Department of Justice

STATEMENT OF

BRYAN A. VORNDRAN
ASSISTANT DIRECTOR
CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION
UNITED STATES DEPARTMENT OF JUSTICE

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED

"AMERICA UNDER CYBER SIEGE:
PREVENTING AND RESPONDING TO RANSOMWARE ATTACKS"

PRESENTED

JULY 27, 2021

STATEMENT OF
BRYAN A. VORNDRAN
ASSISTANT DIRECTOR
CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION
UNITED STATES DEPARTMENT OF JUSTICE

BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED

"AMERICA UNDER CYBER SIEGE:
PREVENTING AND RESPONDING TO RANSOMWARE ATTACKS"

PRESENTED
JULY 27, 2021

Chairman Durbin, Ranking Member Grassley, and Members of the Committee, thank you for the invitation to provide remarks on the FBI's role in our nation's fight against ransomware.

Ransomware is a growing threat to the health and safety of the American people and our national and economic security, with the Kaseya incident being the most recent example of ransomware's wide-ranging effects. I am honored to lead the men and women of the FBI's cyber program, where we are using our unique authorities to impose risk and consequences on the malicious cyber actors who are committing these crimes. But we cannot go at it alone, and as you will hear today, our strategy involves not only our partners in the federal government but also those in the private sector and abroad.

The individuals who conduct cyber intrusions and ransomware campaigns, and the officials who direct or harbor them, believe they can compromise U.S. networks, steal our financial and intellectual property, and hold our critical infrastructure hostage for ransom, all without incurring risk themselves.

The FBI sits at the convergence of U.S. government efforts to change this risk calculus. As a member of both the law enforcement and intelligence communities, with domestic and international reach, 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 adversaries **before** they compromise U.S. networks, and hold them accountable when they do.

Key to the FBI's strategy is using the information and insight we develop through our investigations to support our full range of public and private sector partners. There are many countries, companies, and agencies who play roles in defending networks, sanctioning destabilizing behavior, collecting cyber threat intelligence, and conducting cyber effects

operations. We seek to work with all of them, in the belief that our collective actions to combat cyber threats are most impactful when they are planned jointly and sequenced for maximum impact.

In coordination with our partners, the FBI has successfully disrupted numerous cybercriminal enterprises, including those deploying ransomware, but lasting impact will require joint, sequenced operations with our U.S. counterparts and foreign allies as well as a removal of sense of impunity many of these actors currently feel.

What is Ransomware?

At its most basic, ransomware is a computer program created by malicious actors to 1) infect a computer or server, 2) encrypt its contents so they cannot be accessed or used, and 3) allow the malicious actors to demand that a ransom be paid in exchange for the decryption key. Victim organizations without effective backups are not able to operate until their data is restored. Ransomware can paralyze organizations, and the cost to rebuild an encrypted network can be catastrophic for small- and medium-sized businesses and municipalities.

The ransomware threat is not new, and it has been one of the FBI's top priorities for cybercriminal investigations for some time. In 2018, for example, we eliminated the threat from a highly impactful ransomware variant called SamSam that infected victims in nearly every U.S. state, including the city of Atlanta, the Port of San Diego, and multiple major healthcare companies. Our investigation led to a November 2018 indictment of the responsible Iranian cybercriminals and sanctions against two digital currency exchanges that enabled their operations; this ransomware variant has not been seen since.

In a trend not unique to cybercrime, as we expand our capability to disrupt ransomware actors, criminals have adapted to increase the scale, impact, and prevalence of ransomware attacks. The increasingly sophisticated and targeted nature of ransomware campaigns has significantly increased their impacts on U.S. businesses, and ransom demands are growing larger. Simultaneously, "ransomware-as-a-service" (RaaS), in which a developer sells or leases the ransomware tools to their criminal customers, has decreased the barrier to entry and technological savvy needed to carry out and benefit from these compromises and increased the number of criminals conducting ransomware campaigns. As this has happened, the number of ransomware variants has grown; today, we have investigations into more than 100 variants, many of which have been used in multiple ransomware campaigns. Recently, we have seen "double extortion" ransomware – where actors encrypt, steal, and threaten to leak or sell victims' data – emerge as a leading tactic for cybercriminals, raising the stakes for victims, which in turn has increased the likelihood of ransom payments being made. While cybercriminals remain opportunistic, they have also become more targeted in their campaigns, purposely aiming their malware at those institutions which can least afford downtime – specifically infrastructure critical to public safety, including hospitals and emergency services.

These ransom payments are typically requested in the form of a virtual currency, like Bitcoin. Virtual currency is not governed by a central authority, and regulation of the industry is still evolving globally, which can make it difficult to find out who is behind a transaction.

Cryptocurrency can be moved anywhere in the world, often more quickly than traditional currency, and these transactions frequently take place on the dark web, which presents its own set of problems. While these ransom demands often used to be just a few hundred dollars, we now see American businesses targeted with ransom demands in the millions, and in some cases tens of millions, of dollars. The statistics paint a stark picture: in 2020, the FBI's Internet Crime Complaint Center (IC3) statistics showed a 20 percent increase in reported ransomware incidents and a 225 percent increase in ransom amounts. Unfortunately, what is reported is only a fraction of the incidents out there.[1]

We have also seen both nation-state adversaries and cybercriminals targeting managed service providers (MSPs), where by infecting one system, they can access the networks of hundreds of potential victims – as we saw in the recent Kaseya incident. But we are working to bring awareness to this method of compromise. Last month, our partners at the U.S. Secret Service (USSS) put together a cyber incident response simulation for companies that use MSPs, and it was my pleasure to join the Secret Service and give a unified federal message on the importance of hardening their systems and engaging with law enforcement before they are victims of an attack.

Ransomware has become one of the most costly and destructive threats to businesses and governments. On top of this, throughout the COVID-19 pandemic, we saw callous opportunism by criminal groups who put public safety at risk by attacking health care providers during a global pandemic. These groups demonstrate no morality; they will target entities big and small, public and private, and show little care for how their actions affect vulnerable populations.

How the FBI's Cyber Strategy Counters the Ransomware Threat

Because this criminal activity has become more lucrative and enticing, it is our job to make it harder and more painful for hackers to do what they are doing. That is why we announced a new FBI cyber strategy last year, using our 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 risk and consequences on cyber adversaries and use our unique law enforcement and intelligence capabilities and authorities to do so through joint operations sequenced appropriately for maximum impact. We have to target the entire criminal ecosystem – including malware developers, money launderers, and shady infrastructure providers – and work with agencies like the Cybersecurity and Infrastructure Security Agency (CISA), victims, and cybersecurity firms. All the while, we must continue to team with the Department of State to ensure our foreign partners are able and willing to cooperate in our efforts to bring the perpetrators of cybercrime to justice.

[1] In 2019, the IC3 received 2,047 ransomware complaints with adjusted losses of more than $8.9 million, though that is likely a small fraction of the true scope of the threat because it captures only those who individually reported to the IC3. These numbers represent a nearly 40 percent increase in ransomware complaints to the IC3, and more than double the adjusted losses reported in 2018. In 2020, the IC3 received 2,474 complaints identified as ransomware with adjusted losses of over $29.1 million.

More specifically, and in conjunction with the Department of Justice's recently-formed 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. When pursuing these actors, we work with like-minded countries to identify those responsible for damaging ransomware schemes, arrest them, and extradite them to the United States to face justice whenever possible. At the same time, taking down cybercriminals' technical infrastructure adds to the impact, as it raises their costs, disrupts their operations, prevents new victims, and often gives us new intelligence on their operations. Lastly, since virtual currencies are so central to ransomware, we have developed our ability to trace these transactions and have been able to seize funds and shut down illicit currency exchanges in some instances. We were recently able to accomplish this objective in the Colonial Pipeline case, when the victim and our federal partners worked quickly and closely with us to recover a substantial portion of the cryptocurrency paid as ransom.

We do all this with victims at the center of our efforts. At the FBI, we aim to inform, support, and assist victims in navigating the aftermath of crime and the criminal justice process with dignity and resilience. We want to empower all victims of cyber intrusions, just as we do for victims of other crimes. In some instances, we have done this by developing or acquiring a ransomware's decryption key to help victims recover without paying the ransom. We have also, on occasion, been able to give advance warning to vulnerable or targeted entities. 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.

As I mentioned, we have certain unique investigative authorities. Using our authorities, through our investigations, we are able to collect information that enables disruptions, which are most impactful when they include coordinated actions by us, our domestic partners like the Department of the Treasury and U.S. Cyber Command, and our foreign partners. As an example, the FBI is leading a whole-of-government counter-ransomware campaign coordinated through the National Cyber Investigative Joint Task Force (NCIJTF), which includes the U.S. Intelligence Community (USIC) and law enforcement partners from across the federal government. As an initial step in the campaign, the FBI partnered with the National Cyber Forensics and Training Alliance (NCFTA) to host its first annual ransomware summit in September 2019, which brought together the USIC, federal law enforcement agencies, and private sector partners with expertise in ransomware, cybersecurity, and cyber incident response to work on possible solutions to the ransomware problem.

Our strategy has enabled us to land some major blows against the threat actors behind ransomware and its delivery mechanisms. In addition to imposing these consequences against our adversaries, we shared the information from our investigations, intelligence collection, and incident response with foreign partners, others in the USIC, and agencies with a role in cybersecurity. And we worked especially closely with CISA to share information with critical infrastructure owners and operators via FBI reports and joint advisories. The ransomware threat

is not going away, so we must carry this strategy and its momentum forward through the rest of 2021 and into 2022.

Addressing Ransomware's Global Footprint

As I mentioned earlier, without strong foreign partnerships, our cyber strategy cannot be fully implemented and we cannot successfully counter the ransomware threat.

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 their whereabouts.

Not every foreign nation helps us in this fight. While we seek to disrupt entire cybercriminal enterprises, the most impactful consequence we can impose on a malicious cyber actor is an arrest as part of comprehensive disruption. If an actor is in a country like Russia or China, an arrest is currently not a viable option. Even when an indicted cybercriminal is in another country, Russia in particular takes actions to interfere with our extraditions. To make things more difficult, the lines between nation-states and cybercriminal actors are blurred, and even though a foreign nation may not be directing a ransomware campaign, it may still be complicit by providing a safe haven to those malicious actors who are doing harm to the United States, our citizens, and our businesses.

But our allies outnumber our foes, and in just the past few months, our work with foreign partners – supported by our legal attaches overseas – has led to impactful consequences against cybercriminals and sent a strong message that the reach of the U.S. government extends beyond its borders.

In January 2021, the FBI and others at the Department of Justice (DOJ) partnered with law enforcement and judicial authorities in the Netherlands, Germany, the United Kingdom, France, Lithuania, Canada, and Ukraine, with international activity coordinated by Europol and Eurojust, to disrupt the infrastructure of a highly destructive malware known as Emotet. Among other things, Emotet could also be used as a way 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.

Also this January, 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, and a subject was arrested in Canada pending extradition proceedings. In addition, we seized more than $450,000 in cryptocurrency.

Last month, through coordination with law enforcement and judicial authorities in The Netherlands, Germany, the United Kingdom, Canada, Sweden, Italy, Bulgaria, and Switzerland, we seized the web domains and server infrastructure of DoubleVPN, a virtual private network

that allowed ransomware actors to attack their victims and hide their tracks. Thanks to this international operation, this service, which was heavily advertised on both Russian and English-speaking cybercrime forums, is no longer available to cybercriminals.

How Victims and Potential Victims Can Help Themselves and Others

We have the strategy to take action against our cyber adversaries. But the strategy will fail if we do not know about suspicious activity or that a compromise has occurred. And because of the nature of U.S. laws and network infrastructure, we will never know about most malicious activity if it is not reported to us by the private sector.

We know ransomware victims, particularly large enterprises, risk negative publicity if they disclose being impacted by ransomware. As a result, ransomware incidents are often addressed by the victim directly and are never reported to the public or law enforcement. Ransomware incidents targeting public entities, such as state or local municipalities, often receive high levels of publicity. In addition to the losses reported to the IC3 I mentioned earlier, these groups face costs associated with business disruption and remediation, which can eclipse the ransom demand itself. For example, these costs were $17 million and $18.2 million, respectively, in ransomware campaigns against Atlanta and Baltimore.

I would like to spend a moment on the decision of whether or not to make a ransom payment. The FBI discourages ransomware victims from paying ransom for a variety of reasons. Even if a ransom is paid, there is no guarantee the business or individual will regain access to their data. On top of this, paying a ransom does not always keep data from ultimately being leaked. Additionally, paying a ransom incentivizes future ransomware attacks and emboldens criminal actors to continue their illicit work. However, **regardless of whether or not a victim chooses to pay, the FBI strongly encourages victims to report ransomware incidents to the FBI.** Our goal is to identify, pursue, and impose consequences on criminal actors, not their victims.

We are pushing important threat information to network defenders, and we are making it as easy as possible for the private sector to share 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 we speak with one voice. A call to one federal agency is a call to all federal agencies, and I hope we are sending that message by sitting as a unified front here today.

At the same time, we need the private sector to do its part. We need to be warned – quickly – when they see malicious cyber activity. We also need companies to work with us when we warn them they are being targeted. The recent examples of significant cyber incidents – SolarWinds, Microsoft Exchange, Colonial Pipeline, JBS, and Kaseya – only emphasize what Director Wray 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 really no other option for defending a country where nearly all of our critical infrastructure, personal data, intellectual property, and network infrastructure sit 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 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, CISA's website and the new interagency site www.StopRansomware.gov have 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 of 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 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 incident response. But it cannot stop there. Continue to share information with us after that meeting, and you have my word 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 via the Internet Crime Complaint Center at www.IC3.gov or 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.

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 ransomware 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.

Mandatory Reporting of Ransomware and Other Cyber Incidents

Because far too many ransomware incidents go unreported, and because silence benefits ransomware actors the most, we wholeheartedly believe a federal standard is needed to mandate the reporting of certain cyber incidents, including most ransomware incidents. Unlike other types of cybercrimes, the victim will almost always know when a ransomware incident has occurred. The scope and severity of this threat has reached the point where we can no longer rely on voluntary reports alone to learn about incidents. We support a nationwide standard that establishes which ransomware incidents must be disclosed, when and to whom they must be reported, and what those reports must include.

Mandatory ransomware incident reporting alone will not defeat the ransomware threat. However, it is a crucial step on that path for a number of reasons, and there are five in particular I would like to highlight. First, it will enhance the federal government's view of the threat and allow us to understand the full extent of ransomware activity nationwide. Second, this level of visibility will enhance cybersecurity efforts by informing cybersecurity advisories used to warn the public about incident trends and ransomware actors' specific tactics, techniques, and procedures. This in turn helps the public take appropriate steps to defend their networks. Having a better grasp of these trends and the specifics about individual incidents behind them will help the FBI organize strategic engagement with entities and industries that are experiencing the greatest harm. Third, it will assist incident response efforts so federal incident response agencies can provide support to a greater number of victims and collect evidence to open and advance cases. Fourth, having greater transparency into nationwide ransomware activity will help the FBI connect seemingly unrelated incidents to common actors so we can investigate the full extent of their activity and work to hold them accountable for all of their crimes. Fifth, reporting of ransom demands, payments, and details about those payments allows the FBI to "follow the money" to investigate where these payments are going and to whom, with the ultimate goal of seizing those funds.

One of the most important things Congress can do to assist the U.S. government's fight against ransomware is to pass a national cyber incident reporting standard. We believe the status quo is untenable, and to make significant progress against this threat, we need transparency into the full scope of the threat and the damage it is causing. Cybersecurity is national security. Simply put, if ransomware victims do not report these incidents, we cannot have cybersecurity, and we cannot have national security. Mandatory reporting legislation would take us a giant step toward protecting both.

The Resource Demands of Malicious Cyber Activity

When we do learn of a ransomware incident, our agents are in direct contact with victims and with private industry partners to share threat indicators—such as malicious IP addresses—and gather evidence that helps us identify who is compromised and who else is vulnerable. Our technically trained incident response assets throughout the country, collectively known as our

Cyber Action Team (CAT), assist affected entities. Our field offices with experience in complex national security and cyber investigations are our hubs for triaging the data we acquire through legal process, from partners, and through other lawful means. And our digital forensics and intelligence personnel exploit that information for indicators and intelligence that will help us to attribute the malicious activity to those responsible.

With the growing frequency and scale of recent significant cyber incidents – in some cases involving tens of thousands of victims – we are increasingly faced with hard choices that carry risk, include moving personnel away from long-term investigations or other significant incidents so we can surge toward the immediate need. 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. The FBI continues to exploit and analyze intelligence and technical data to uncover adversary tactics, share our findings, and pursue actions that will prevent those responsible from striking again.

Recent ransomware campaigns have shown us the investments in time, money, and talent cybercriminals are willing to make to compromise our networks. Accordingly, it requires a teams-based approach among various departments and agencies to understand, defend against, and counter these malicious cyber actors. Congress can help us by providing the resources requested in the President's 2022 Budget request to ensure the FBI and our partners are resourced to play our respective parts as we defend the nation together.

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 ransomware. As part of our strategy, we have been putting a lot of energy and resources into cultivating these partnerships. As Director Wray has put it, cyber is the ultimate team sport, and I truly believe our partners are seeing the benefits of having FBI Cyber on their team.

Chairman Durbin, Ranking Member Grassley, and members of the Committee, thank you for the opportunity to testify today. I am happy to answer any questions you might have and to work together with you in the nation's fight against ransomware so the FBI can help achieve our collective cyber mission – to give the American people safety, security, and confidence in our digitally connected world.