Department of Justice

STATEMENT OF

CHRISTOPHER A. WRAY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

AT A HEARING ENTITLED

"THREATS TO THE HOMELAND"

PRESENTED

NOVEMBER 17, 2022

STATEMENT OF
CHRISTOPHER A. WRAY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

AT A HEARING ENTITLED
"THREATS TO THE HOMELAND"

PRESENTED
NOVEMBER 17, 2022

Good morning, Chairman Peters, Ranking Member Portman, and Members of the Committee. Today, I am honored to be here, representing the people of the Federal Bureau of Investigation ("FBI"), who tackle some of the most complex and most grave threats we face every day with perseverance, professionalism, and integrity. Sometimes at the greatest of costs. I am extremely proud of their service and commitment to the FBI's mission and to ensuring the safety and security of communities throughout our nation. On their behalf, I would like to express my appreciation for the support you have given them in the past and ask for your continued support in the future.

Despite the many challenges our FBI workforce has faced, I am immensely proud of their dedication to protecting the American people and upholding the Constitution. Our country continues to face unimaginable challenges, yet, through it all, the women and men of the FBI have unwaveringly stood at the ready and taken it upon themselves to tackle any and all challenges thrown their way. 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 our people adhere to the highest of standards while it conducts its Mission. I am pleased to have received your invitation to appear today and am looking forward to engaging in a thorough, robust, and frank discussion regarding some of the most critical threats facing the FBI and the Nation as a whole.

Key Threats and Challenges

Our nation continues to face a multitude of serious and evolving threats ranging from homegrown violent extremists to hostile foreign intelligence services and operatives, from sophisticated cyber-based attacks to Internet facilitated sexual exploitation of children, from violent gangs and criminal organizations to public corruption and corporate fraud. Keeping pace with these threats is a significant challenge for the FBI. As an organization, we must be able to stay current with constantly evolving technologies. Our adversaries—terrorists, foreign intelligence services, and criminals—take advantage of modern technology, including the

Internet and social media, to facilitate illegal activities, recruit followers, encourage terrorist attacks and other illicit actions, to spread misinformation, and to disperse information on building improvised explosive devices and other means to attack the U.S. The breadth of these threats and challenges are as complex as any time in our history. And the consequences of not responding to and countering threats and challenges have never been greater.

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

Today's FBI is a national security and law enforcement organization that uses, collects, and shares intelligence in everything we do. Each FBI employee understands that, to defeat the key threats facing our nation, we must constantly strive to be more efficient and more effective. Just as our adversaries continue to evolve, so, too, must the FBI. We live in a time of acute and persistent terrorist, nation-state, 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

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. We are in an environment where the threats from international terrorism, domestic terrorism, and state-sponsored terrorism are all simultaneously elevated.

The greatest terrorism threat to our Homeland is 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. We see the lone offender threat with 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 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, wholly or in part, through unlawful acts of force or violence are described as DVEs, whereas 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 (including providing support to

terrorism) 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 mass public gatherings. Lone actors present a particular challenge to law enforcement and intelligence agencies. These actors are difficult to identify, investigate, and disrupt before they take violent action, especially because of the insular nature of their radicalization and mobilization to violence and limited discussions with others regarding their plans.

The top domestic terrorism threat we face continues to be from DVEs we categorize as Racially or Ethnically Motivated Violent Extremists ("RMVEs") and Anti-Government or Anti-Authority Violent Extremists ("AGAAVEs"). While RMVEs, who advocate for the superiority of the white race were the primary source of lethal attacks perpetrated by DVEs in recent years, AGAAVEs, specifically Militia Violent Extremists and Anarchist Violent Extremists were responsible for three of the four lethal DVE attacks in 2020. Notably, 2020 included the first lethal attack committed by an Anarchist Violent Extremist in over 20 years. More recently, in 2021, DVEs committed at least four lethal attacks, resulting in 13 deaths. DVEs with mixed or personalized ideologies committed two of the four attacks. The other two lethal attacks were committed by RMVEs—one who advocated for the superiority of the white race and one who allegedly used his interpretations of religious teachings to justify the murder of a police officer. The number of FBI domestic terrorism investigations has more than doubled since the spring of 2020, and as of the end of fiscal year 2022, the FBI was conducting approximately 2,700 domestic terrorism investigations.

We are approaching the two-year anniversary of the January 6 siege of the U.S. Capitol, which has led to unprecedented efforts by the Department of Justice, including the FBI, to investigate and hold accountable all who engaged in violence, destruction of property, and other criminal activity on that day. To date, the Department has arrested and charged more than 880 individuals who took part in the Capitol siege.

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

The FBI assesses HVEs are the greatest, most immediate international terrorism threat to the Homeland. HVEs are people located and radicalized to violence primarily in the United States, who are not receiving individualized direction from FTOs but are inspired by FTOs, including the self-proclaimed Islamic State of Iraq and ash-Sham ("ISIS") and al-Qa'ida and

their affiliates, to commit violence. An HVE's lack of a direct connection with an FTO, ability to rapidly mobilize without detection, and use of encrypted communications pose significant challenges to our ability to proactively identify and disrupt potential violent attacks.

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

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

Iran and its global proxies and partners, including Iraqi Shia militant groups, continue to attack and plot against the United States and our allies throughout the Middle East in response to U.S. pressure. 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 threat was exemplified in 2022, when the Department charged an Iranian national and member of the IRGC, working on behalf of the Qods Force, with a plot to murder a former National Security Advisor.

The terrorism threat continues to evolve, but the FBI resolve to counter that threat remains constant. As an organization, we continually adapt and rely heavily on the strength of our federal, state, local, tribal, territorial, and international partnerships to combat all terrorist threats to the United States and our interests. To that end, we use all available lawful investigative techniques and methods to combat these threats while continuing to collect,

analyze, and share intelligence concerning the threat posed by violent extremists, in all their forms, who desire to harm Americans and U.S. interests. We will continue to share information and encourage the sharing of information among our numerous partners via our Joint Terrorism Task Forces across the country, and our Legal Attaché offices around the world.

Cyber

Throughout these last two years, the FBI has seen a wider-than-ever range of cyber actors threaten Americans' safety, security, and confidence in our digitally-connected world. Cyber-criminal syndicates and nation-states keep innovating ways to compromise our networks and maximize the reach and impact of their operations, such as by selling malware as a service or by targeting vendors to access the networks of the vendors' customers.

These criminals and nation-states believe that they can compromise our networks, steal our property, extort us, and hold our critical infrastructure at risk without incurring any risk themselves. In the last few years, we have seen—and have publicly called out—the People's Republic of China ("PRC"), the Democratic People's Republic of Korea ("DPRK"), and Russia for using cyber operations to target U.S. COVID-19 vaccines and research. We have seen the far-reaching disruptive impact a serious supply-chain compromise can have through the SolarWinds-related intrusions, conducted by the Russian SVR. We have seen the PRC working to obtain controlled dual-use technology and developing an arsenal of advanced cyber capabilities that could be used against other countries in the event of a real-world conflict. As these adversaries become more sophisticated, we are increasingly concerned about our ability to detect and warn about specific cyber operations against U.S. organizations. One of the most worrisome facets is their focus on compromising U.S. critical infrastructure, especially during a crisis.

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

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

We have also seen the rise of an ecosystem of services dedicated to supporting cybercrime in exchange for cryptocurrency. The effect is that what were once unsophisticated criminals now have the tools to engage in destructive behavior—for example, deploying ransomware to paralyze entire hospitals, police departments, and businesses—and the means to

better conceal their tracks. It is not that individual malicious cyber actors have become much more sophisticated, but—unlike previously—they are able to rent sophisticated capabilities.

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

An example of this approach is the international seizure in April 2022 of Hydra Market—the world's largest and longest-running darknet market. Hydra was an online criminal marketplace that enabled users in mainly Russian-speaking countries to buy and sell illicit goods and services, including illegal drugs, stolen financial information, fraudulent identification documents, and money laundering and mixing services, anonymously and outside the reach of law enforcement. Transactions on Hydra were conducted in cryptocurrency and Hydra's operators charged a commission for every such transaction. In 2021, Hydra accounted for an estimated 80% of all darknet market-related cryptocurrency transactions, and since 2015, the marketplace had received approximately $5.2 billion in cryptocurrency. The seizure of the Hydra servers and cryptocurrency wallets containing $25 million worth of bitcoin was made in Germany by the German Federal Criminal Police (the Bundeskriminalamt), in coordination with the FBI and our other federal partners in the Drug Enforcement Administration, the Internal Revenue Service, U.S. Postal Inspection Service, Homeland Security Investigations, and Organized Crime Drug Enforcement Task Forces. The FBI used technical expertise and legal authorities, and, most importantly, our worldwide partnerships to significantly disrupt this illegal marketplace.

In March, the FBI conducted a successful court-authorized operation to remove botnet malware known as Cyclops Blink from the botnet's command and control devices, cutting off the Russian Main Intelligence Directorate's (GRU) control over thousands of infected devices—mainly in small to mid-sized businesses—worldwide. The GRU had been building this malicious botnet, which ultimately spanned the globe, as early as June 2019, as a replacement for the VPNFilter malware we exposed and disrupted in 2018. Over several months, the FBI worked closely with WatchGuard Technologies, the developer of many of the infected devices, to analyze the malware, and WatchGuard developed detection tools and remediation techniques. In February, before the FBI's technical disruption, the FBI, NSA, CISA, and the UK's National Cyber Security Centre proactively released an advisory identifying the Cyclops Blink malware. That same day, WatchGuard released the detection and remediation tools. This latest disruption,

in addition to highlighting the benefits of close public-private partnerships, proves that success against cyber threats doesn't only involve arrests and convictions.

In total, we took over 1,100 actions against cyber adversaries last year, 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 more than 100 public threat advisories by way of Joint Cybersecurity Advisories, FBI Liaison Alert System ("FLASH") reports, Private Industry Notifications ("PINs"), and Public Service Announcements ("PSAs")—many of which were jointly authored with other U.S. agencies and international partners.

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

In summation, 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 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, disrupt, and hold accountable those who pose a threat in cyberspace.

Foreign Intelligence Threats

Top Threats

We see nations such as China, Russia, and Iran becoming more aggressive and more capable in their nefarious activity than ever before. These nations seek to undermine our core democratic, economic, and scientific institutions. They employ a growing range of tactics to

advance their interests and to harm the United States. Defending American institutions and values against these threats is a national security imperative and a priority for the FBI.

With that, the greatest long-term threat to our nation's ideas, innovation, and economic security is the foreign intelligence and economic espionage threat from China. It's a threat to our economic security—and by extension—to our national security. The Chinese government aspires to equal or surpass the United States as a global superpower and influence the world with a value system shaped by undemocratic authoritarian ideals. The pursuit of these goals is often with little regard for international norms and laws.

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

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

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

The Department of Defense has been a key partner in the NCITF since its founding in 2019. While the FBI has had long-term collaborative relationships with DoD entities such as the Air Force Office of Special Investigations, Naval Criminal Investigative Service, and Army Counterintelligence, the NCITF has allowed us to enhance our collaboration with each other for

greater impact. We plan to emphasize this whole-of-government approach moving forward as a powerful formula to mitigate the modern counterintelligence threat.

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. It's important to note countries like China, Russia and Iran, stalk, intimidate, and harass certain people in the U.S. This is called transnational repression. It's illegal and the FBI is investigating it.

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

Foreign Malign Influence

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

Foreign malign influence is not a new problem, but the interconnectedness of the modern world, combined with the anonymity of the Internet, have changed the nature of the threat and how the FBI and its partners must address it. Foreign malign influence operations have taken many forms and used many tactics over the years. Most widely reported these days are attempts by adversaries—hoping to reach a wide swath of Americans covertly from outside the United States—to amplify existing stories on social media in an attempt to discredit U.S. individuals and institutions.

The FBI is the lead federal agency responsible for investigating foreign malign influence threats. Several years ago, we established the Foreign Influence Task Force ("FITF") to identify and counteract foreign malign influence operations targeting the United States. The FITF is led by the Counterintelligence Division and comprises agents, analysts, and professional staff from the Counterintelligence, Cyber, Counterterrorism, and Criminal Investigative Divisions. It is specifically charged with identifying and combating foreign malign influence operations

targeting democratic institutions and values inside the United States. In all instances, the FITF strives to protect democratic institutions, develop a common operating picture, raise adversaries' costs, and reduce their overall asymmetric advantage.

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

Following the 2018 midterm elections, we reviewed the threat and the effectiveness of our coordination and outreach. As a result of this review, we further expanded the scope of the FITF. Previously, our efforts to combat malign foreign influence focused solely on the threat posed by Russia. Utilizing lessons learned since 2018, the FITF widened its aperture to confront malign foreign operations of the PRC, Iran, and other global adversaries. To address this expanding focus and wider set of adversaries and influence efforts, we have also added resources to maintain permanent "surge" capability on election and foreign influence threats.

In addition, the domestic counterintelligence environment is more complex than ever. This nation faces a persistent and pervasive national security threat from foreign adversaries, particularly Russia and China, conducting sophisticated intelligence operations using coercion, subversion, malign influence, disinformation, cyber and economic espionage, traditional spying and non-traditional human intelligence collection. Together, they pose a continuous threat to U.S. national security and its economy by targeting strategic technologies, industries, sectors, and critical infrastructures. Historically, these asymmetric national security threats involved foreign intelligence service officers seeking U.S. Government and U.S. Intelligence Community information. The FBI has observed foreign adversaries employing a wide range of nontraditional collection techniques, including the use of human collectors not affiliated with intelligence services, foreign investment in critical U.S. sectors, and infiltration of U.S. supply chains. The FBI continues to adjust its CI priorities and posture to address the evolving and multifaceted threat.

Criminal Threats

We continue to face many criminal threats, from complex white-collar fraud in the financial, health care, and housing sectors to transnational and regional organized criminal enterprises to violent crime and public corruption. Criminal organizations—domestic and international—and individual criminal activity represent a significant threat to our 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 and 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, territorial, and tribal officers and deputies on joint task forces and individual investigations.

Like the FBI's work combatting gangs, the FBI also investigates the most serious crimes in Indian Country—such as murder, child sexual and physical abuse, violent assaults, domestic violence, drug trafficking, public corruption, financial crimes, and Indian gaming violations. As you are aware, there are 574 federally recognized American Indian Tribes in the United States, and the FBI has federal law enforcement responsibility on 188 Indian reservations. The FBI coordinates and collaborates with the Bureau of Indian Affairs ("BIA"), Office of Justice Services; and other federal, state, and Tribal partners across the United States to investigate crimes in Indian Country."

Over the past two years, the FBI's work in Indian Country increased significantly due to the July 9, 2020, Supreme Court ruling in *McGirt v. Oklahoma*, which determined that the original boundaries of the Muscogee Creek Nation ("MCN") were never disestablished. This decision had the practical effect of requiring all land within MCN's territorial boundaries to fall under federal Indian Country jurisdiction, thus expanding the FBI's responsibility for investigating felony offenses committed by or against an Indian. The principles of the *McGirt* decision also apply to Cherokee, Chickasaw, Choctaw, Seminole, and Quapaw Tribal territories in Oklahoma. Combined, all six reservations encompass approximately 32,000 square miles, or 45 percent of the State of Oklahoma. The total population within the combined borders is roughly 1.9 million, of which approximately 420,000 are enrolled Tribal members.

This drastic increase in FBI jurisdiction has significant and long-term operational and public safety implications given the increased number of violent criminal cases now under federal jurisdiction within Oklahoma's Indian Country. Since this decision, the FBI's Oklahoma City Field Office ("OC") has seen a drastic increase in the total number of Indian Country investigations and now has the FBI's largest investigative responsibility. Since the federal court ruling in the *McGirt* case, the FBI's Oklahoma City field office, which previously investigated approximately 50 criminal cases a year involving Native Americans, has managed thousands of Indian Country cases, prioritizing cases involving the most violent offenders who pose the most serious risk to the public.

To effectively conduct these investigations, the FBI has conducted temporary duty ("TDY") rotations of Special Agents, Intelligence Analysts, Victim Specialists and other professional staff to the Muskogee and Tulsa RAs, the offices most impacted by the decision. The FBI has also expanded state, local, and tribal participation on task forces to assist with

response and investigative efforts. To support the U.S. Attorney's effective prosecution of these crimes, the FBI must have the capability to sustain an enhanced presence in FBI OC.

The FBI is committed to its mission of protecting Tribal communities through its Indian Country investigative program. With more than 150 Special Agents and 23 Safe Trails Task Forces around the country, the FBI has demonstrated its commitment to the safety and security of indigenous people by vigorously investigating the most serious crimes facing their communities. The FBI works to enhance its effectiveness by leveraging its relationships with its state, local and federal partners, both on and off the reservations.

The 2020 *McGirt* decision significantly increased the FBI's investigative responsibilities in Oklahoma by dramatically increasing both its territorial jurisdiction and caseload requirements. Furthermore, the decision created a jurisdictional gap, in that a large number of general crimes affecting Native American victims became unaddressed. In response the FBI surged national resources to ensure it was able to address its mission requirements to investigate major crimes in the newly designated Tribal Territory. These surges subsequently caused resource strains on other investigative programs and threats. The *Castro-Huerta* decision began to relieve that pressure and has the future potential to reduce FBI caseloads by an estimated 15% – 20% in Oklahoma, while bridging the jurisdictional gap by allowing state authorities to address certain general crimes. This would free FBI resources to return to other national threat issues, while still providing Tribal communities with the FBI law enforcement services they've historically relied on.

The FBI fully recognizes and supports Tribal sovereignty while still seeking innovative ways to service the law enforcement needs of indigenous communities. The FBI believes ensuring public safety is a top priority and *Castro-Huerta* provides an avenue of bolstering that safety with the addition of state law enforcement services, while relieving resource burdens on the FBI. The FBI therefore supports the underlying policy as established in *Castro-Huerta* and would be opposed to legislation to abrogate the decision.

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 targeting stock market fraud and manipulation, cyber-facilitated bank fraud and embezzlement, drug trafficking, identity theft, human trafficking, money laundering, human smuggling, public corruption, weapons trafficking, extortion, kidnapping, wildlife and timber trafficking, illegal fishing, illegal mining, 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.

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 emerging technology to traffic illicit drugs and contraband across international borders and into the U.S.

Crimes Against Children and Human Trafficking

It is unthinkable, but every year, thousands of children become victims of crimes, whether it is through kidnappings, violent attacks, sexual abuse, human trafficking, or online predators. The FBI is uniquely positioned to provide a rapid, proactive, and comprehensive response; identify, locate, and recover child victims; and strengthen relationships between the FBI and federal, state, local, tribal, and international law enforcement partners to identify, prioritize, investigate, and deter individuals and criminal networks from exploiting children.

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

The FBI combats this pernicious crime problem through investigations such as Operation Pacifier, which targeted the administrators and users of a highly sophisticated, Tor-based global enterprise dedicated to the sexual exploitation of children. This multi-year operation led to the arrest of approximately 350 individuals based in the United States, the prosecution of 25 American child pornography producers and 51 American hands-on abusers, the rescue or identification of 55 American children, the arrest of 548 international individuals, and the identification or rescue of 296 children abroad.

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

the FBI also has the ability to quickly collaborate with partners throughout the world, which plays an integral role in crime prevention.

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

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

The majority of human trafficking victims recovered during FBI investigations are United States citizens, but traffickers are opportunists who will exploit any victim with a vulnerability, including foreign nationals and victims of all ages, by subjecting them to forced labor or sex trafficking. We take a victim-centered, trauma-informed approach to investigating these cases and strive to ensure the needs of victims are fully addressed at all stages. To accomplish this, the FBI works in conjunction with other law enforcement agencies and victim specialists on the local, state, tribal, and federal levels, as well as with a variety of vetted non-governmental organizations. Even after the arrest and conviction of human traffickers, the FBI often continues to work with partner agencies and organizations to assist victims and survivors in moving beyond their exploitation.

Civil Rights

The FBI remains dedicated to protecting the cherished freedoms of all Americans. Civil rights crimes are among the most egregious violations of federal law—they include color of law violations, hate crimes, Freedom of Access to Clinic Entrances ("FACE") Act violations, and voter suppression. These crimes cause long-term, enduring damage to communities and economic infrastructure, compromise law enforcement and judicial system capabilities, and provoke widespread fear and trauma. We also support the work and cases of our state and local partners, as needed.

The investigation of hate crimes is the number one priority within the FBI's civil rights program due to the devastating effect these types of crimes can have not just on the victims and their families, but also on entire communities. A hate crime is a criminal offense against a person or property motivated in whole or in part by the perpetrator's bias against a race, religion, disability, ethnic/national origin, sexual orientation, gender, or gender identity. While the First Amendment to the Constitution allows for the free expression of both offensive and hateful speech, this protection does not extend to criminal acts, even those done to express an idea or belief. The First Amendment also does not protect someone who issues a true threat to inflict physical harm on individuals or groups, or who intentionally solicits others to commit unlawful

acts of violence on his or her behalf. The FBI remains dedicated to investigating these types of crimes.

Beyond investigative work, the FBI recognizes proper and thorough handling of civil rights crimes does not begin the moment they are reported—it begins before they occur, with a solid and trusting relationship between the community and law enforcement. Each FBI field office will be taking specific actions to combat civil rights crimes in their area of responsibility ("AOR") to encourage systemic change. These actions include identifying appropriate partner agencies and local groups to develop outreach relationships at all levels, especially those that will spark institutional change; increasing civil rights-focused working groups and task forces with federal, state, local, private, public, and non-profit partners; and providing increased training for State and local agencies and community groups centered on color of law investigations and hate crimes statutes to provide education about civil rights violations, promote increased reporting of hate crimes, and rebuild community trust in law enforcement.

Furthermore, we are focused on working with our state and local partners to collectively do a better job of tracking and reporting hate crime and color of law violations to fully understand what is happening in our communities and how to stop it. Our ability to address significant national issues, such as the use of force and officer-involved shootings and jurisdictional increases in violent crime, depends on fuller statistical understanding of the underlying facts and circumstances. Some jurisdictions fail to report hate crime statistics, while others claim there are no hate crimes in their community—a fact that would be welcome, if true. We are dedicated to working vigorously with our state and local counterparts in every jurisdiction to better track and report hate crimes, in an accurate, timely, and publicly transparent manner.

Lawful Access

The FBI remains a strong advocate for the wide and consistent use of encryption. Protecting data and privacy in a digitally connected world is a top priority for the FBI, and we believe that promoting encryption is a vital part of that mission. Encryption without lawful access, though, does have a negative effect on law enforcement's ability to protect the public. As I have testified previously, when the FBI discusses lawful access, we mean putting providers who manage encrypted data in a position to decrypt it and provide it to us in response to a legal process. We do not mean for encryption to be weakened or compromised so that it can be defeated from the outside by law enforcement or anyone else. Unfortunately, too much of the debate over lawful access has revolved around discussions of this concept that the FBI would not support.

The problems caused by law enforcement agencies' inability to easily access electronic evidence continue to grow. Increasingly, commercial device manufacturers have employed encryption in such a manner that only the device users can access the content of the devices. Similarly, more and more communications service providers are designing their platforms and apps such that only the parties to the communication can access the content. This is generally

known as “end-to-end” encryption. The proliferation of end-to-end encryption is a serious issue that increasingly limits law enforcement’s ability, even after obtaining a lawful warrant or court order, to access critical evidence and information needed to disrupt threats, protect the public, and bring perpetrators to justice.

For example, even with our substantial resources, accessing the content of known or suspected terrorists’ data pursuant to court-authorized legal process is increasingly difficult. The often-online nature of the terrorist radicalization process, along with the insular nature of most of today’s attack plotters, leaves fewer dots for investigators to connect in time to stop an attack, and end-to-end encryption increasingly hide even those often precious few and fleeting dots.

In one instance, while planning—and right up until the eve of—the December 6, 2019, shooting at Naval Air Station Pensacola that killed three U.S. sailors and severely wounded eight other Americans, deceased terrorist Mohammed Saeed Al-Shamrani communicated undetected with overseas al Qaeda terrorists using an end-to-end encrypted app. Then, after the attack, encryption prevented the FBI from accessing information contained in his phones for several months. As a result, during the critical time period immediately following the shooting and despite obtaining search warrants for the deceased killer’s devices, the FBI could not access the information on those phones to identify co-conspirators or determine whether they may have been plotting additional attacks.

This problem spans international and domestic terrorism threats. For example, subjects of our investigation into the January 6 Capitol siege used end-to-end encrypted communications.

We face the same problem in protecting children against violent sexual exploitation. End-to-end encryption frequently prevent us from discovering and searching for victims, since the vital tips we receive from providers only arrive when those providers themselves are able to detect and report child exploitation being facilitated on their platforms and services.

When we are able to open investigations, end-to-end encryption make it much more difficult to bring perpetrators to justice. Much evidence of crimes against children, just like the evidence of many other kinds of crime today, exists primarily in electronic form. If we cannot obtain that critical electronic evidence, our efforts are frequently hamstrung.

This problem is not just limited to federal investigations. Our state and local law enforcement partners have been consistently advising the FBI that they, too, are experiencing similar end-to-end encryption challenges, which are now being felt across the full range of state and local criminal law enforcement. Many report that even relatively unsophisticated criminal groups, like street gangs, are frequently using encrypted smartphones and end-to-end encrypted communications apps to shield their activities from detection or disruption. As this problem becomes more and more acute for state and local law enforcement, the advanced technical resources needed to address even a single investigation involving end-to-end encryption will continue to increase.

Conclusion

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

Chairman Peters, Ranking Member Portman, and Members of the Committee, thank you for the opportunity to testify today. I am happy to answer any questions you might have.