 ends, the FBI anticipates an additional 50,000 samples per month due to increased DHS detentions. This will eventually bring the total monthly samples received to approximately 120,000 (~1,440,000 samples per year). This substantial increase has created massive budget and personnel shortfalls for the FBI. While the FBI has worked with DHS components to automate and streamline workflows, a backlog of approximately 650,000 samples has developed, increasing the likelihood of arrestees and non-U.S. detainees being released before identification through investigative leads.

Investment in additional DNA expansion capabilities and technology is critical to maintaining and enhancing the FBI's ability to address emerging threats and help mission critical information reach partners and investigators in an expeditious manner. The FY 2024 Request includes an additional 7 positions and $53.1 million to assist the FBI in processing DNA samples in a timely manner and leverage technology to modernize the aging CODIS system.

In addition to forensic advancements, the FBI must also invest in technologies to help its workforce. This includes reliable, secure access to classified information and systems in a remote environment. This technology – the Enterprise Remote Access System (ERAS) – provides FBI users the ability to access the FBI's Secret Enclave securely and remotely. This is particularly important in field offices where Special Agents may be several hours from the nearest FBI Field Office (FO) or Resident Agency (RA). This remote access significantly improves the timely completion of investigative activities, dissemination of intelligence, and sustainment of necessary business operations.

Another technology in which the FBI must make investments is in the body worn camera (BWC) arena. BWCs are critical tools that enhance law enforcement transparency and accountability, and thereby assist in building and maintaining public trust. In the past decade, BWC use has become commonplace in large law enforcement organizations throughout the U.S. According to a study by DOJ's Office of Justice Programs (OJP), as of 2016, about 80% of non-Federal law enforcement agencies with at least 500 full-time officers had acquired BWCs. Additionally, other Federal entities have implemented BWC programs, including select agencies within the Department of the Interior (DOI) and Customs and Border Patrol (CBP).

In 2020, DOJ announced the Department would permit state, local, territorial, and tribal task force officers to use BWCs on Federal task forces across the nation. In 2021, DOJ's BWC working group expressed the need to phase implementation of a BWC program for DOJ Federal Agents. As a result, in FY 2022, the FBI launched a pilot program in five field offices; the FBI

plans to expand this pilot to additional field offices across the country in FY 2023, as well as in FY 2024 should funding become available. The FBI has always been committed to transparency and accountability. BWC technology would enable the FBI to further this commitment to the public.

Also, to begin to address executive order requirements and meet standards for sustainable, resilient vehicle fleet electrification, the FBI proposes to begin deployment of zero emission vehicles – including battery electric, plug-in electric hybrid, and hydrogen fuel cell vehicles – along with applicable charging stations in select Field Offices across the nation.

FBI special agents and intelligence analysts need the best technological tools available to be responsive to the advanced and evolving threats that face our nation. The FY 2024 Request includes an additional $3.1 million for secure communications, $14.1 million for zero emissions vehicles, and $2.8 million for body worn cameras.

Conclusion

Finally, the strength of any organization is its people. The threats we face as a nation have never been greater or more diverse and the expectations placed on the FBI have never been higher. Our fellow citizens look to the FBI to protect the United States from all of those threats, and the men and women of the FBI continue to meet and exceed those expectations, every day. I want to thank them for their dedicated service.

Chairwoman Shaheen, Ranking Member Moran, and Members of the Subcommittee, thank you for the opportunity to testify today. I am happy to answer any questions you might have.