Testimony

Eric Goldstein

Executive Assistant Director for Cybersecurity
Cybersecurity and Infrastructure Security Agency

U.S. Department of Homeland Security

FOR A HEARING

BEFORE THE UNITED STATES SENATE

Committee on the Judiciary

America Under Cyber Siege: Preventing and Responding to Ransomware Attacks

July 27, 2021

Washington, D.C.

Chairman Durbin, Ranking Member Grassley, 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 combat this growing threat.

Given the surge of debilitating ransomware attacks against private sector businesses and our critical infrastructure, as well as recent cybersecurity incidents impacting the federal government, this hearing provides a timely opportunity to review how CISA works with federal agencies and private sector entities to manage cybersecurity incidents in light of the urgent ransomware challenge. I also look forward to discussing lessons learned from recent cybersecurity incidents and sharing some perspective on how we can apply those lessons to improve our collective cybersecurity.

CISA's Mission and Role in Cybersecurity

CISA leads national efforts to advance the cybersecurity, physical security, and resilience of our critical infrastructure. In particular, CISA is a focal point to exchange cyber defense information and enable defensive operational collaboration among the Federal Government, and state, local, tribal and territorial (SLTT) governments, the private sector, and international partners.

One of CISA's primary missions is to enhance the security of federal networks. To accomplish this mission, CISA leads a collaborative effort with its partners throughout the Department of Homeland Security (DHS), the Office of Management and Budget and the broader interagency to identify and drive reduction of the most significant cyber risks, which includes providing tools, services, training, guidance and direction that helps enable timely identification of, protection against, and response to cybersecurity risks. We *Defend Today* through collective defense against threats and vulnerabilities and *Secure Tomorrow* by providing effective strategies and approaches to long-term risk management and cyber resilience. Our vision is a secure and resilient cyber enterprise that enables the federal government to provide critical services to the American people under all conditions.

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 help victims and provide timely information to help prevent future incidents. We work to 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.

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 an ever-evolving 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, and CISA is urgently focused on reducing the risk of ransomware attacks that are targeting organizations across sectors.

Recently, ransomware attacks have surged among SLTT governments and critical infrastructure organizations. In fact, it is estimated that over 100 federal, state and municipal agencies, over 500 medical centers, and 1,680 educational institutions in the United States were hit by ransomware in 2020 and ransom demands exceeded $1 billion dollars.[1] This epidemic is now affecting our nation's most critical infrastructure: municipal governments, police departments, hospitals, schools, manufacturing facilities, and of course, pipelines.

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

[1] Emisoft, *The State of Ransomware in the US: Report and Statistics 2020*, https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/; Emisoft, *The Cost of Ransomware in 2020: A Country-by-Country Analysis*, https://blog.emsisoft.com/en/35583/report-the-cost-of-ransomware-in-2020-a-country-by-country-analysis/.

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. 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 governments, organizations and businesses can take to prevent themselves from becoming a victim of a ransomware attack in the first place.

To that end, CISA and DHS have acted urgently to catalyze national action around this risk, and in January 2021, CISA unveiled the Reduce the Risk of Ransomware Campaign to raise awareness and blunt this ongoing and evolving threat. The campaign is a focused, coordinated and sustained effort to encourage public and private sector organizations to implement best practices, tools, and resources that mitigate ransomware risk. 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.

Moreover, in February, during his first remarks dedicated to cybersecurity, Secretary Mayorkas issued a call for action to tackle ransomware more effectively, and to further drive a call to action, Secretary Mayorkas initiated a Ransomware Sprint in April 2021 that has 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.

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 (IDS) 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 law enforcement and to CISA 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. Moreover, CISA recently launched a new Ransomware Readiness Assessment 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 Cyber Security Advisors (CSAs) deployed across the country to advise on best practices and to connect governments and businesses with additional CISA resources.

Most recently, building on earlier ransomware campaigns, on July 15, 2021 DHS spearheaded a new inter-agency website – *StopRansomware.gov,* a collaborative initiative to make it easier for organizations across the country to access the information they need to prepare for and respond to ransomware intrusions. *StopRansomware.gov* is the new ransomware homepage for federal government agencies, including CISA, the FBI, U.S. Department of Health and Human Services, U.S. Secret Service, and the National Institute of Standards and Technology (NIST), to pool resources that can give businesses and organizations of all sizes a one-stop-shop to learn how to reduce their ransomware risk and provide them the opportunity to better protect their networks. The website will also highlight the latest ransomware-related alerts from these agencies.

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* will drive critical progress in advancing cybersecurity across the federal government. Going forward, we must take lessons learned from our investments in federal cybersecurity to support organizations across sectors in driving similar change.

Second, CISA must work with all possible 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 TSA to develop two 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 reinforces the need for CISA to continue to invest in and mature our partnerships with critical infrastructure entities across industries. For example, our Cyber Information Sharing and Collaboration Program (CISCP) serves as a bi-directional forum in which CISA and private industry are collaborating on significant risks, developing sector-specific threat-focused products, and providing briefings on new trends, threats, and capabilities across the sectors. With information sharing protections available through the Cybersecurity Information Sharing Act of 2015 and the Protected Critical Infrastructure Information Act, the program enables trusted sharing between CISA and a network of high impact companies, Information Sharing and Analysis Centers (ISACs), and service providers.

Within CISCP, the Mutual Interest Initiative brings together cyber threat companies and Internet service providers to work with CISA and the broader government community to exchange analysis and collaboratively work on threat actor focused products. Furthermore, CISCP enables CISA to work in close coordination with software vendors and endpoint detection companies to both assess the impact of and mitigate the risk of critical vulnerabilities. From a technical standpoint, these partnerships with industry enable us to better understand the nature of vulnerabilities pre-and post-disclosure and in turn provided timely and thorough mitigation guidance to government agencies and critical infrastructure.

Going forward, CISA is establishing a Joint Cyber Planning Office (JCPO), as required by the Fiscal Year 2021 National Defense Authorization Act, to further mature our capabilities to plan, exercise, and coordinate cyber defense operations with partners across the government and private sectors. The JCPO 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 JCPO 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.

Lastly, 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.

Conclusion

Our nation is facing unprecedented risk from cyber attacks undertaken by both nation-state adversaries and criminals. 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.