Department of Justice

STATEMENT OF

CHRISTOPHER A. WRAY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

SELECT COMMITTEE ON STRATEGIC COMPETITION BETWEEN THE UNITED STATES AND THE CHINESE COMMUNIST PARTY
U.S. HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED
"THE CCP CYBER THREATS TO THE AMERICAN HOMELAND AND NATIONAL SECURITY"

PRESENTED
JANUARY 31, 2024

STATEMENT OF
CHRISTOPHER A. WRAY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
SELECT COMMITTEE ON STRATEGIC COMPETITION BETWEEN THE UNITED STATES AND THE CHINESE COMMUNIST PARTY
U.S. HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED
"THE CCP CYBER THREATS TO THE AMERICAN HOMELAND AND NATIONAL SECURITY"

PRESENTED
JANUARY 31, 2024

Good morning, Chairman Gallagher, Ranking Member Krishnamoorthi, distinguished Members of the Committee, thank you for inviting me to testify about the ongoing efforts of the Federal Bureau of Investigation (FBI) to identify, disrupt, and impose cost on People's Republic of China (PRC) cyber actors.

Cybersecurity is national security, and that has never been more apparent than it is today. In recent years, PRC actors have become increasingly stealthy and sophisticated, making our ability to detect and disrupt them even more difficult.

To combat this threat, the FBI has over 1,000 cyber personnel distributed throughout the United States who respond to incidents every single day. As the most geographically distributed cyber workforce in the federal government, the FBI responds to intrusions that affect not only U.S. critical infrastructure and big-name corporations, but also small businesses, our schools, and local government services in the communities you represent. The FBI's response to each one of those incidents supports victims and allows us to learn how our adversaries operate—and who they might target next. We share that insight with cybersecurity agencies, the U.S. Intelligence Community (USIC), private industry, and international partners, so the global community of those fighting against cyber threats benefits from the FBI's access and authorities.

"Investigations" are the umbrella under which the FBI conducts its activities, but that term should not imply that we only respond to events after the fact. Just the opposite: the FBI is focusing our unique authorities—and our ability to engage with international law enforcement, domestic targeted entities and victims, and key technology service providers—to identify and disrupt cyber adversaries before they compromise U.S. networks.

The information that the FBI uniquely collects assists our partner agencies, such as the Cybersecurity and Infrastructure Security Agency (CISA), as we work together to counter our adversaries. For example, FBI collection helps to identify other networks vulnerable to the same adversary technique. We help sector risk management agencies assess and mitigate cyber threats

to critical infrastructure. We often provide U.S. Cyber Command or the National Security Agency (NSA) information on a piece of a malicious foreign actor's infrastructure to disrupt or exploit. FBI collection facilitates the coordinative function of the Office of the National Cyber Director as they ensure coherence across federal cybersecurity. FBI's collection also helps inform the National Security Council, so they can focus all the instruments of power the government might bring to bear against possible cyber threat actors. We also work with the State Department, including the new Bureau of Cyberspace and Digital Policy (CDP) and the Bureau of International Narcotics and Law Enforcement (INL), to build partner-country political and law enforcement support and partnerships for international investigations to counter cyber enabled criminal activity impacting the United States. We value working with these federal partners toward the same goal, and when we use all these agencies' complementary authorities together, we create a whole that's greater than the sum of the agency parts.

This emphasis on sharing information and enabling our partners is part of the FBI's continued move away from pursuing only indictments and arrests and towards a playbook where we work with government and industry partners around the world to execute joint, sequenced operations. That is how we impose the greatest possible costs on our adversaries and best protect our country. The willingness of the Department of Justice, including FBI, to publicly attribute and expose damaging cyber intrusions by Russia, China, Iran, and North Korea has undermined those governments' denials and created a platform for U.S. allies to condemn destabilizing cyber activity and impose costs of their own. Our decisions on how best to disrupt a cyber threat are guided by an assessment of which actions will most strengthen cybersecurity, regardless of who takes the shot or gets the credit.

In coordination with our partners, the FBI has successfully disrupted numerous nation-state campaigns and cybercriminal enterprises. Continued success will require repeated operations with our U.S. counterparts and foreign allies, and we must eliminate the sense of impunity many of these actors currently feel. Yes, the cyber threat is daunting, but when we combine the right people, the right tools, and the right authorities, we best protect our critical infrastructure.

Threat Overview

The USIC has assessed that China is attempting to pre-position on U.S. critical infrastructure—setting up back doors to cripple vital assets and systems in the event China invades Taiwan and therefore, limiting our ability to assist Taiwan.

We have observed the CCP target multiple critical infrastructure entities, attacks which could potentially jeopardize the physical safety of Americans. To give just one example, the FBI has identified PRC-backed hackers who gained access to the computer networks of a major U.S. transportation hub. In this case, the FBI quickly alerted the network operators to the particular portion of their network that had been compromised and assisted with fixing the vulnerabilities.

We are no longer in the Advanced Persistent Threat 1, or "APT1", days of the PRC's

cyber program. In 2013, Mandiant, an American cybersecurity firm, publicly attributed APT1 activities to the People's Liberation Army (PLA). Their pivotal report disclosed the bespoke malware commonly deployed by the PLA, which could easily be discovered by anti-virus/anti-malware programs. Today, we see PRC state-sponsored cyber actors, such as Volt Typhoon, "living off the land." This technique uses legitimate network administration tools to perform malicious objectives, allows them to evade detection by blending in with normal operating system and network activities, avoid endpoint detection and response (EDR) products that would alert on the introduction of third-party applications to the host, and limit the amount of activity that is captured in default logging configurations.

The FBI's Efforts to Counter PRC Cyber Actors

Together with our partners, we have released multiple Joint Cybersecurity Advisories on PRC State-Sponsored Cyber Actors. These advisories provide details on PRC tactics, techniques, and procedures (TTPs) that can be used by network defenders to both find and prevent malicious cyber actors from accessing their networks. Increasingly, the scale and tradecraft of PRC cyber operations must be met with combined resources of the government and partners in the cybersecurity industry and others with broad insight into malicious activity on the Internet.

Additionally, we work with our partners such as CISA and other sector risk management agencies to notify victims of cyber intrusions. These efforts include providing information to victim organizations to help respond to the intrusion, working with their IT team to collect evidence, coordinating with attorneys, and conducing analysis to inform future responses. This evidence informs the public advisories that we release and other efforts to combat the threat.

Section 702 of the FISA Amendments Act of 2008

Section 702 of the FISA Amendments Act of 2008 is paramount to our ability to combat PRC state-sponsored cyber actors. In the last half of 2023, 97 percent of the FBI's raw technical reporting on malicious cyber actors, and 93 percent of our reporting on emerging technologies, such as artificial intelligence, came from Section 702 collections. On average over the past 10 years, malicious foreign cyber actors have accounted for more than half of our Section 702 targets. The FBI's Cyber Division uses this intelligence to conduct strategic disruption activities against those malicious cyber actors. Thanks to the foreign intelligence we receive from Section 702, the FBI's Cyber Division is able to work with the FBI's USIC partners and warn victims when cyber criminals are prepositioning for attacks—so before the attack begins—and help the potential victims close identified backdoors and remove the opportunity for malicious actors to exploit their systems.

Section 702 has been pivotal for the FBI to detect and thwart PRC-backed cyber threat actors attempting to access U.S. critical infrastructure. The FBI has seen China-based cyber threat actors access a variety of critical infrastructure in the United States. Section 702 allows us to detect these cyber threat actors by monitoring them as they traverse the internet and determining when they access networks within the United States. Using queries for the

identifiers of potential victims—namely American businesses and organizations—we can identify whether the cyber threat actors are merely researching a victim for possible future attacks or if they have already successfully compromised systems. This critical tool directly protects Americans and American businesses.

Investing in a More Capable Cyber Response

The PRC represents the defining threat of this era. There is no country that presents a broader, more comprehensive threat to our ideas, our innovation, our economic security, and, ultimately, our national security. Now is not the time to reduce the FBI's resources or capabilities. The PRC uses every means at its disposal to impact our economic security – blending cyber capabilities, human intelligence, corporate transactions, and other means of attacking and exploiting U.S. companies to advance its own economic growth, national power, and military capability.

The FBI faces significant resource challenges to address the scale and sophistication of national security and criminal cyber threats targeting the United States. Although there are many resource gaps, the FBI is appreciative of the President's *Fiscal Year 2024 Budget Request*, which would expand our ability to pursue cyber threats through investments that support efforts to build investigative capabilities at FBI field offices nationwide. The Fiscal Year 2024 Budget Request includes an additional $63 million for more agents, enhanced response capabilities, and strengthened intelligence collection and analysis capabilities. These investments reflect the *National Cybersecurity Strategy*'s emphasis on a whole-of-Nation approach to addressing the ongoing cyber threat.

Reductions to the FBI's budget would adversely impact the FBI's computer intrusion program, undermining its ability to continue to aggressively and successfully thwart countless PRC threats to our economic and national security before they can do significant harm. Even if the FBI focused all of its cyber agents and intelligence analysts on the PRC threat, PRC-backed cyber threat actors would still outnumber FBI Cyber personnel at least 50 to 1, and they are attempting multiple cyber operations each day in domestic Internet space, where only the FBI has the authorities to monitor and disrupt.

Conclusion

The strength of any organization is its people, and that is especially true in the FBI. 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 those threats, and, every day, the men and women of the FBI continue to meet and exceed those expectations. I want to thank them for their dedicated service.

Chairman Gallagher, Ranking Member Krishnamoorthi, and Members of the Committee, thank you for the opportunity to testify today. I am happy to answer any questions you might have and to work together with you in the nation's fight against malicious cyber activity so the

FBI can help achieve our collective cyber mission—to give the American people safety, security, and confidence in our digitally connected world.