Bryan A. Vorndran
Assistant Director, Cyber Division
Federal Bureau of Investigation

Statement Before the House Judiciary Committee
Washington, D.C.
March 29, 2022

Oversight of the FBI Cyber Division

Statement for the Record

Chairman Nadler, Ranking Member Jordan, and members of the committee, thank you for the invitation today to provide remarks on the FBI Cyber Division and our role in identifying, disrupting, and imposing costs on our cyber adversaries.

Cybersecurity is national security, and that has never been more apparent than it is today.

Currently, the FBI's work to identify and disrupt cyber threats emanating from Russia against Ukraine, our allies, and our own U.S. networks is an excellent example of how the FBI uses our unique authorities, capabilities, and partnerships as part of the global fight against malicious cyber activity. When it comes to disrupting and countering Russian cyber activity in particular, our work is building on the FBI's decades of expertise countering foreign intelligence and cyber threats in the United States.

On Russian cyber threats alone, since the start of the year, the FBI has:

- Issued hundreds of intelligence reports that provided the U.S. Intelligence Community and our international partners with key intelligence.
- Provided threat warnings to thousands of partners across the United States, including major banks, Sector Risk Management Agencies, state secretaries of state, law enforcement, and other private industry
- Shared information directly with Ukrainian services through our personnel in Kyiv, including an Assistant Legal Attaché dedicated to cyber

The FBI's strong relationships in Ukraine have been a resource for the entire U.S. government, built through years of collaboration with our counterparts there, including during the 2015 Russian Black Energy attacks on the Ukrainian power grid and the 2017 NotPetya attack that first targeted Ukraine before spreading globally to become the costliest cyberattack in history.

It is these types of partnerships that allowed the White House to publicly attribute the recent cyberattacks in Ukraine on the eve of Russia's further invasion so quickly. Just days after Ukrainian websites first suffered distributed denial of service (DDoS) attacks, the White House attributed those attacks to Russia's GRU. This is what the FBI can uniquely contribute to national and international cybersecurity by leveraging our authorities, resources, and national and international partnerships.

Cyber risk is also business risk—there is no shortage of recent examples of cyberattacks' wide-ranging economic effects. That is why we are here today. While much attention has been paid to ransomware in the past year—and deservedly so—the FBI's Internet Crime Complaint Center (IC3) just issued its annual report showing that, yet again, Business E-mail Compromise (BEC) schemes cost U.S. businesses more than $2 billion last year—losses these businesses absorbed into the cost of doing business but should not have had to do.

Cyber intrusions make the headlines only occasionally, but the FBI has over 1,000 cyber personnel distributed throughout the United States and responding 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 Intelligence Community, 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 victims, and key technology service providers—to identify and disrupt cyber adversaries before they compromise U.S. networks, and to hold them accountable when they do.

The information that the FBI uniquely collects helps the Cybersecurity and Infrastructure Security Agency (CISA) to identify other networks vulnerable to the same adversary technique, helps Sector Risk Management Agencies assess and mitigate cyber threats to critical infrastructure, provides 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, facilitates the coordinative function of the Office of the National Cyber Director in ensuring coherence across federal cybersecurity, and helps the National Security Council know where to focus all the instruments of power the government might bring to bear against those responsible. We are lucky to be 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 disrupting cyber adversaries by sharing information and enabling our partners is part of the FBI's continued move away from pursuing only indictments and arrests, toward a playbook where we work with government and industry partners around the world to execute joint, sequenced operations that impose the greatest possible costs on our adversaries. As this committee knows, there is a right time for judicial outcomes, and the willingness of the Department of Justice, including the 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. But our decisions on how best to disrupt a cyber threat are guided not by statistics, but 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, but the lasting impact will require repeated operations with our U.S. counterparts and foreign allies, as well as removing 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, our adversaries are no match for what we can accomplish together. I am here today to tell you how the FBI is doing that; what we do before, during, and after a cyber incident; and why the American people will want to call us if they become victims.

The FBI Cyber Value Proposition

Although cyber threats are global, victims in our communities need and deserve a rapid, local response. That is where the FBI comes in. With the support of the American people, the FBI has invested enormously in its decentralized workforce. We have more than 800 cyber- trained agents spread across 56 field offices and more than 350 sub-offices, with each office having significant threat response, counterintelligence, domestic intelligence, and computer intrusion expertise and responsibilities. We can put a cyber-trained FBI agent on nearly any doorstep in this country within one hour, and we can accomplish the same in more than 70 countries in one day through our network of legal attachés and cyber assistant legal attachés. No other organization in the world has this reach, our unique tools and resources, or the sense for what victims need. When we show up, we bring all this with us. Kaseya CEO Fred Voccola recently remarked, "When we were hit, our playbook had as a standard process (luckily) to call the FBI the second something seemed suspicious. And we did just that. To this day, it was the single best decision that I, as the CEO, and we as a company, made."

In addition to these resources dispersed around the country, we have dedicated teams in our Headquarters that provide specialized support to victims of cyber intrusions. Our Cyber Action Team (CAT) is a rapid response technical investigative team that deploys nationally and internationally to provide technical assistance to assist in the most complex intrusions and cyber incidents. Our Recovery Asset Team (RAT) acts quickly to help victims recover funds that otherwise would be lost to fraud. In fiscal year 2021, RAT used the Financial Fraud Kill Chain (FFKC) 1,726 times and was able to successfully freeze more than $328 million—a 74% success rate—that could then be returned to individual and business victims of cyber fraud.

The FBI's cyber capabilities are one of a kind, but our roles and responsibilities are designed to complement those of our federal partners. Whether our agencies specialize in offense, defense, or a combination of both, we are all contributing to improved resilience and cybersecurity, and all of our efforts need to work seamlessly to protect our networks. The FBI plays a key role in this, but we cannot do it alone, and that acknowledgment is a major part of the FBI's cyber strategy.