Department of Justice

STATEMENT OF

BRYAN A. VORNDRAN

ASSISTANT DIRECTOR

CYBER DIVISION

FEDERAL BUREAU OF INVESTIGATION
U.S DEPARTMENT OF JUSTICE

BEFORE THE

COMMITTEE ON JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES

FOR HEARING ENTITLED

"OVERSIGHT OF THE FBI CYBER DIVISION"

PRESENTED

MARCH 29, 2022

STATEMENT OF
BRYAN A. VORNDRAN
ASSISTANT DIRECTOR
CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION
U.S. DEPARTMENT OF JUSTICE

AT A HEARING ENTITLED
"OVERSIGHT OF THE FBI CYBER DIVISION"

BEFORE THE
COMMITTEE ON JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES

MARCH 29, 2022

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 Email 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 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."[1]

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

[1] Kaseya CEO Fred Voccola, "The FBI Was Our #1 Partner During the Worst Time of Our Company's History, and They Should Be Yours Too," https://www.kaseya.com/blog/2022/03/09/the-fbi-was-our-number-one-partner/, March 9, 2022.

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.

The FBI Cyber Strategy

In September 2020, Director Wray announced the FBI's current cyber strategy, which focuses on imposing risk and consequences on cyber adversaries through unique authorities,[2] world-class capabilities, and enduring partnerships, building on a century of innovation. Through this strategy, we work to raise the costs for malicious actors and their enablers who conduct cyber intrusions, steal our financial and intellectual property, and hold our critical infrastructure hostage for ransom. Over the past 18 months, this strategy and its principles have enabled us to make significant progress in advancing our cyber program and making it harder and more painful for malicious hackers to achieve their objectives. This is the same strategy we are using today to counter cyber threats originating from Russia.

One of the most notable examples of recent success is our work to disrupt Sodinokibi/REvil ransomware, which cyber actors used to compromise global meat processing company JBS and software company Kaseya in 2021. Over the course of several months last year, we strategically sequenced actions with foreign partners on three continents and the State, Justice, and Treasury Departments to release decryption keys to victims, seize virtual currency proceeds in excess of $7 million, and arrest three affiliates of the group. One of these affiliates, Yaroslav Vasinskyi, was extradited to the United States and made his initial court appearance in the Northern District of Texas earlier this month. It takes deep, trust-based relationships to coordinate these actions to ensure maximum impact on the cybercriminals we were targeting.

As mentioned, our strategy builds on a century of FBI innovation in addition to our partnerships. Last year, Chinese state actors exploited a vulnerability in Microsoft Exchange Server software to compromise thousands of U.S. computers and install web shells—essentially,

[2] The FBI's authorities allow us to conduct investigations, collect intelligence, and work closely with targets of malicious cyber activity to find who is responsible, stop them from striking again, and hold them accountable. These authorities include: Presidential Policy Directive (PPD)-41, which names the FBI the lead federal agency for threat response in the event of a significant cyber incident; Executive Order 12333, which names the FBI the lead agency for exposing, preventing, and investigating intelligence activities on U.S. soil; and 18 U.S.C. § 1030, which designates the FBI to lead cyber investigations involving espionage and foreign counterintelligence. Because of these authorities and the FBI's organizational structure and history, the FBI is the best positioned investigative agency to conduct complex, long-term cyber investigations into both cybercriminals and nation-state actors.

a back door allowing them to come and go into those networks as they pleased. China tried to prop open these doors, and we slammed them shut. Thanks to information shared with us by a member of private industry, the FBI executed an innovative court-authorized operation to copy and remove those backdoors from hundreds of vulnerable computers across the country. Maybe most importantly to the private sector, we only did this after publicly releasing information on the compromises and working with Microsoft to directly contact server owners to allow them time to fix the problem on their own. And, consistent with our respect for privacy and civil liberties, we removed the web shells surgically without exposing the contents of victim computers to the FBI.

Our strategy also integrates our foreign partners so we can take the fight to our adversaries overseas, since we know our most significant threats come from foreign actors using global infrastructure to compromise U.S. networks. By working with friendly foreign law enforcement agencies and intelligence partners, we make it harder for these actors to conceal their activities and whereabouts. Unfortunately, not every nation helps us in this fight, and if an adversary is in a country that refuses to hold them accountable, an arrest is rarely a viable option. But our allies outnumber our foes, and in just the past year, our work with foreign partners—supported by our Legal Attachés overseas—has led to impactful consequences against cybercriminals and sent a strong message that the reach of the U.S. government extends far beyond its borders.

For example, in January 2021, the Department of Justice, including the FBI, partnered with the Netherlands, Germany, the United Kingdom, France, Lithuania, Canada, and Ukraine—with international activity coordinated by Europol and Eurojust—to disrupt the use of highly destructive malware known as Emotet which criminals used, among other things, to spread ransomware. This was one of the longest-standing professional cybercrime tools and had enabled criminals to cause hundreds of millions of dollars in damage to government, educational, and corporate networks. In this case, we used sophisticated techniques and our unique legal authorities, but it could never have happened without our international partners.

That same month, we worked with international partners in Canada and Bulgaria to disrupt NetWalker, a ransomware variant that affected numerous victims, including companies, municipalities, hospitals, law enforcement, emergency services, school districts, colleges, and universities. In this case, we obtained federal charges on a Canadian subject, Sebastien Vachon-Desjardins, who was extradited to the United States and made his first court appearance in the Middle District of Florida earlier this month. In addition, our Canadian partners seized over $28 million[3] in virtual currency from Vachon-Desjardins traceable to his criminal acts.

As you can see, cyber is the ultimate team sport. Effective protection and response efforts require not just FBI action, but an all-hands-on-deck approach, to include assistance from our state, local, federal, foreign, and private sector partners, and even the public.

[3] Value is approximate as of March 10, 2022.

As you may have noticed, one term we use constantly when describing the heart of our work is "victims." Victims lie at the center of our efforts, and our cyber strategy specifically includes a pledge to them. In fact, we are often able to notify and help vulnerable targets before the worst happens, like last year, when we were able to notify a children's hospital targeted by Iranian government-sponsored hackers before it was attacked. At the FBI, we aim to inform, support, and assist victims in navigating the aftermath of crime with dignity and resilience. We want to empower all victims of cyber intrusions, just as we do for victims of other federal crimes. In some instances, we have done this by sharing a ransomware decryption key to help victims recover without paying a ransom. While the FBI is not a remediation service, the work we do to investigate and respond to cybercrime enables us to collect information, which we share to prevent future attacks and use to assist victims if they have already been hit. When the FBI responds to a cyber incident, the Bureau is not just there to collect evidence of a crime; we're also there to help those who have been hurt. Your needs are our needs. But we can't help if we don't know what happened.

In just 18 months, our strategy has enabled us to land some major blows against our cyber adversaries, and in 2021 alone, through work with our partners, the consequences we imposed on cyber actors included 240 arrests, 175 convictions, 290 indictments, 18 dismantlements, and 453 disruptions. 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. However, the cyber threat is not going away, and there is always more work to be done, so we must carry this strategy and its momentum forward through 2022 and beyond.

Top Cyber Threats: 2022 and Beyond

As we look ahead at cyber threats, it worries us that nation-states and cyber criminals are showing a complete disregard for the safety of our civilian population. In the past year, we have seen cyber actors compromise networks without care for what they are connected to. Hospitals, pipelines, 9-1-1 call centers, and service providers to critical infrastructure—nothing is off limits.

Nation-State Threats

The most significant nation-state threats we face are those from China, Russia, Iran, and North Korea. For years, our adversaries and strategic competitors have engaged in cyber espionage to collect intelligence and intellectual property to advance their geopolitical and economic goals. Now, these nations have calculated that the cyber arena offers them the best return on their investment, so they're coming at us using every element of their national power, including through regulations, the recruitment of cybercriminal actors, their militaries, and coercion of the private sector, which raises the prospect of more destructive and disruptive cyber activities. As these adversaries become more sophisticated and stealthier, we are most concerned

about our ability to detect and warn about specific cyber operations against U.S. organizations. Maybe most worrisome 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 where nation-state activity ends, and cybercriminal activity begins. Some cybercriminals contract for or sell services to nation-states; some nation-state actors moonlight as financially motivated cybercriminals to make money on the side; and nation-states are increasingly using tools typically used by criminal actors, like ransomware. It is useful to think of this more as a continuum.

Ransomware and Other Cybercrime

If there is one thing the FBI understands, it is taking down criminal organizations, and when it comes to ransomware and other cybercrime, we are working with an unprecedented number of government and private sector organizations to do just that.

There is not a day that goes by without multiple FBI field offices responding to ransomware attacks. The ransomware threat is not new, and it has been one of the FBI's top cybercriminal investigative priorities for some time, but we have seen ransomware attack reporting increase significantly in the past two years, and the impact of these attacks has grown to dangerous proportions, threatening our economic and national security. [4] The number of ransomware variants has also grown; today, we are investigating more than 100, many of which have been used in multiple ransomware campaigns.

Ransomware actors have evolved, but their motive remains the same: maximizing profit by crippling victims. Cybercriminals recognize profit can be maximized by targeting organizations where down time cannot be tolerated—specifically, infrastructure critical to public safety. In 2021 alone, the FBI, CISA, and NSA observed incidents involving ransomware against 14 of the 16 U.S. critical infrastructure sectors.

Ransomware is increasingly targeted and lucrative, and beyond the threat to critical infrastructure, it has become one of the most costly and destructive threats to businesses and governments. Ransomware can paralyze organizations, and the cost to rebuild a compromised network can be catastrophic for small and medium-sized businesses and municipalities. "Ransomware-as-a-service" (when a developer sells or leases ransomware tools to criminal customers) has decreased the barrier to entry and technological savviness needed to carry out and benefit from these compromises and increased the number of criminals conducting ransomware campaigns.

[4] The statistics paint a stark picture: From 2019 to 2021, the number of ransomware complaints reported to the FBI's Internet Crime Complaint Center (IC3) increased by 82%, with a 449% rise in ransom payments over the same time period. Unfortunately, what is reported is only a fraction of the incidents out there, which makes trends difficult to track with certainty.

In conjunction with the Department of Justice's Ransomware and Digital Extortion Task Force, our strategy for countering ransomware and other complex cybercriminal schemes is focused on pursuing and disrupting: 1) the actors, 2) their infrastructure, and 3) their money—all while providing help to victims and actionable intelligence to warn potential future victims. Each of these factors is crucial, but we have the most durable impact when we disrupt all three together *and* when we combine the capabilities and authorities of multiple agencies and private industry partners. We must target the entire criminal ecosystem—including malware developers, money launderers, and shady infrastructure providers—to prevent bad actors from simply reconstituting under a different name, and we need to do it jointly with our partners across the U.S. Government, the Intelligence Community, and the globe. But there is no substitute for quick, voluntary action and information sharing by U.S. providers and victim companies.

Although the FBI discourages ransomware victims from paying ransom, we still strongly encourage victims who ultimately pay a ransom to report the incident to the FBI. Knowing about the incident gives us valuable information about how and where criminals are operating and knowing payment details gives us a hot trail to follow the money. We put a lot of effort into making sure that victims who do pay a ransom don't feel re-victimized as they work with us to deal with the incident's fallout. Our goal is to identify, pursue, and impose consequences on criminal actors, not their victims.

Election Interference

We are committed to continuing and expanding our work with election officials and private sector partners to counter cyber threats against U.S. elections and election officials, as well as continuing to impose risk and consequences on cyber actors who seek to interfere in our elections or undermine our democratic processes. We do this through criminal process, sanctions, and public attribution of cyber operations.

In November 2021, the Department of Justice, including the FBI, the Department of State, and the Department of the Treasury announced a series of coordinated U.S. Government actions against Iranian cyber actors who participated in influence operations targeting the 2020 U.S. presidential election. First, the Department of Justice unsealed indictments charging two Iranian nationals for computer intrusion, voter intimidation, and interstate threat offenses. Both are experienced Iran-based hackers who worked as contractors for an Iranian company known to have provided services to the Iranian government. In conjunction with the unsealing, our Executive Branch partners sanctioned the two individuals who were indicted as well as other Iranian cyber actors, offered monetary incentives through the Rewards for Justice program, and disseminated related information on the threat.

As we have been for years, we remain committed to investigating, warning, notifying, and sharing information about suspicious cyber activity to help election officials and administrators protect their networks. We brief election officials and network defenders on supply chain, data theft, ransomware, and influence threats, but our overarching message is that

cyber hygiene and defense are critical, no matter which actor or method worries us the most. We know our adversaries will continue to target election-related networks and systems again and again using the same unpatched vulnerabilities, by guessing simple passwords, and by spear phishing. That is why it is critical to maintain close collaboration with election officials, political organizations, candidates, social media and tech companies, and technical defenders.

Beyond targeted engagements with national organizations and one-on-one outreach with smaller groups, we continue to push out information in as close to real time as we can. Whenever possible, we will do the work upfront to sanitize information so we may get actionable threat intelligence out to the network defenders. Meanwhile, we will continue to engage with state and local entities—as appropriate and authorized under the law—to build relationships, communication channels, and information sharing processes as we prepare for another election cycle. We do all this in lockstep with our Counterintelligence Division through the FBI's Foreign Influence Task Force (FITF).

Deepfakes and Synthetic Content

We are seeing advances in artificial intelligence and machine learning that are improving the speed, believability, scale, and automation of the creation and dissemination of deepfakes and other synthetic content to produce high-quality videos, pictures, audio, and text of events which never happened. Although deepfake videos are currently difficult to create and require resources and sophistication, they are becoming increasingly more accessible. Cybercriminals can create highly personalized content for targeted social engineering, spear phishing, business email compromises, other fraud schemes, and to victimize vulnerable individuals, and nation-states could use these techniques for malign foreign influence and to spread disinformation and misinformation.

Trust in evidentiary information from photos, body cam footage, surveillance camera footage, and other forms of content could be challenged as synthetic content and deepfake technologies improve in accessibility and quality enough to similarly depict evidentiary content. Right now, it is easier to detect and determine if content has been manipulated or synthetically generated, but as synthetic content improves, it may become more difficult to convince others legitimate data is authentic.

The FBI is working with our IC counterparts and private industry to understand technological developments and evaluate and develop detection, authentication, and mitigation tools and techniques to counter the misuse of deepfakes. We also provide awareness to the public about these types of threats. We cannot open an investigation purely because a deepfake exists, as fake speech may be protected by the First Amendment, but we can investigate this content and its creators when there is a clear nexus to a federal crime or a foreign actor.

Virtual Currency

Over the next five years, innovations in blockchain technology, decentralized finance, and central bank digital currencies will very likely provide financial conduits for illicit actors to exploit. In some cases, these conduits may limit U.S. law enforcement's ability to identify those actors, track, funds, compel the production of financial records, or to use existing laws to prosecute crimes. However, we are evolving with the actors, and we have had recent success in this arena.

Cryptocurrency is sometimes attractive to cybercriminals due to its perceived relative anonymity, ease of transfer, and use on the dark web, so it is no surprise this is how ransomware payments—sometimes in the millions of dollars—are demanded and laundered. But, in addition to the Sodinokibi/REvil and NetWalker cryptocurrency seizures I mentioned, we were also able to claw back about $2.3 million of the ransom paid in last year's Colonial Pipeline ransomware case, which we could do because the victim and our federal partners worked quickly and closely with us.

Additionally, we are also evolving organizationally to adapt to the threat. The FBI recently brought together expertise from cyber, criminal, and other programs to develop the Virtual Assets Unit (VAU), a nerve center for the FBI's virtual currency efforts. In VAU, virtual currency experts and cross-divisional resources are embedded in a task force setting to seamlessly integrate intelligence and operations across the FBI. Since becoming operational last month, VAU has enabled the FBI to continue to aggressively track the movement of illicit funds, attribute criminal activity to specific actors, and disrupt illegal activity.

How Victims and Potential Victims Can Help Themselves and Others

We have the strategy to act against our cyber adversaries, we can provide significant value, and we have shown we can be successful. But none of that matters, and we will not continue our success if we don't know about suspicious activity or that a compromise has occurred. We look forward to working with our partners at CISA as the Cyber Incident Reporting for Critical Infrastructure Act of 2022 is implemented to ensure that all new incident reports are accessible as soon as possible and used for purposes authorized under the Act, i.e., to advance our nation's cybersecurity and support cyber investigations that enable the U.S. Government to attribute malicious cyber activity, disrupt it, and bring cybercriminals to justice.

We know victims of cyber intrusions, particularly large enterprises, risk negative publicity if they disclose being impacted by cybercrime, so many incidents are often addressed by the victim directly and are never reported to the public or law enforcement. But this is my call to action—we need the private sector to do its part. We need to be warned **quickly** when companies see malicious cyber activity. We also need companies to work with us when we warn them that they are being targeted. The recent examples of significant cyber incidents (SolarWinds, Microsoft Exchange, Colonial Pipeline, JBS, and Kaseya) only emphasize what the

FBI has been saying for a long time: The government cannot protect against cyber threats on its own. We need a whole-of-society approach that matches the scope of the danger. There is no other option for defending a country where nearly all our critical infrastructure, personal data, intellectual property, and network infrastructure sits in private hands.

So, what specific steps can companies take to follow our guidance, protect themselves and our nation, and help themselves if ransomware strikes? First, the public, cybersecurity professionals and system administrators, and business leaders can use threat information shared by the FBI, CISA, NSA, and the rest of the federal government to strengthen their network defenses and guard against ransomware and other malicious cyber activity. Our reports, which are coordinated with our federal partners, are shared directly with critical infrastructure owners and operators, and when possible are posted to our IC3 website to warn the public about the trends we are seeing and the specific threats out there. In addition to these threat advisories, the new federal site **www.StopRansomware.gov** has resources on how people and businesses can protect themselves. Some of the general cybersecurity practices we encourage include creating and securing offline backups of critical data, installing patches as soon as they become available, updating anti-virus software, connecting only to secure networks, employing multi-factor authentication, and ensuring the validity of all emails and the links they contain before clicking them.

Second, if you are an organization, create an incident response plan. If you are compromised, you need to know what to do. All your leaders and security professionals need to be on the same page, and you must be able to make decisions quickly. Having worked with victims who had incident response plans versus those who did not, the difference is stark. Victims with incident response plans are often able to respond faster and more efficiently and can significantly limit the damage caused by a ransomware incident.

Third, organizations should work to build relationships with their local FBI field offices. Whether you are a small organization or a large corporation, our local offices welcome making connections before anything has gone wrong. If you see us speaking at an event in your area, show up, and talk to us after. We would be thrilled to meet your CEO, chief information security officer (CISO), general counsel, or anyone who has a role in keeping your networks secure and responding to cyber incidents. But it cannot stop there. Continue to share information with us after that meeting, and we will do the same back to you.

Fourth, **if you are compromised, or if you think you may have been, report it to us as quickly as you can**. You can report these incidents by contacting your local FBI field office—hopefully to the FBI agent you already know. We will take it from there and make sure the wheels of the entire federal government incident response team are set into motion so you can focus on remediation. **Reporting quickly is the best chance for you to make an impact and the best chance to protect others and our nation.**

If an incident occurs, it may not be too late, but time is of the essence. The difference between seeking help on day one and day five is real—it can be the difference between a company reconstituting its network or declaring bankruptcy. We will always use our full range of national security authorities and criminal legal processes to investigate cyber incidents, but many of those techniques require probable cause and prior court authorization, so there is no substitute for quick, voluntary action by private owners of U.S. networks and infrastructure in helping us act rapidly against a threat. Swift action from the private sector is an enormous public service, and we truly appreciate private sector cooperation whenever we can get it. In the Colonial Pipeline and Kaseya incidents, for example, swift reporting and response contained the impact of what could have been significantly worse events.

Swift reporting also helps us warn others who are vulnerable to similar intrusions. Recently, when assisting a major critical infrastructure victim during an ongoing incident, we identified a zero-day vulnerability the attackers were exploiting, used our investigative tools to search for other victims affected by this vulnerability, and worked with CISA to provide cybersecurity assistance to these entities while a patch for the vulnerability was being developed.

In another incident reported to the FBI, a victim reported a malicious sever that connected to its network. We used our law enforcement and intelligence authorities to quickly monitor the malicious actor's virtual infrastructure, dispatched agents across the country to warn targeted entities who the actor planned to compromise next, provided these entities with security advice, and intercepted and corrupted some stolen information before it could be exfiltrated.

The Resource Demands of Investigating Malicious Cyber Activity

Unfortunately, the number and scale of major cyber incidents—some of which can involve tens of thousands of victims—is growing and is challenging our collective ability to respond. The FBI is increasingly faced with hard choices that carry risk, including the redirection of personnel away from long-term investigations so they can surge to address immediate needs. In our SolarWinds investigation alone, a single FBI field office collected more than 170 terabytes of data—about 17 times the content of the entire Library of Congress. Because of our role in attributing cyber incidents so that those responsible can be held accountable, the FBI's response to an incident like SolarWinds is measured in months or years, not weeks. When others have moved on to the next incident, FBI agents, analysts, computer scientists, and others across multiple headquarters divisions and field offices pursue new leads to identify those responsible and provide policymakers options to hold them accountable.

Recent ransomware and nation state campaigns have shown us the investments in time, money, and talent cyber adversaries are willing to make to compromise our networks. The FBI must have the ability to not only keep pace with these criminals but also ensure we invest in critical areas to stay ahead of the threat. Congress can help us by providing the resources requested in the President's 2023 Budget Request to ensure the FBI and our partners are resourced to play our respective parts in the cyber ecosystem as we defend the nation together.

At the same time, receiving funding through the budget process can only get us so far. We need to be able to attract talent to put that funding to use, and an additional challenge for the Department of Justice—to include the FBI—is that we do not possess the same human capital flexibilities to recruit, retain, and incentivize our cyber workforce as the Department of Defense and Department of Homeland Security. Further, we all know the private sector can offer salaries the government cannot, and it is hard enough to compete on that talent management front. While at the FBI, we have been working hard on ways to better attract, train, and retain talented tech minds with existing personnel authorities, and we do sell our mission and the value of public service to the greatest extent possible, we have seen time and again our inability to pay those minds market value be a dealbreaker.

Conclusion

Even more than the other criminal violations we investigate, the FBI depends on our partners—public and private, foreign, and domestic—to help us keep Americans safe from the many threats posed by malicious cyber actors. As part of our strategy, we have been putting a lot of energy and resources into cultivating these partnerships, and I truly believe our partners are seeing the benefits of having FBI Cyber on their team.

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 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.