Testimony

Mr. Brandon Wales

Executive Director
Cybersecurity and Infrastructure Security Agency

U.S. Department of Homeland Security

FOR A HEARING

BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES

Committee on Oversight and Reform

"Cracking Down on Ransomware: Strategies for Disrupting Criminal Hackers and Building Resilience Against Cyber Threats"

November 16, 2021

Washington, D.C.

Chairwoman Maloney, Ranking Member Comer, and members of the Committee, thank you for the opportunity to testify today on behalf of the Cybersecurity and Infrastructure Security Agency (CISA) regarding ransomware and the federal response to countering this growing threat. I am truly honored to appear before the Committee today alongside National Cyber Director Chris Inglis and Bryan Vorndran, Assistant Director for the Cyber Division at the Federal Bureau of Investigation (FBI), to provide an update on our efforts to address the scourge of ransomware.

CISA's Mission and Role in Cybersecurity

At CISA, our mission is to lead the National effort to understand, manage, and reduce risk to the cyber and physical infrastructure Americans rely on every hour of every day. This mission includes two critical roles. First, we serve as the operational lead for federal cybersecurity and the federal government's support to the private sector, responsible for working with departments and agencies to protect and defend our civilian government networks and critical infrastructure. Second, we are the national coordinator for critical infrastructure security and resilience, another partnership endeavor given that of the vast majority of our nation's critical infrastructure is owned and operated by the private sector.

Indeed, our ability to execute our mission is built on collaboration. Securing our Nation's cyber and critical infrastructure is a shared responsibility, and never has collaboration been more important than it is today. At CISA, we are challenging traditional ways of doing business and are actively working with our government, industry, academic, and international partners to move from traditional public-private partnerships to public-private operational collaboration.

While our programmatic mission areas include cyber defense, infrastructure security, and secure communications, holistically, as one CISA, the organization is comprised of teams of individuals with expertise across a wide spectrum of professional backgrounds and disciplines. Each of them relies on each other to achieve our shared objectives. We recognize the connective tissue that binds us together to ensure the success of our mission, underpinned by our core values that represent the fundamental tenets of our CISA organization: collaboration, innovation, service, and accountability.

To achieve success in our cybersecurity mission, we build the national capacity to defend against cyber-attacks and work with our federal partners and provide them with cybersecurity tools, incident response services, and assessment capabilities to safeguard the federal civilian executive branch networks that support our Nation's essential operations. We strengthen our Nation's cyber defense by leading asset response for significant cyber incidents and ensuring that timely and actionable information about known cyber threats and incidents is shared with federal and state, local, territorial, and tribal (SLTT) officials, as well as our international and private sector partners, to ensure the security and resilience of our critical infrastructure.

We have an equally important mission to lead efforts to secure the nation's critical infrastructure, including SLTT government networks, against cybersecurity risks that could result in disruption to National Critical Functions upon which the American people depend. Federal civilian agencies, private sector businesses of all sizes, and critical infrastructure owners are facing urgent cybersecurity risks, including from nation-states and criminal groups such as ransomware gangs. To address these risks, CISA focuses on gaining visibility, improving operational coordination, and driving remediation.

First, CISA is focused on gaining visibility into cybersecurity risks that will allow us to more effectively assist victims and provide timely information to help prevent future incidents. We achieve this goal by providing sensors and other capabilities, such as remote scanning and threat hunting to identify suspicious, malicious, or potentially risky activity across federal civilian networks.

Second, CISA is uniquely positioned to receive and analyze data from multiple sources, including the intelligence community, the private sector, SLTT governments, and other partners, to understand how seemingly unrelated activity may indicate a significant intrusion or even a widespread campaign. CISA also works to prioritize identified risks by leveraging the capabilities of our National Risk Management Center (NRMC) to understand relative criticality of critical infrastructure assets – such as our oil and gas pipeline and electric-grid infrastructure – and working with our partners across government to understand our adversaries' intent and capabilities to exploit existing and emerging vulnerabilities.

Third, CISA drives remediation actions by providing incident response support and by coordinating with government and private sector partners for joint cyber defense operations that bring together capabilities from both sectors. Additionally, CISA further drives remediation by issuing binding directives for federal agencies to carry out, and a suite of recommendations through alerts and notices for the private sector's use and implementation in their own networks and cybersecurity defenses.

Earlier this month, we issued Binding Operational Directive (BOD) 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities.* This BOD will drive interagency action to aggressively manage government-wide risk, direct focus on actively exploited vulnerabilities causing harm now, and establish a catalog of vulnerabilities and mitigation guidance accessible to federal agencies and public and private organizations alike. This catalog includes a compiled list of vulnerabilities that CISA has deemed significant enough to pose a serious threat to federal networks. This directive will move federal agencies to improve their vulnerability management practices and dramatically reduce their exposure to cyber-attacks. Also, it requires them to review and refresh their vulnerability management policies and playbooks and establishes a more aggressive turnaround time for agencies to protect themselves against urgent, active threats.

While the BOD is only binding for federal civilian agencies, the actively exploited vulnerabilities covered by BOD 22-01 are exploited by actors of all types, including those who carry out ransomware activity. As a result, CISA strongly recommends that network defenders everywhere, including private businesses and state and local governments take the same to strengthen their security and resilience posture.

Cyber intrusions over the past several months have further reflected the fact that our country is facing an immediate threat to our national security, economic prosperity, and public health and safety. Nation-state actors and criminal groups continue to increase their sophistication and their willingness to target organizations across all sectors of the economy. The impacts of these attacks continue to increase, including impacts to the provision of National Critical

Functions from healthcare to energy to agriculture.

Ransomware: CISA Actions to Combat a Growing Threat

Ransomware is a form of malware that encrypts files on a device, rendering the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption, and often threaten to sell or leak the victim's data if the ransom is not paid. Malicious actors continue to evolve their ransomware tactics over time, highlighting a prime example of the vulnerabilities that are emerging as our digital and our physical infrastructure increasingly converge. Earlier this year, we saw the Colonial Pipeline attack shutter gas stations along the East Coast and the JBS attack cause certain food prices to rise. We have also seen ransomware attacks on schools, police departments, hospitals, and small businesses around the country, and they are growing in number, scale, and sophistication.

Ransomware incidents have become more destructive and impactful in nature and scope, and CISA remains vigilant in maintaining awareness of ransomware attacks and associated tactics, techniques, and procedures. While some recent incidents like the intrusion affecting Kaseya, an IT company providing remote management services for global customers including many Managed Service Providers, were more ambitious than usually observed from ransomware actors, most ransomware attacks generally do not use zero-day vulnerabilities or exquisite tradecraft, but rather exploit known security weaknesses or a failure to adopt generally accepted best practices. These actors are increasingly using tactics that make restoration and recovery more difficult or infeasible for impacted organizations. Consequently, much of CISA's efforts to mitigate ransomware are focused on ensuring that all organizations in our country understand the risks of ransomware and providing proactive measures that governments, organizations, and businesses can take to prevent themselves from becoming a victim of a ransomware attack in the first place.

Ransomware is a threat to national security, and President Biden has made countering it a priority. Just last week, the Department of Justice announced the indictment of a foreign national associated with the REvil ransomware group and believed to be responsible for the Kaseya ransomware attack and the seizure of $6.1 million in funds traceable to alleged ransomware payments received by a Russian national. CISA's mission focuses on raising awareness before disaster strikes and supporting victims when it does. We help potential victims understand their risk, reduce vulnerabilities, and mitigate the impact if they are attacked. When attacks threaten our critical infrastructure or national critical functions, we offer on-site assistance to help victims get back on their feet and share operationally relevant information with our partners and the public to prevent the spread to other potential victims and sectors. Our partners can use these resources to reduce the risk and impact of ransomware attacks.

In January 2021, CISA launched the "Reduce the Risk of Ransomware" awareness campaign to promote resources and best practices available focused on educating the public about the risks that ransomware poses and actions that can be taken immediately to strengthen cyber defenses. Additionally, in coordination with the Multi-State Information Sharing and Analysis Center (MS-ISAC), CISA released a joint Ransomware Guide that details industry best practices and a response checklist that can serve as a ransomware-specific addendum to state and local governments' cyber incident response plans.

In February, Secretary Mayorkas issued a call for action to tackle ransomware more effectively. To further drive a call to action, Secretary Mayorkas initiated a Ransomware Sprint in March 2021 that included a series of high-profile national events intended to ensure that leaders across all sectors of the economy understand the criticality of this risk and take urgent action in response. CISA supported the Ransomware Sprint, which ran through April and May 2021.

In July, building on the foundations of the ransomware campaigns, DHS launched the whole-of-government website, StopRansomware.gov, which provides users with a central, authoritative source for guidance, toolkits, and other resources from across the Federal Government. This collaborative initiative makes it easier for organizations and individuals to find free, authoritative information, resources, and tools from across the Federal Government in one place that they can use to prepare for and respond to ransomware intrusions. *StopRansomware.gov* is a whole-of-government resource hub hosted by CISA, sourcing content from across the federal government to highlight the latest ransomware-related alerts from these agencies. CISA will continue to work collaboratively with federal partners to add more resources to the website and promote on social media. Since launch, the site has had more than 458,834 pageviews.

By implementing various best practices, governments and businesses can reduce their ransomware attack surface. For example, we encourage our partners to maintain offline and encrypted backups of data; conduct regular vulnerability scanning to identify and address vulnerabilities; regularly patch and update software and operating systems, including antivirus and anti-malware software; implement a cybersecurity user awareness and training program, including guidance on identifying and reporting suspicious activity; and implement an intrusion detection system to detect command and control activity. These are among many other best practices contained in CISA's numerous guides and directives that organizations can access to help protect themselves from becoming the next ransomware victim. In addition, we urge all organizations impacted by a ransomware intrusion to immediately report their incident to CISA and to law enforcement so that the incident can be appropriately investigated. Upon receiving a report of a ransomware intrusion, CISA can offer technical guidance to help an organization effectively recover and develop alerts to help protect other possible victims.

To support our partners' cybersecurity posture, CISA provides a number of no-cost resources we encourage everyone to take advantage of. For example, we encourage SLTT governments to join the MS-ISAC, which is a free and voluntary center enabling bi-directional sharing of best-practices and network defense information regarding cybersecurity trends, including ransomware and malware that is a precursor to ransomware. Similarly, the Nationwide Cybersecurity Review is a no-cost, anonymous, annual self-assessment designed to measure gaps and capabilities of SLTT governments' cybersecurity programs. The Cybersecurity Review is based on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and is sponsored by DHS and the MS-ISAC.

Additionally, CISA provides assessments to help organizations understand how they can improve their defenses to avoid ransomware infection along with cyber exercises to evaluate and develop a cyber incident response plan in the context of a ransomware incident scenario.

CISA recently launched a new Ransomware Readiness Assessment, which has been downloaded over 14,797 times, to help all organizations evaluate their maturity in preparing for and responding to ransomware attacks. CISA also offers several services such as vulnerability scanning and remote penetration testing to assess, identify and reduce organizations' exposure to cybersecurity threats, including ransomware, at no cost. By requesting these services, organizations of any size can reduce their risk to ransomware attacks and other cyber threats. Finally, CISA has Cybersecurity Advisors (CSAs) deployed across the country to advise on best practices and to connect governments and businesses with additional CISA resources.

CISA is working with our partners – both at home and abroad – to provide actionable information so organizations both large and small can protect their networks, operations, data, and employees from ransomware attacks. Together with our industry and interagency partners, including law enforcement, we are working together to make it more difficult and more expensive for hackers and cybercriminals to operate.

Ransomware is a critical challenge and the risks posed to our nation are severe. But the challenge is not insurmountable. By investing in improved cybersecurity as recommended in CISA guidance, organizations can reduce the risk of a ransomware intrusion and limit its potential impacts.

Mitigating Future Risks

The recent high-profile ransomware attacks the country has faced – from the intrusions into the Colonial Pipeline Company and JBS Foods to the Kaseya supply-chain compromise – must serve as an urgent call to action to address our nation's cybersecurity risks. We must collectively and with great urgency strengthen our nation's cyber defenses, invest in new capabilities, and change how we think about cybersecurity, recognizing that all organizations are at risk, and we must focus on ensuring the resilience of essential services. To that end, CISA is acting with the utmost resolve to drive reduction of cyber risk to federal networks, SLTT governments, the private sector, and across the National Critical Functions. Achieving the progress we seek will require consideration of several key areas.

First, CISA is currently investing in and growing capabilities to increase visibility into cybersecurity risks across federal agencies and across non-federal entities. To accomplish this, we must enhance our ability to conduct persistent hunts for threat activity, ingest and analyze security data at all levels of the network, and conduct rapid analysis to identify and act upon known threats. At the same time, CISA is driving adoption of defensible network architectures, including implementation of zero-trust environments in which the perimeter is presumed compromised, and security must focus on protecting the most critical accounts and data. President Biden's Executive Order on *Improving the Nation's Cybersecurity* is driving critical progress in advancing cybersecurity across the federal government.

Second, CISA must work with all partners to gain increased visibility into national risks. With increased visibility, we can better identify adversary activity across sectors, which allows us to produce more targeted guidance, understand the degree to which adversary activity across sectors is increasing risk, and identify particular incidents requiring a specialized CISA response team. Our partnership with the Transportation Security Administration to develop Security

Directives requiring reporting of cybersecurity incidents to CISA is an important step and an example of such collaboration. We look forward to working with Congress to further encourage reporting of cybersecurity incidents to the federal government in order to further enable this essential visibility.

Third, incidents such as the Colonial Pipeline Company ransomware attack reinforce the need for CISA to continue to invest in and mature our partnerships with critical infrastructure entities across industries. The newly established Joint Cyber Defense Collaborative (JCDC) is building on these partnerships to lead the development of the Nation's cyber defense plans by working across the public and private sectors to help defend against cyber threats to the nation. Authorized in the National Defense Authorization Act for Fiscal Year 2021, the JCDC brings together the authorities, capabilities, and talents of the interagency – CISA, the National Security Agency, the Secret Service, the Federal Bureau of Investigation, Cyber Command, the Department of Justice, and the Office of the Director of National Intelligence – with the power of industry to enable shared situational awareness of the threat landscape, to plan and exercise against the most significant threats to the nation, and to implement cyber defense operations against these threats.

This new collaborative promotes national resilience by coordinating across federal agencies, to include Sector Risk Management Agencies (SRMAs); state, local, tribal and territorial (SLTT) partners; and industry to protect against, identify, detect, and plan for and respond to malicious cyber activity targeting U.S. critical infrastructure. The JCDC also leverages CISA's broad authorities to share information about threats and vulnerabilities to enable early warning and prevent other victims from being attacked. This shifting paradigm will enable us to transform information sharing into information enabling – timely, relevant, and actionable. On ransomware specifically, the JCDC will develop a comprehensive ransomware campaign plan that will unify efforts, synchronize activities, and identify strategic objectives to increase resilience and reduce the likelihood of a ransomware attack. Further, the JCDC will design and implement joint cyber defense plans to thwart efforts by malicious cyber actors to disrupt critical infrastructure through a whole-of-nation approach to cyber defense operations.

Along with development and implementation of a planning process to address identified cybersecurity risks, the JCDC provides a new model for collaborating with companies that can drive cybersecurity change at scale, including directly reducing the risk of ransomware intrusions. Collaboration through the JCDC has already yielded several successes over the past year:

- Received multiple "indicator packages" of technical information from JCDC partners, which was then circulated to other members for enrichment and dissemination broadly across federal and critical infrastructure partners;
- Enriched pre-release versions of recent high-profile products, such as our joint alerts on Conti and BlackMatter ransomware, using input from JCDC partners leveraging their visibility into ransomware risks across sectors; and
- Information from an international partner enabled us to engage a trusted industry partner to facilitate the provision of decryption keys to recent ransomware victims in the food and agriculture sector.

Recognizing that we cannot prevent all intrusions, we must drive a focus on resilience and functional continuity even as we drive improvements in security. We must advance business continuity exercises even as we catalyze adoption of cybersecurity best practices; we must ensure that operational technologies are segmented from and can run independently from business networks even as we advance our ability to detect threats in both environments; and we must reduce single points of failure across our National Critical Functions as we identify and harden identified nodes of systemic risk.

Finally, I would like to thank Congress for entrusting DHS with two new authorities that will enhance our ability to reduce the frequency and impact of ransomware attacks. Congress recently passed H.R. 3684, the Infrastructure Investment and Jobs Act, which included language authorizing and resourcing a Cyber Response and Recovery Fund (CRRF) at CISA. The CRRF sets aside dedicated funding and authorizes CISA to quickly access that funding at scale to provide incident response and recovery activities. The ability to quickly deploy resources in response to major cybersecurity incidents will help CISA quickly access information about the incident, render assistance to victims, and share information potential victims can use to prevent or mitigate the impact of the attack. The bill also authorizes a new DHS cybersecurity grant program administered by the Federal Emergency Management Agency with the support of CISA. This program will allow SLTT partners to apply for federal resources they can use to enhance the security and resilience of their networks. CISA looks forward to implementing these authorities as quickly as possible so we can enhance CISA's ability to respond to major incidents and raise our SLTT partner's security and resilience against cyber incidents, including ransomware attacks.

Cyber Incident Reporting Legislation

As our adversaires continue to target our Nation's critical infrastructure via ransomware or other cyber attacks, CISA will continue to pursue ways to increase visibility into federal and critical infrastructure networks. We must also continue to rely on network owners and operators to identify and report anomalous and potentially nefarious activity on their networks to CISA and our partners.

Although incident reporting requirements exist within certain sectors, there is currently no single mandatory federal requirement to report cyber incidents. Rather, entitities must assess the complex disclosure requirements imposed by an array of agencies at the Federal and State levels. When a victim does seek to do the right thing and report an incident to the Federal government, they may not know which agencies to contact, delaying their reporting during an emergency situation. Among the harms this may cause is a lag in availability of critical mitigation guidance to the operators who are positioned to take action.

We appreciate the work of members of Congress in both the House and the Senate who have drafted or introduced bills on cyber incident notification over the past several months, including members of this Committee. The earlier that CISA, the Federal lead for asset response, receives information about a cyber incident, the faster we can conduct urgent analysis and share information to protect other potential victims.

To that end, cyber incident reporting must be timely, as soon as possible after a covered incident is determined to have occurred. Reporting should be broad-based, and not limited by type or sector, with the Government retaining the ability to set reporting thresholds and requirements for covered entities. These entities include critical infrastructure, federal agencies, and government contractors. It should also provide clear and compelling enforcement mechanisms that ensure compliance. We encourage Congress to adopt a cyber incident notification reporting approach that appropriately focuses broadly on cybersecurity incidents, including cyber supply chain and ransomware attacks, and provides CISA and DOJ, in coordination with other relevant agencies, the flexibility to modify the scope of the requirements as necessary, balancing the benefits of reporting against burdens to industry and government.

Conclusion

Our nation faces unprecedented risk from cyber-attacks undertaken by both nation-state adversaries and criminals. Ransomware is not a new phenomenon, but its continued growth and recent high-profile attacks should serve as a wake-up call to organizations to take this threat seriously and shore up their systems. The list of significant incidents in recent months is long and growing. Now is the time to act – and CISA is helping to lead our national call to action. We will deepen our partnerships with critical infrastructure partners, enhance our visibility into national cybersecurity, and drive targeted action to reduce vulnerabilities and detect our adversaries. In collaboration with our government partners, critical infrastructure entities, our international allies, and with the support of Congress, we will make progress in addressing this risk and maintain the availability of critical services to the American people under all conditions.

Thank you again for the opportunity to be to appear before the committee. I look forward to your questions.