Department of Justice

STATEMENT OF

CHRISTOPHER A. WRAY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
COMMITTEE ON THE JUDICIARY
U.S. HOUSE OF REPRESENTATIVES

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

PRESENTED
JUNE 10, 2021

STATEMENT OF
CHRISTOPHER A. WRAY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
COMMITTEE ON THE JUDICIARY
U.S. HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED
"FBI OVERSIGHT"

PRESENTED
JUNE 10, 2021

Good morning, Chairman Nadler, Ranking Member Jordan, and Members of the Committee. I am honored to be here, representing the men and women of the FBI. Our people — nearly 37,000 of them — are the heart of the Bureau. I am proud of their service and their commitment to our mission. Every day, they tackle their jobs with perseverance, professionalism, and integrity – sometimes at the greatest of costs.

Earlier this year, two of our agents made the ultimate sacrifice in the line of duty. Special Agents Dan Alfin and Laura Schwartzenberger left home to carry out the mission they signed up for – to keep the American people safe. They were executing a federal court-ordered search warrant in a violent crimes against children investigation in Sunrise, Florida, when they were shot and killed. Three other agents were also wounded that day. We'll be forever grateful for their commitment and their dedication – for their last full measure of devotion to the people they served and defended. We will always honor their sacrifice.

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 has faced unimaginable challenges this past year. Yet, through it all, whether it was coming to the aid of our partners during the Capitol siege and committing all of our resources to ensuring that those involved in that brutal assault on our Democracy are brought to justice, the proliferation of terrorist violence moving at the speed of social media, abhorrent hate crimes, COVID-19 related fraud and misinformation, the increasing threat of cyber intrusions and state-sponsored economic espionage, malign foreign influence and interference, the scourge of opioid trafficking and abuse, or human trafficking and crimes against children, 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 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 our organization and the Nation as a whole.

Capitol Violence

First and foremost, I want to assure you, your staff, and the American people that the FBI has deployed our full investigative resources and is working closely with our federal, State, local, Tribal, and territorial partners to aggressively pursue those involved in criminal activity during the events of January 6, 2021. We are working closely with our federal, state, and local law enforcement partners, as well as private sector partners, to identify those responsible for the violence and destruction of property at the U.S. Capitol building who showed blatant and appalling disregard for our institutions of government and the orderly administration of the democratic process.

FBI Special Agents, Intelligence Analysts, and professional staff have been hard at work gathering evidence, sharing intelligence, and working with federal prosecutors to bring charges against the individuals involved. As we have said consistently, we do not and will not tolerate violent extremists who use the guise of First Amendment-protected activity to engage in violent criminal activity. Thus far, the FBI has arrested hundreds of individuals with regards to rioting, assault on a federal officer, property crimes violations, and conspiracy charges, and the work continues.

Overall, the FBI assesses that the January 6th siege of the Capitol Complex demonstrates a willingness by some to use violence against the government in furtherance of their political and social goals. This ideologically motivated violence underscores the symbolic nature of the National Capital Region and the willingness of some Domestic Violent Extremists to travel to events in this area and violently engage law enforcement and their perceived adversaries. The American people should rest assured that we will continue to work to hold accountable those individuals who participated in the violent breach of the Capitol on January 6th, and any others who attempt to use violence to intimidate, coerce, or influence the American people or affect the conduct of our government.

Top Terrorism Threats

As has been stated multiple times in the past, 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 online and look to attack soft targets with easily accessible weapons. We see these threats manifested within both Domestic Violent Extremists ("DVEs") and

Homegrown Violent Extremists ("HVEs"), two distinct threats, both of which are located primarily in the United States and typically radicalize and mobilize to violence on their own. Individuals who commit violent criminal acts in furtherance of social or political goals stemming from domestic influences – some of which include racial or ethnic bias, or anti-government or anti-authority sentiments – are described as DVEs, whereas HVEs are individuals who are inspired primarily by global jihad but are not receiving individualized direction from Foreign Terrorist Organizations ("FTOs").

Domestic and Homegrown Violent Extremists are often motivated and inspired by a mix of socio-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. 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, increases the challenge faced by law enforcement to detect and disrupt the activities of lone actors before they occur.

The top threat we face from DVEs continues to be from those we categorize as Racially or Ethnically Motivated Violent Extremists ("RMVEs"), largely those who advocate for the superiority of the white race, who were the primary source of lethal attacks perpetrated by DVEs in 2018 and 2019. 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.

Consistent with our mission, the FBI does not investigate First Amendment-protected speech or association, peaceful protests, or political activity. The FBI holds sacred the rights of individuals to peacefully exercise their First Amendment freedoms. Non-violent protests are signs of a healthy democracy, not an ailing one. Regardless of their specific ideology, the FBI will aggressively pursue those who seek to hijack legitimate First Amendment-protected activity by engaging in violent criminal activity such as the destruction of property and violent assaults on law enforcement officers that we witnessed on January 6th and during protests throughout the U.S. during the summer of 2020 and beyond. In other words, we will actively pursue the opening of FBI investigations when an individual uses – or threatens the use of – force, violence, or coercion, in violation of federal law and in the furtherance of social or political goals.

The FBI assesses HVEs are the greatest, most immediate IT threat to the Homeland. As I have described, HVEs are located in and radicalized primarily in the United States, who are not receiving individualized direction from global jihad-inspired FTOs but are inspired largely by the Islamic State of Iraq and ash-Sham ("ISIS") and al-Qa'ida 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 them.

The FBI remains concerned that FTOs, such as ISIS and al-Qa'ida, 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. To this day, ISIS continues 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 seeking a sense of belonging 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, in the near term, we assess 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. Lebanese Hizballah has sent operatives to build terrorist infrastructures worldwide. The arrests of individuals in the United States allegedly linked to Lebanese Hizballah's main overseas terrorist arm, and their intelligence collection and procurement efforts, demonstrate Lebanese Hizballah's interest in long-term contingency planning activities here in the Homeland. Lebanese Hizballah Secretary-General Hasan 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.

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 – encryption that providers can decrypt and provide to law enforcement when served with a legal order. Protecting data and privacy in a digitally connected world is a top priority for the FBI and the U.S. government, and we believe that promoting encryption is a vital part of that mission. But we have seen that the broad application of end-to-end and user-only-access encryption adds negligible security advantages. It does have a negative effect on law enforcement's ability to protect the public. What we mean when we talk about lawful access is putting providers who manage encrypted data in a position to decrypt it and provide it to us in response to legal process. We are not asking for, and do not want, any "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" straw man instead of what we really want and need.

We are deeply concerned with the threat end-to-end and user-only-access encryption pose to our ability to fulfill the FBI's duty of protecting the American people from every manner of federal crime, from cyber-attacks and violence against children to drug trafficking and organized crime. We believe Americans deserve security in every walk of life – in their data, their streets, their businesses, and their communities.

End-to-end and user-only-access encryption erode that security against every danger the FBI combats. 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-Qa'ida 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. Like Al-Shamrani, the plotters who sought to kidnap the Governor of Michigan late last year used end-to-end encrypted apps to hide their communications from law enforcement. Their plot was only disrupted by well-timed human source reporting and the resulting undercover operation. 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. For example, while Facebook Messenger and Apple iMessage each boasts over one billion users, in 2020, the National Center for Missing and Exploited Children ("NCMEC") received over 20 million tips from Facebook[1], compared to 265 tips from Apple, according to NCMEC data and publicly available information. Apple's use of end-to-end encryption, which blinds it to child sexual abuse material being transmitted through its services, likely plays a role in the disparities in reporting between the two companies. We do not know how many children are being harmed across the country as a result of this under-reporting by Apple and other end-to-end providers.

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 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

[1]Facebook is planning to move its Facebook Messenger platform to end-to-end encryption as a default in the near future. This will result in the loss of even these tips.

involving end-to-end and user-only-access encryption will continue to diminish and ultimately overwhelm State and local capacity to investigate even common crimes.

Cyber

In 2020, nation-state and criminal cyber actors took advantage of people and networks made more vulnerable by the sudden shift of our personal and professional lives online due to the COVID-19 pandemic, targeting those searching for personal protective equipment, worried about stimulus checks, and conducting vaccine research.

Throughout the last year, the FBI has seen a wider-than-ever range of cyber actors threaten Americans' safety, security, and confidence in our digitally connected world. But these threats will not disappear when the pandemic ends. 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 as a way to access scores of victims by hacking just one provider.

These criminals and nation-states believe that they can compromise our networks, steal our property, and hold our critical infrastructure at risk without incurring any risk themselves. In the last year alone, we have seen – and have publicly called out – China, North Korea, 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 China working to obtain controlled defense technology and developing the ability to use cyber means to complement any future real-world conflict. We have seen Iran use cyber means to try to sow divisions and undermine our elections, targeting voters before the November election and threatening election officials after.

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 cyber criminals 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 are also seeing dark web vendors who sell capabilities in exchange for cryptocurrency increase the difficulty of stopping what would once have been less dangerous offenders. What was once a ring of unsophisticated criminals now has the tools to paralyze entire hospitals, police departments, and businesses with ransomware. It is not that individual hackers alone have necessarily become much more sophisticated, but — unlike previously — they are able to rent sophisticated capabilities.

We have to make it harder and more painful for hackers and criminals to do what they are doing. That is why I announced a new FBI cyber strategy last year, using the FBI's role as the lead federal agency with law enforcement and intelligence responsibilities to not only pursue our own actions, but to work seamlessly with our 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.

An example of this approach is the international takedown in January 2021 of the Emotet botnet, which enabled a network of cyber criminals to cause hundreds of millions of dollars in damages to government, educational, and corporate networks. The FBI used sophisticated techniques, our unique legal authorities, and, most importantly, our worldwide partnerships to significantly disrupt the malware.

A few months ago, cybersecurity companies including Microsoft disclosed that hackers were using previously unknown vulnerabilities related to Microsoft Exchange software to access email servers that companies physically keep on their premises rather than in the cloud. These "zero day" vulnerabilities allowed the actors to potentially exploit victim networks, engaging in activities such as grabbing login credentials, installing malicious programs to send commands to the victim network, and stealing emails in bulk. The FBI first put out a joint advisory in partnership with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA") to give network defenders the technical information they needed to mitigate the vulnerability. However, while many infected system owners successfully removed the web shells others were not able to do so. That left many systems vulnerable to adversaries who could continue to steal information, encrypt data for ransom, or potentially even execute a destructive attack. In response, through a court-authorized operation in partnership with the private sector, we were able to copy and remove malicious web shells from hundreds of vulnerable computers in the U.S. running Microsoft Exchange Server software. This is another example of how the FBI used its unique authorities, in this case, court-issued legal process, and its partnerships with the private sector to have tangible, real-world impact on the problem.

We took upwards of 1,100 actions against cyber adversaries last year, including arrests, criminal charges, convictions, dismantlements, and disruptions, and enabled many more actions through our dedicated partnerships with the private sector, foreign partners, and at the federal, State, and local entities.

We have been putting a lot of energy and resources into all of 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 a breach; how we protect information that companies, and universities share with us, and commit to providing useful feedback; and how we coordinate 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 incident — SolarWinds, HAFNIUM, 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.

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. The FBI and our interagency partners remain concerned about, and focused on, the covert and overt influence measures used by certain adversaries 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 processes.

Foreign influence operations — which include subversive, undeclared, coercive, and criminal actions by foreign governments to influence U.S. political sentiment or public discourse or interfere in our processes themselves — are 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 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 use false personas and fabricated stories on social media platforms to discredit U.S. individuals and institutions.

The FBI is the lead federal agency responsible for investigating foreign influence operations. In the fall of 2017, we established the Foreign Influence Task Force ("FITF") to identify and counteract malign foreign 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 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 China, 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 reports are separate but complementary. The first report — referred to as the 1a report and authored by the Office of the Director of National Intelligence — outlines the intentions of foreign adversaries with regard to influencing and interfering in the election but does not evaluate impact. The second report — referred to as the 1b report and authored by the Department of Justice, including the FBI, and Department of Homeland Security, including the CISA — evaluates the impact of foreign government activity on the security or integrity of election infrastructure or infrastructure pertaining to political organizations, candidates, or campaigns.[2]

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

While the 2020 election is over, the FBI will not stop working with our partners to impose costs on adversaries who have or are seeking to influence or interfere in our elections.

Conclusion

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

[2]These reports are required by sections 1(a) and 1(b) of Executive Order 13,848.

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