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
"A REVIEW OF THE PRESIDENT'S FISCAL YEAR 2025 BUDGET REQUEST FOR THE FEDERAL BUREAU OF INVESTIGATION"

PRESENTED
JUNE 4, 2024

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
"A REVIEW OF THE PRESIDENT'S FISCAL YEAR 2025 BUDGET REQUEST FOR THE FEDERAL BUREAU OF INVESTIGATION"

PRESENTED
JUNE 4, 2024

Good afternoon, Chairwoman Shaheen, Ranking Member Moran, and Members of the Subcommittee. Thank you for inviting me to appear before you today. Each day, Federal Bureau of Investigation ("FBI") personnel are making a real difference in communities across the nation, tackling some of the most complex national security and criminal threats with perseverance, professionalism, and integrity – sometimes at the greatest of costs. I am extremely proud of their service and commitment. On their behalf, I ask for your support 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 2025 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 2025 Budget Overview

The FY 2025 budget request proposes a total of $11.3 billion in direct budget authority to carry out the FBI's national security, intelligence, criminal law enforcement, and criminal justice services missions. The gross request includes a total of $11.3 billion for Salaries and Expenses, which will support 37,083 positions (13,623 Special Agents, 3,337 Intelligence Analysts, and 20,123 professional staff), and $61.9 million for Construction. The request includes program enhancements under Salaries and Expenses, including $7.0 million to enhance cyber investigative capabilities, $17.8 million to mitigate threats from foreign intelligence services, and $8.4 million to address the increased volume of firearms background checks. The request also provides funding to allow the FBI to fund critical national security and law enforcement positions reduced as a result of reductions in the FY 2024 enacted appropriation. Congress has long supported these positions in years past, and the safety and security of the

American people would be well served by allowing the FBI to continue filling these positions in FY 2025 through the requested budget.

As described in this threat summary, our adversaries are not scaling back their efforts because of the constrained budget environment. In fact, threat actors may try to take advantage of federal budget reductions to conduct nefarious activities. The FBI cannot afford to be playing catch-up to the People's Republic of China ("PRC"), Hamas, and transnational organized criminals coming across the border, and cyber actors. With the requested resources, the FBI will have the talent, tools, and authorities to do more to protect the American people and uphold the Constitution.

Key Threats and Challenges

Over the past year, the threats facing our nation have escalated. These threats emanate from myriad sources – nation-states, hostile foreign intelligence services, and criminals. They range from homegrown violent extremists (HVEs) to sophisticated cyber-attacks, from internet facilitated sexual exploitation of children to human trafficking, from violent gangs and criminal organizations to public corruption and corporate fraud. Keeping pace with these threats is a significant challenge for the FBI, especially as technology evolves and allows adversaries to use 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 United States. Cyber actors also exploit technology to infiltrate U.S. networks, steal our intellectual property and secrets, spread malware, hold our critical infrastructure at risk, and create chaos. The breadth of these threats and challenges are as complex as at 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 funding the FBI to do its part in thwarting these threats and facing these challenges is greatly appreciated. That support will allow us to establish strong capabilities and capacities to assess threats, share intelligence, leverage key technologies, and — in some respects, most importantly — hire the best personnel 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 will face 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. As we saw in October with the devastating attack in Israel, terrorist actors are still very intent on using violence and brutality to spread their ideologies. We are in an environment where the threats from international terrorism (IT), domestic terrorism (DT), and state-sponsored terrorism are all simultaneously elevated.

Over the past few years, the greatest terrorism threat to our homeland has been posed by lone actors or small cells of individuals who typically radicalize to violence online and who primarily use easily accessible weapons to attack soft targets. In addition to this threat, which has not diminished, we are also increasingly concerned that foreign terrorist organizations will enable or direct attacks on U.S, soil. We see the lone offender threat with both domestic violent extremists ("DVEs") and HVEs, two distinct threats, both primarily located in the United States that typically radicalize and mobilize to violence on their own. DVEs are individuals based and operating primarily within the United States or its territories without direction or inspiration from a foreign terrorist group or other foreign power who seek to further political or social goals through unlawful acts of force or violence. In comparison, HVEs are individuals of any citizenship who have lived and/or operated primarily in the United States or its territories, who advocate, are engaged in, or are preparing to engage in ideologically motivated terrorist activities in furtherance of political or social objectives promoted by a foreign terrorist organization but are acting independently of direction by a foreign terrorist organization ("FTO").

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 public mass 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"). The number of FBI domestic terrorism investigations has more than doubled since the spring of 2020. At the end of FY 2023, the FBI was conducting approximately 2,700 investigations within the domestic terrorism program and

was also conducting approximately 4,000 investigations within its international terrorism program.

The FBI assesses HVEs as 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 to commit violence by FTOs, including the self-proclaimed Islamic State of Iraq and ash-Sham ("ISIS") and al-Qaida and their affiliates. The 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 by HVEs.

While we assist our Israeli colleagues and we understand the global implications of the ongoing conflict in Israel, we are paying heightened attention to how the events abroad could directly affect and inspire people to commit violence here in the Homeland. Terrorist organizations worldwide, as well as individuals attracted to violence, have praised Hamas' horrific attack on Israeli civilians. We have seen violent extremists across ideologies seeking to target Jewish and Muslim people and institutions through physical assaults, bomb threats, and online calls for mass casualty attacks. Our top concern stems from lone offenders inspired by—or reacting to—the ongoing Israel-Hamas conflict, as they pose the most likely threat to Americans, especially Jewish, Muslim, and Arab-American communities in the United States. We have seen an increase in reported threats to Jewish and Muslim people, institutions, and houses of worship here in the United States, and we are moving quickly to mitigate them.

Presently, we have no information to indicate that Hamas has the intent or capability to conduct operations inside the United States, though we cannot, and do not, discount that possibility, but we are especially concerned about the possibility of Hamas supporters engaging in violence on the group's behalf. As always, we are concerned with any FTO that may exploit the attacks in Israel as a tool to mobilize their followers around the world. In recent years, there have been several events and incidents in the United States that were purportedly motivated, at least in part, by the conflict between Israel and Hamas. These have included the targeting of individuals, houses of worship, and institutions associated with the Jewish and Muslim faiths with acts of physical assault, vandalism, or harassment. Anti-Semitism and anti-Islamic sentiment permeate many violent extremist ideologies and serve as a primary driver for attacks by a diverse set of violent extremists who pose a persistent threat to Jewish and Muslim communities and institutions in the United States and abroad. FTOs have exploited previous conflicts between Israel and Hamas via media outlets and online communications to call on their supporters located in the United States to conduct attacks. Some violent extremists have used times of heightened tensions to incite violence against religious minorities, targeting both Jewish and Muslim Americans.

The FBI remains concerned about the intent of FTOs, such as ISIS and al-Qaida 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 its partners— 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' 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 specifically advocated for attacks against civilians, the military, law enforcement, and intelligence community personnel.

Al-Qaida also maintains its desire to conduct and to inspire large-scale attacks. Because continued pressure has degraded some of the group's senior leadership, we assess that, in the near term, al-Qaida 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. Nevertheless, propaganda from al-Qaida leaders continues to seek individuals inspired 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, attack and plot against the United States and our allies throughout the Middle East. Iran's Islamic Revolutionary Guard Corps-Qods Force ("IRGC-QF") has also provided support to militant resistance groups and terrorist organizations. And Iran has supported Lebanese Hizballah and other terrorist groups. Hizballah has sent operatives to build terrorist infrastructure 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 has also threatened retaliation for the death of IRGC-QF Commander Qassem Soleimani.

While the terrorism threat continues to evolve, the FBI's resolve to counter that threat remains constant. 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 its 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 threats posed by violent extremists 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.

In addition to fighting terrorism, countering the proliferation of weapons-of-mass-destruction materials ("WMD"), technologies, and expertise, preventing their use by any actor, and securing nuclear and radioactive materials of concern are also top national security priorities 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, and yield significant social, economic, political, and other national security consequences.

The FY 2025 budget request will allow the FBI to invest resources in counterterrorism programs previously funded prior to the FY 2024 appropriation. In a rapidly evolving threat environment, now is not the time to reduce resources against international terrorism threats.

Cyber

The FBI has seen a wider-than-ever range of cyber actors threaten Americans' safety, security, and confidence in our digitally connected world. Cybercriminal syndicates and nation-states continue to innovate, using unique techniques to compromise our networks and maximize the reach and impact of their operations. Those techniques include selling malware as a service or targeting vendors 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 the People's Republic of China ("PRC"), the Democratic People's Republic of Korea ("DPRK"), and Russia use cyber operations to target U.S. research. We have seen the PRC working to obtain controlled dual-use technology, while developing an arsenal of advanced cyber capabilities that could be used against other countries in the event of a real-world conflict. And we have seen the disruptive impact a serious supply-chain compromise can have through the SolarWinds-related intrusions, conducted by the Russian Foreign Intelligence Service. As these adversaries become more sophisticated, we are increasingly concerned about our ability to detect 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.

Making things even more difficult, there is often 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, such as ransomware, typically used by criminal actors.

So, as dangerous as nation-states are, we do not have the luxury of focusing only on them. 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. Incidents affecting medical centers have led to the interruption of computer networks and systems that put patients' lives at increased risk.

We have also seen the rise of an ecosystem of services dedicated to supporting cybercrime in exchange for cryptocurrency. Criminals now have new tools to engage in destructive behavior—for example, deploying ransomware to paralyze entire hospitals, police departments, and businesses—as well as new means to better conceal their tracks. It is not that

individual malicious cyber actors have necessarily become much more sophisticated, but that they can now 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. As the lead federal agency for threat response, the FBI 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 departments and agencies to ensure that our foreign partners are able and willing to cooperate in our efforts to disrupt perpetrators of cybercrime.

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 assisted the FBI Milwaukee Field Office investigating the case. And on April 5, 2023, the U.S. Department of Treasury announced sanctions against Genesis Market.

In January 2024, the FBI announced an operation where the FBI and its partners identified a network of hundreds of compromised routers used by the PRC sponsored hacking group known as Volt Typhoon. The botnet enabled China to hide, among other things, pre-operational reconnaissance and network exploitation against critical infrastructure like our communications, energy, transportation, and water sectors. The PRC took these steps to find and prepare to destroy or degrade the civilian critical infrastructure that keeps us safe and prosperous. To be extremely clear, cyber threats to our critical infrastructure represent real-world threats to our physical safety. Working with our partners, the FBI ran a court-authorized, on-network operation that significantly disrupted this Volt Typhoon botnet and the access it enabled.

This operation was an important step. But there's a lot more to do. To quantify what we are up against: the PRC has a bigger hacking program than every other major nation combined. In fact, if each one of the FBI's cyber agents and intelligence analysts focused exclusively on the PRC threat, the PRC's hackers would still outnumber FBI cyber personnel at least 50 to 1. The appropriations this Committee decides on this year will dictate what resources can apply to counter the growing PRC cyber threat, especially as 2027, the year that the Chinese Communist Party (CCP) has targeted for a potential invasion of Taiwan, approaches.

The FBI is doing everything in its power to combat these threats. In total, we took over 1,000 actions against cyber adversaries in 2023, 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 78 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.

Along with our partners in the interagency, the FBI has devoted significant energy and resources to partnerships 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, as well as how we protect identities and other information that the private sector shares with us. We are still 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 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. Our collective response to significant cyber threats—the SolarWinds campaign, Russia's Cyclops Blink botnet,, and the Colonial Pipeline incident—only emphasize what we have been saying for a long time: the government cannot protect against cyber threats on its own. We need a fully resourced 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 myriad 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 2025 Request includes an additional 12 positions (including 4 Special Agents and 8 Professional Staff) and $7.0 million to enhance cyber response capabilities.

Foreign Intelligence Threats

Nations such as the PRC, Russia, and Iran are becoming more aggressive and more capable than ever before. These nations seek to undermine our core democratic, economic, and scientific institutions, and they employ a growing range of tactics. 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 from PRC foreign intelligence and economic espionage. By extension, it is also a threat to our national security. The PRC aspires to reshape the international rules-based system to its benefit, often with little regard for international norms and laws.

When it comes to economic espionage, the PRC uses every means at its disposal, blending cyber, human intelligence, diplomacy, corporate transactions, and other pressure on U.S. companies operating in the PRC, to steal our companies' innovations. These efforts are consistent with the PRC's expressed goals of becoming the preeminent power on the world stage through technology-enabled economic and military development.

To pursue this goal, the PRC uses human intelligence officers, co-optees, and corrupt corporate insiders, as well as 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 is nothing traditional about the scale of their theft. It is unprecedented. American workers and companies are facing a greater, more complex danger than they have dealt with before. Stolen innovation means stolen jobs, stolen opportunities for American workers, and stolen national power.

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 NCITF, in the National Capital Region to coordinate, facilitate, and focus multi-agency counterintelligence operations, and to programmatically support local Counterintelligence Task Force ("CITF") operations in each FBI field office. Combining the authorities and operational capabilities of the U.S. Intelligence Community, Federal, state, and local law enforcement, and local CITFs, the NCITF coordinates and leads whole-of-government efforts to defeat hostile intelligence activities targeting the United States.

The Department of Defense ("DoD") 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 threats.

In recent years, we have seen a rise in efforts by authoritarian regimes to interfere with freedom of expression and punish dissidents, political opponents, and others abroad. These acts of repression cross national borders, often reaching into the United States. The governments of China, Russia, and Iran, and their proxies stalk, intimidate, and harass expatriates or dissidents who speak against the regime from within the United States and elsewhere, as well as other individuals these governments view as threats to their regime.

Transnational repression can occur in different forms, including assault, kidnapping, and murder. Governments use transnational repression tactics to silence the voices of their own or former citizens, U.S. residents, and family members living abroad who are critical of their regimes. This sort of repressive behavior is antithetical to our values. People from all over the world are drawn to the United States by the promise of living in a free and open society 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 own shores.

In addition, our Nation is confronting multifaceted foreign threats seeking both to influence our national policies and public opinion and to harm our national dialogue and debate. The FBI and our interagency partners remain focused on foreign malign influence operations, including subversive, undeclared, coercive, and criminal actions used by foreign governments in their attempts to sway U.S. citizens' 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. 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 our 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 inside the United States.

The domestic counterintelligence environment is more complex than ever. We face a persistent and pervasive national security threat from foreign adversaries, particularly the governments of China, Russia, and Iran, who conduct sophisticated intelligence operations using coercion, subversion, malign influence, cyber and economic espionage, traditional spying, and non-traditional human intelligence collection. Together, they pose a continuous threat to U.S. national security and our economy by targeting strategic technologies, industries, sectors, and critical infrastructure. Historically, these asymmetric national security threats involved foreign intelligence service officers seeking U.S. government and U.S. Intelligence Community information. Now, however, the FBI has observed foreign adversaries employing a wider 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 counterintelligence priorities to address this evolution.

The FY 2025 Request includes an additional 44 positions (12 Special Agents, 18 Intelligence Analysts, and 14 Professional Staff) and $17.8 million to help combat the threats posed by foreign, and potentially hostile, intelligence services and other foreign government actors.

Criminal Threats

The United States. faces many criminal threats, including financial and health care fraud, transnational and regional organized criminal enterprises, crimes against children, 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 harm is the National Instant Criminal Background Check System, or NICS. The goal of NICS is to ensure that guns do not 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 are not 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. By contrast, in 2023, approximately 2.4 million checks were processed per month, for a total of 29.9 million processed last year.

The Bipartisan Safer Communities Act (BSCA), signed into law in June 2022, requires enhanced NICS background checks for any person under the age of 21. These enhanced background checks are more labor-intensive but have prevented ineligible persons from acquiring firearms. As provisions from the BSCA continue to be implemented, the FBI expects the volume of NICS transactions to continue to grow. 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 2025 Request includes an additional 27 positions (including 1 Special Agent and 26 Professional Staff) and $8.4 million.

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— identify and target major groups operating as criminal enterprises. Much of the FBI criminal intelligence is derived from our state, local, territorial, 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 United States. while simultaneously gathering intelligence from 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 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 collaborating efforts, the FBI has achieved substantial success in countering the MS-13 threat.

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 such as loan-sharking, extortion, and murder, modern criminal enterprises are now also involved in trafficking counterfeit prescription drugs containing deadly fentanyl, conducting stock market fraud and manipulation, committing cyber-facilitated bank fraud and embezzlement, illicit drug trafficking, identity theft, human trafficking, money laundering, alien smuggling, engaging in 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, territorial, 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 borders. The FBI has over 350 cases linked to cartel leadership, and 91 of those are along the southern border. Additionally, the FBI actively participates in 18 Organized Crime Drug Enforcement Task Forces ("OCDETF") Strike Forces across the United States, investigating major drug trafficking, money laundering, and other high-priority TOC networks. On top of that, through our prescription drug initiative we are pursuing healthcare fraud investigations against medical professionals and pill mills, through our Safe Streets Task Forces, investigating the gangs and criminal groups responsible for distributing dangerous substances like fentanyl, and through our Joint Criminal Opioid Darknet Enforcement team disrupting and dismantling DarkNet marketplaces for prescription opioids and drugs like fentanyl.

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 United States.

Crimes Against Children and Human Trafficking

Every year, thousands of children become victims of crimes, whether it results from kidnappings, violent attacks, sexual abuse, human trafficking, or online predators. The FBI is uniquely positioned to provide a rapid, proactive, and comprehensive response. We help identify, locate, and recover child victims. Our strong relationships with Federal, state, local, territorial, Tribal, and international law enforcement partners also help 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 on the Darknet and end-to-end encryption. For example, currently, there are at least 30 Child Sexual Abuse Material (CSAM) sites operating openly and notoriously on the Darknet. Some of these exploitative sites are exclusively dedicated to the sexual abuse of infants and toddlers. The sites often expand rapidly, with one site obtaining as many as 200,000 new members within its first few weeks of operation. End-to-end encrypted apps allow offenders to form groups of like-minded individuals to trade files of CSAM and trade tips for how to exploit children - all with no fear of detection.

Another growing area of concern involving the sexual exploitation of children and adults alike is the explosion in incidents of children, teens, and adults being coerced into sending explicit images online and being extorted for money. Known as financially motivated "sextortion," between October 2021 and March 2023, law enforcement received over 13,000 reports of this type of crime, resulting in at least 12,600 victims here and abroad, and more than 20 suicides. A large percentage of these sextortion schemes originate outside the United States,

primarily in West African countries such as Nigeria and Ivory Coast. The continued development of Artificial Intelligence (AI) has made this crime even easier to commit. Perhaps the most difficult part of a successful sextortion is convincing the child to initially share a sexually explicit depiction. Now, with AI, offenders can create the sexually explicit depiction from innocent images available on social media – and then use that created image to extort the child into creating actual depictions or making a financial payment. The FBI continues to collaborate with other law enforcement partners and the National Center for Missing and Exploited Children to mitigate this criminal activity and provide the public with informational alerts and victim resources regarding these crimes.

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 and constructs, including the Innocence Lost National Initiative, the Innocent Images National Initiative, Operation Cross Country, Child Abduction Rapid Deployment Team, Victim Services, over 80 Child Exploitation and Human Trafficking Task Forces, over 74 International Violent Crimes Against Children Task Force officers, and numerous community outreach programs to educate parents and children about safety measures they can follow. Through improved communications, the FBI collaborates with partners throughout the world quickly, playing an integral role in preventing crimes against children.

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

The FBI also focuses efforts to stop human trafficking of both children and adults, including both sex trafficking and forced labor. The FBI works collaboratively with law enforcement partners to disrupt all forms of human trafficking through Human Trafficking Task Forces nationwide. Over a two-week period in 2023, the FBI and its Federal, state, local, and Tribal partners, executed approximately 350 operations to recover potential survivors of human trafficking and other forms of exploitation, and to disrupt potential trafficking and exploitation crimes. These operations identified and located 59 minors who were potential victims of child sex trafficking, child sexual exploitation, or related state or federal offenses and located 59 actively missing children. Furthermore, the FBI and its partners located 141 adults who were identified as potential victims of sexual exploitation, human trafficking, or related state or federal offenses. In addition to identifying and recovering missing children and potential victims, these law enforcement actions led to the identification or arrest of 126 suspects implicated in potential child sexual exploitation, human trafficking, or related state or federal offenses.

While many potential victims of human trafficking encountered or recovered by the FBI are adult U.S. citizens, foreign nationals, children, and other vulnerable populations are

disproportionately harmed by both sex and labor trafficking. In 2023, the FBI initiated efforts to develop specialized strategies for identifying and investigating crimes involving forced labor and transnational trafficking of foreign-national victims into the United States. The FBI and its partners 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 Federal, state, local, territorial, and Tribal 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.

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 a 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 WMDs.

One example of the Lab's key services and programs is the Combined DNA Index System (CODIS), 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 675,000 investigations, while maintaining its sterling reputation and the confidence of the American public.

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 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 amended the DNA Fingerprint Act's implementing rule that now precludes the Department of Homeland Security (DHS) from waiving DNA collections. As a result, during the past twelve months, the FBI received an average of 146,000 DNA samples per month, which is more than quadruple the average monthly submission rate for FY 2021 of 36,300 samples. 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 over 1.6 million samples (as of April 2024) has developed, increasing the likelihood of arrestees and non-U.S. detainees being released before identification through investigative leads. The Administration requested $204 million in its national security supplemental to address this backlog.

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.

Conclusion

In conclusion, 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. I also want to pledge to this Committee to be good stewards of the resources provided.

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.