Department of Justice

STATEMENT OF

CHRISTOPHER A. WRAY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED

"OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION"

PRESENTED

AUGUST 4, 2022

STATEMENT OF
CHRISTOPHER A. WRAY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED
"OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION"

PRESENTED
AUGUST 4, 2022

Good afternoon, Chairman Durbin, Ranking Member Grassley, 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. 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 matters facing the FBI and the Nation as a whole.

National Security

Top Terrorism Threats

Preventing terrorist attacks, from any place, by any actor, remains the FBI's top priority. The nature of the threat posed by terrorism – both international terrorism ("IT") and domestic terrorism ("DT") – continues to evolve.

The greatest terrorism threat to our Homeland is posed by lone actors or small cells who typically radicalize to violence online and look to attack soft targets with easily accessible

weapons. We see these threats manifested within both Domestic Violent Extremists ("DVEs") and Homegrown Violent Extremists ("HVEs"), two distinct threats, both of which are located primarily in the United States and typically radicalize and mobilize to violence on their own. Individuals who commit violent criminal acts in furtherance of social or political goals stemming from domestic influences – some of which include racial or ethnic bias, or antigovernment or anti-authority sentiments – are described as DVEs, whereas HVEs are individuals who are inspired primarily by international terrorist actors but are not receiving individualized direction from Foreign Terrorist Organizations ("FTOs") or Specially Designated Global Terrorists ("SDGTs").

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. By selecting these types of soft targets, in addition to the insular nature of their radicalization and mobilization to violence and limited discussions with others regarding their plans, lone actors present a persistent challenge for law enforcement who work to detect and disrupt their activities before they occur.

The top domestic terrorism threat we face continues to be from DVEs we categorize as Racially or Ethnically Motivated Violent Extremists ("RMVEs"), including those who advocate for the superiority of the white race, who were the primary source of lethal attacks perpetrated by DVEs in recent years. It is important to note that we have also recently seen an increase in fatal DVE attacks perpetrated by Anti-Government or Anti-Authority Violent Extremists, specifically Militia Violent Extremists and Anarchist Violent Extremists. Anti-Government or Anti-Authority Violent Extremists were responsible for three of the four lethal DVE attacks in 2020. Also, in 2020, we saw the first lethal attack committed by an Anarchist Violent Extremist in over 20 years. These Anti-Government or Anti-Authority Violent Extremists have specifically targeted law enforcement and the military as well as institutions or members of the U.S. Government.

The number of FBI investigations of suspected DVEs has more than doubled since the spring of 2020. In January, we marked the one-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 850 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 policy to address the many facets of the domestic terrorism threat.

The FBI assesses HVEs are the greatest, most immediate international terrorism ("IT") threat to the Homeland. As I have described, HVEs are people located and radicalized to violence primarily in the United States, who are not receiving individualized direction from FTOs but are inspired largely by foreign terrorist organizations 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 or SDGT, 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 that 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.

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 scores of victims by hacking just one provider.

These criminals and nation-states believe that they can compromise our networks, steal our property, 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 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. We have seen Iran use cyber means to try to sow divisions and undermine our elections, targeting voters before elections and threatening election officials after. 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, and educational institutions for theft or ransomware. Such incidents affecting medical centers 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. And we have seen criminal groups targeting critical infrastructure for ransom, causing massive disruption to our daily lives.

We have also seen the rise of an ecosystem of services dedicated to supporting cybercrime in exchange for cryptocurrency. For example, "bullet-proof" hosts refuse to

cooperate with law enforcement authorities, allowing criminals to carry out criminal schemes without being identified or taken offline; "ransomware-as-a-service" groups lease their ransomware for a fee; "crypters" assist criminals by ensuring that their malware will not be detected by anti-virus software; and "mixers" and "tumblers" help criminals hide illicit virtual currency payments. 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 do what they are doing. 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 transaction conducted on Hydra. In 2021, Hydra accounted for an estimated 80% of all darknet market-related cryptocurrency transactions, and since 2015, the marketplace has 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, and Homeland Security Investigations. 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 GRU's 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 to analyze the malware, and WatchGuard developed detection tools and

remediation techniques. In February, before the 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 imposing risk and consequences 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.

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. 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 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 really 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 and hold accountable those who pose a threat in cyberspace.

Foreign 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 is comprised of 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.

These additional resources were also devoted to working with U.S. Government partners on two documents regarding the U.S. Government's analysis of foreign efforts to influence or interfere with the 2020 Election. The main takeaway from both reports is there is no evidence — not through intelligence collection on the foreign actors themselves, not through physical security and cybersecurity monitoring of voting systems across the country, not through

postelection audits, and not through any other means — that a foreign government or other actors compromised election infrastructure to manipulate election results.

The FBI will continue to investigate this threat leading up to the FY 2022 mid-term election and will not stop working with our partners to impose costs on adversaries who have or are seeking to influence or interfere in our elections.

In addition, the domestic counterintelligence environment is more complex than ever, posing a continuous threat to U.S. national security and its economy by targeting strategic technologies, industries, sectors, and critical infrastructures. Historically, asymmetric CI threats involved foreign intelligence service officers seeking 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, 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, drug trafficking, public corruption, financial crimes, and Indian gaming violations. As you are aware, there are almost 600 federally recognized American Indian Tribes in the United States, and the FBI has Federal law enforcement responsibility on nearly 200 Indian reservations. This Federal jurisdiction is shared concurrently with the Bureau of Indian Affairs ("BIA"), Office of Justice Services; the FBI works very closely with BIA and other Federal, State, and Tribal partners across the United States on crimes in Indian Country.

Over the past year, 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 territorial boundaries of the Muscogee Creek Nation ("MCN") would fall under Federal Indian Country jurisdiction, expanding the FBI's responsibility for investigating felony offenses committed by or victimizing a Tribal member. The principles of the McGirt decision also apply to the status of the Cherokee, Chickasaw, Choctaw, Seminole, and Quapaw Tribal territories in Oklahoma. Combined, all six reservation territories encompass approximately 32,000 square miles, or 45 percent of the State of Oklahoma. The total population within the combined borders is roughly 1.9 million, of which approximately 420,000 are enrolled Tribal members.

This drastic increase in FBI jurisdiction 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 territory. 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. The U.S. Attorney's Offices in the Eastern District of Oklahoma and the Northern District of Oklahoma also increased their staffing. 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.

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 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 Teams, 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.

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 has 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.

Child Abduction Rapid Deployment Teams are ready response teams stationed across the country to quickly respond to abductions. Investigators bring to this issue the full array of forensic tools such as DNA analysis, trace evidence, impression evidence, and digital forensics. Through improved communications, law enforcement also has the ability to quickly share information with partners throughout the world, and these outreach programs play an integral role in prevention.

In addition to programs to combat child exploitation, the FBI also focuses efforts to stop human trafficking. 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 as well as U.S. citizens, and adults as well as minors — subjecting them to forced labor or sex trafficking. The FBI is working hard with its partners to combat all forms. The FBI works collaboratively with law enforcement partners to investigate and arrest human traffickers through Human Trafficking Task Forces nationwide. 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, voter suppression, and human trafficking, which I just discussed. 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 local and State 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 individual'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 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 problems caused by law enforcement agencies' inability to 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. This is commonly referred to as "user-only-access" device encryption. 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 and user-only-access 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.

The FBI remains a strong advocate for the wide and consistent use of responsibly-managed 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 legal process. We do not mean a "backdoor," that is, 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 "backdoor" concept that the FBI would not support.

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 and user-only-access 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, user-only-access 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 as well.

We face the same problem in protecting children against violent sexual exploitation. End-to-end and user-only-access 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. They cannot do that when their platforms are end-to-end encrypted.

When we are able to open investigations, end-to-end and user-only-access encryption makes 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 and user-only-access 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 user-only-access 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 and user-only-access encryption will continue to diminish and ultimately the capacity of State and local law enforcement to investigate even common crimes will be overwhelmed.

Conclusion

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

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