



Department of Justice

STATEMENT OF

**CHRISTOPHER A. WRAY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION**

**BEFORE THE
HOUSE JUDICIARY COMMITTEE
UNITED STATES HOUSE OF REPRESENTATIVES**

**AT A HEARING TITLED
“FEDERAL BUREAU OF INVESTIGATION OVERSIGHT”**

**PRESENTED
JULY 12, 2023**

**STATEMENT OF
CHRISTOPHER A. WRAY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION**

**BEFORE THE
HOUSE JUDICIARY COMMITTEE
UNITED STATES HOUSE OF REPRESENTATIVES**

**AT A HEARING TITLED
“FEDERAL BUREAU OF INVESTIGATION OVERSIGHT”**

**PRESENTED
JULY 12, 2023**

Good afternoon, Chairman Jordan, Ranking Member Nadler, and Members of the Committee. 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.

Despite the many challenges our FBI workforce faces, I am immensely proud of their dedication to protecting the American people and upholding the Constitution. The list of diverse threats we face underscores the complexity and breadth of the FBI’s mission: to protect the American people and uphold the Constitution of the United States. I am prepared to discuss with you what the FBI is doing to address these threats and what the FBI is doing to ensure that our people adhere to the highest of standards while it conducts its mission.

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, and requires us 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, to recruit followers, to encourage terrorist attacks and other illicit actions, and to disperse information on building improvised explosive devices and other means to attack the United States. 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 Congress, including this Committee, is critical in helping the FBI do its part to thwart these threats and face these challenges. That support enables us to establish strong capabilities and capacities to assess threats, to share intelligence, to leverage key technologies, and—often most importantly—to hire some of the best talent to serve as Special Agents, Intelligence Analysts, and professional staff. We are continuously enhancing a workforce that possesses 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. The threats from international terrorism, domestic terrorism, and state-sponsored terrorism all remain at elevated levels, requiring continued investment and vigilance.

The greatest terrorism threat to our Homeland comes from lone actors or small cells who radicalize—typically 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 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. Recently, they have focused on accessible targets, including 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, as well as their 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. As of the end of fiscal year 2022, the FBI was conducting approximately 2,700 investigations 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.

As for international terrorism, the FBI assesses that HVEs are the greatest, most immediate threat to the Homeland. Rather than receiving individualized direction from FTOs, HVEs are people 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. A HVE’s lack of a direct connection with an FTO, ability to rapidly mobilize without detection, and use of encrypted communications can pose significant challenges to our ability to proactively identify and disrupt potential violent attacks. For example, on New Year’s Eve last year in New York City, an HVE attacked three New York Police Department Officers using an edged weapon.

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 hate-fueled rhetoric and to attract like-minded violent extremists with a willingness to conduct attacks against the United States and our interests abroad. We are also concerned about ISIS’s successful use of social media and messaging applications, like other foreign terrorist groups, to advocate for lone-offender attacks in the United States and Western countries. They use videos and other English language propaganda that have specifically advocated for attacks against civilians, the military, law enforcement, and intelligence community personnel.

Al-Qa'ida also maintains its desire to 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, however, 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. This willingness to seek retaliation against the United States was reflected in charges the Department brought in 2022 against a member of the IRGC, working on behalf of the Qods Force, with a plot to murder a former national security advisor.

While the terrorism threat continues to evolve, the FBI's 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. We use all available lawful investigative techniques and methods to combat these threats. We collect, analyze, and share intelligence concerning the threats posed by violent extremists, in all their forms, who desire to harm Americans and U.S. interests. And we will continue to share information and encourage the sharing of information among our numerous partners through our Joint Terrorism Task Forces across the country, as well as our Legal Attaché offices around the world.

In addition to fighting terrorism, 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 are also top national security priority missions for the FBI. The FBI considers preventing, mitigating, investigating, and responding to weapons of mass destruction ("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. In collaboration with Federal, state, local, Tribal, territorial, and other partners, The FBI integrates complementary efforts to counter WMD terrorism. An example of this collaboration is the FBI-led Weapons of Mass Destruction Strategic Group. This interagency crisis action team spans more than fifteen departments and agencies to coordinate the federal government's response to WMD threats and incidents.

Alongside the FBI, the Department of Homeland Security maintains the largest footprint on the Strategic Group.

Cyber

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. Those techniques include selling malware as a service and 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 Foreign Intelligence Service. 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.

Making things 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 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. 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 has faced 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. 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. Using its role 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 agencies to ensure that our foreign partners are able and willing to cooperate in our efforts to disrupt and bring to justice the 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 in the cyber crime world, providing criminals a user-friendly database to search for stolen credentials and more easily infiltrate victims' computers and accounts. 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 U.S. District Court for the Eastern District of Wisconsin. A total of 22 international agencies and 44 FBI field offices worked with the FBI Milwaukee Field Office investigating the case. And on April 5, the U.S. Department of the Treasury announced sanctions against Genesis Market.

In total, along with our Department colleagues, we took over 1,000 actions against cyber adversaries in 2022, including arrests, criminal charges, convictions, dismantlements, and disruptions. We enabled many more actions through our dedicated partnerships with the private sector, with 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.

Along with our partners in the interagency, the FBI has devoted significant energy and resources to these partnerships, especially those involving 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 also committed to providing useful feedback and to 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. Significant cyber incidents—SolarWinds, Cyclops Blink, 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 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.

Foreign Intelligence Threats

Top Threats

Nations such as China, Russia, and Iran are 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 the PRC. It's a threat to our economic security—and, by extension—to our national security. The PRC 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 other pressure on U.S. companies operating in the PRC, to achieve its strategic goals to steal our companies' innovations. These efforts are consistent with the PRC government's expressed goal to become an international power, modernizing its military and creating innovative-driven economic growth.

To pursue this goal, China 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's also nothing traditional about the scale of their theft. It is unprecedented in the history of the FBI. American workers and companies are facing a greater, more complex danger than they have ever dealt with before. Stolen innovation means stolen

jobs, stolen opportunities for American workers, stolen national power, and stolen leadership in the industries.

National Counterintelligence Task Force (“NCITF”)

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. Recognizing the need to coordinate similar efforts across all agencies, the FBI established the NCITF in 2019 to create a whole-of-government approach to counterintelligence. The FBI established this national-level task force 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, NT-50 departments and agencies, law enforcement agencies around the country, 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 (“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 as a powerful formula to mitigate the modern counterintelligence threat.

Transnational Repression

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. Governments such as the PRC, the Russian Federation, and the Government of Iran stalk, intimidate, and harass certain people in the United States. This is called transnational repression. It is 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 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—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 have used many tactics over the years.

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 Russia and China, conducting 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 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 our counterintelligence priorities and posture to address the evolving and multifaceted threat.

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.

Violent Crime

Violent crimes and gang activities exact a high toll on individuals and communities. Many of today's gangs are sophisticated and 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 our 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 United States, 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, primarily, 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 323 pending investigations linked to cartel leadership and 78 of those investigations are along the southern border. Additionally, the FBI actively participates in 17 OCDETF Strike Forces across the United States, 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 United States.

Crimes Against Children and Human Trafficking

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. We help identify, locate, and recover child victims. Our strong relationships with federal, state, local, 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 online on the Darknet. For example, currently, there are at least 30 child sexual abuse material 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 200,000 new members within its first four weeks of operation.

Another growing area of concern involving the sexual exploitation of children is the explosion in incidents of children and teens being coerced into sending explicit images online and extorted for money – a crime known as financial sextortion. In 2022, law enforcement received over 7,000 reports related to the online financial sextortion of minors, resulting in at least 3,000 victims, primarily boys, and more than a dozen 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 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, 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 with 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, the processing of digital forensic evidence, and interviewing expertise.

The FBI also focuses efforts to stop human trafficking of both children and adults. The FBI works collaboratively with law enforcement partners to disrupt all forms of human trafficking through Human Trafficking Task Forces nationwide. One way the FBI combats this pernicious crime problem is through investigations such as Operation Cross Country. Over a two-week period in 2022, the FBI, along with other federal, state, local, and Tribal partners, executed approximately 400 operations to recover survivors of human trafficking and disrupt traffickers. 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. In addition to recovering victims, the law enforcement activity conducted during Operation Cross Country led to the identification and arrest of 85 suspects for child sexual exploitation or human trafficking offenses.

Although many victims of human trafficking recovered by the FBI are adult U.S. citizens, the FBI and its partners recognize that foreign nationals, children, and other vulnerable populations are disproportionately harmed by both sex and labor 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 federal, state, local, 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.

Reauthorization of Section 702 of the Foreign Intelligence Surveillance Act

Before closing, I would be remiss if I didn't underscore an urgent legislative matter directly relevant to our discussion today. As the Committee knows, at the end of December Section 702 and other provisions of the Foreign Intelligence Surveillance Act will expire unless renewed.

Loss of this vital provision, or its reauthorization in a narrowed form, would raise profound risks. For the Bureau in particular, either outcome would mean substantially impairing, or in some cases entirely eliminating, our ability to find and disrupt many of most serious security threats I described earlier in my statement.

I am especially concerned about one frequently-discussed proposal, to require the government to obtain a warrant or court order from a judge before personnel may conduct a "U.S. person query" of information previously obtained through use of Section 702. A warrant requirement would amount to a *de facto* ban, because query applications either would not meet the legal standard to win court approval; or because, when the standard could be met, it would be so only after the expenditure of scarce resources, the submission and review of a lengthy legal filing, and the passage of significant time – which, in the world of rapidly evolving threats, the government often doesn't have. That would be a body blow to the FBI, which relies on this longstanding, lawful capability to rapidly uncover previously hidden threats and connections, and to take swift steps to protect the homeland when needed.

To be sure, nobody more deeply shares Members' concerns regarding past FBI compliance violations related to FISA, including the rules for querying Section 702 collection using U.S. person identifiers, than I do. These violations never should have happened and preventing recurrence is a matter of utmost priority. Fortunately, the Administration's initial response to these episodes was rigorous, and already has yielded significant results – in dramatically reducing the number of "U.S. person queries" by the FBI of the Section 702 database, and in substantially improving its compliance rate. Moreover, as we publicly announced last month, the Bureau is implementing further measures both to keep improving our compliance and to hold our personnel accountable for misuse of Section 702 and other FISA

provisions – including through an escalating scheme for employee discipline, culminating in possible dismissal.

Together with other leaders of the Intelligence Community and the Department of Justice, I remain committed to working with this Committee and others in Congress, on potential reforms to Section 702 that would not diminish its critical intelligence value. There are many options for meaningfully enhancing privacy and oversight, while fully preserving Section 702’s efficacy. Doing that will be critical, in order to ensure the FBI’s continuing ability to fulfill its mission of identifying and stopping national security threats within the U.S. homeland.

Conclusion

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.

Chairman Jordan, Ranking Member Nadler, and Members of the Committee, thank you for the opportunity to testify today. I am happy to answer your questions.