Testimony

Christopher Krebs
Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

FOR A HEARING ON

"What States, Locals and the Business Community Should Know and Do: A Roadmap for Effective Cybersecurity"

BEFORE THE
UNITED STATES SENATE

Homeland Security and Governmental Affairs Committee

February 11, 2020

Washington, DC

Chairman Johnson, Ranking Member Peters, and members of the committee, thank you for the opportunity to testify regarding the Cybersecurity and Infrastructure Security Agency's (CISA) support to state, local, tribal, and territorial (SLTT) and the private sector to mitigate cyber threats. Our mission is to defend against the threats of today and secure against the evolving risks of tomorrow. We work with partners across all levels of government and in the private sector to– "Defend Today, Secure Tomorrow."

CISA leads the Nation's efforts to ensure the security and resilience of our cyber and physical infrastructure. We assist agencies with the protection of civilian federal networks, and coordinate with other federal agencies, SLTT governments, and the private sector to defend our Nation's critical infrastructure from malicious cyber activity. By bringing together all levels of government, the private sector, international partners, and the public, DHS protects against cybersecurity risks, improves our whole-of-government incident response capabilities, enhances information sharing of best practices and cyber threats, and strengthens resilience of our Nation's critical infrastructure and protects our way of life.

Cyber Threats

Cyber threats remain one of the most significant strategic risks for the United States, threatening our national security, economic prosperity, and public health and safety. Advanced persistent threat actors, hackers, cyber criminals, and nation-states, have increased the frequency and sophistication of their attacks. In a 2018 report, *Foreign Economic Espionage in Cyberspace,* the U.S.'s National Counterintelligence and Security Center stated, "We anticipate that China, Russia, and Iran will remain aggressive and capable collectors of sensitive U.S. economic information and technologies, particularly in cyberspace." Our adversaries are developing and using advanced cyber capabilities in attempts to undermine critical infrastructure, target our livelihoods and innovation, steal our national security secrets, and threaten our democratic institutions.

Just last month, in response to increased geopolitical tensions and threats with Iran, CISA released a *CISA Insights Resource*[1] to inform our private sector and SLTT partners about enhanced risk and appropriate security postures. CISA also actively shared information with thousands of public and private sector stakeholders across the critical infrastructure community through regular, coordinated teleconferences. This is dynamic, two-way communication in real time. CISA provides information and stakeholders have a forum to share their experiences, ask questions and get answers. Additionally, CISA coordinated closely with other federal partners and the intelligence community to ensure a coordinated response to the potential threats. These activities will be replicated as the cyber threat landscape continues to evolve.

Cybersecurity threats are all around us, but Ransomware is a specific type of cyber threat that has been in the news a great deal lately. Ransomware is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected

[1] *CISA Insights: Ransomware Outbreak.* Cybersecurity and Infrastructure Security Agency. August 21, 2019. Accessed at: https://www.us-cert.gov/sites/default/files/2019-08/CISA_Insights-Ransomware_Outbreak_S508C.pdf

website. In a typical ransomware attack, hackers have the ability to take over a system, locking out owners and operators and potentially disabling the system functions or holding the system information hostage until a ransom is paid. Ransomware can be devastating to an individual or an organization in the form of critical public safety services suspended, personal information at risk and potentially millions in financial loss possible. Anyone with important data stored on their computer or network is at risk.[2] In 2017, WannaCry was a global example of ransomware that opened our eyes to the potential breadth and depth of the harm that such attacks could cause. Ransomware continues to be a major threat facing US critical infrastructure, SLTT, and the private sector.

Ransomware has rapidly emerged as the most visible cybersecurity risk playing out across our nation's networks. Unfortunately, ransomware seems to be a business model that works, and victims are paying higher and higher ransoms.[3] According to a recent report from EMSISOFT, in 2019 ransomware attacks impacted at least 966 government agencies, educational establishments and healthcare providers at a potential cost of $7.5 billion. A further breakdown shows 113 state and municipal governments and agencies, 764 healthcare providers, and 89 universities, colleges, or school districts were impacted by ransomware.[4]

Between 2018 and 2019, several of the largest US cities fell victim to this type of cyber attack. In 2018, ransomware impacted the city of Atlanta, including its city services and programs.[5] In November of 2018, the Justice Department announced criminal charges against two Iranian citizens in a series of ransomware attacks against Atlanta, Newark, New Jersey, Port of San Diego, the Colorado Department of Transportation, a university, and multiple hospitals using the SamSam Ransomware.[6] In 2019, ransomware infected Baltimore city government computers, demanding a payment of thousands of dollars to free systems.[7] This past December, New Orleans declared a state of emergency due to a ransomware attack, prompting a shutdown of digital services.[8] This represents only a few of the reported ransomware attacks on state and local governments. It's important to note that all statistics we discuss today are based on the landscape of known or reported attacks. A significant concern with ransomware attacks is that we do not know how many incidents go unreported.

CISA Services

In an effort to protect against and respond to evolving cyber threats, CISA offers technical services ranging from proactive vulnerability scanning to malware analysis. CISA leverages technical expertise during cyber incidents providing mitigation recommendations and ensuring that threats are widely known. CISA provides exercises and training programs to

[2] https://www.us-cert.gov/Ransomware

[3] Catalin Cimpanu. "The average ransom demand for a REvil ransomware infection is a whopping $260,000." *ZDNet*. January 28, 2020. Accessed here: https://www.zdnet.com/article/the-average-ransom-demand-for-a-revil-ransomware-infection-is-a-whopping-260000/

[4] "The State of Ransomware in the US: Report and Statistics 2019," ENSISOFT Malware Lab. December 12, 2019. Accessed at: https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/

[5] Benjamin Freed. Atlanta was not prepared to respond to a ransomware attack. *StateScoop*. April 24, 2018. Accessed at: https://statescoop.com/atlanta-was-not-prepared-to-respond-to-a-ransomware-attack/

[6] Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses. Press Release. Department of Justice. November 28, 2018.

[7] Ian Duncan and Colin Campbell. "Baltimore city government computer network hit by ransomware attack." *The Baltimore Sun.* May 7, 2019. Accessed at: https://www.baltimoresun.com/politics/bs-md-ci-it-outage-20190507-story.html

[8] Kristen Korosec. "New Orleans declares state of emergency following ransomware attack." *TechCrunch*. December 14, 2019. Accessed at: https://techcrunch.com/2019/12/14/new-orleans-declares-state-of-emergency-following-ransomware-attack/

critical infrastructure partners around the nation. We help build awareness of an evolving threat as well as increase understanding of what steps to take to mitigate these threats. CISA offers incident management and response capabilities through sharing, and analysis. We also offer response to cyber threats--such as sending experts to Ukraine to assist in the aftermath of the 2015 attack on Ukraine's electric grid.

During the global ransomware attacks in 2017, then NPPD, now CISA, collaborated domestically and internationally to protect critical infrastructure and federal networks. (For example, we conducted malware analysis on multiple samples of the suspected threat vector and collaborated with commercial service providers to discover and share indicators related to the ransomware.) Additionally, CISA issues technical information for network defenders around the globe , enabling them to reduce their exposure to mitigate the consequences of an attack. When the RobbinHood ransomware attack occurred, CISA, in conjunction with the FBI, promptly shared our analysis of the vulnerabilities that the malicious cyber actors were able to exploit.
.

In July 2019, CISA released a joint statement with our partners at the Multi-State Sharing and Analysis Center, (MS-ISAC), the National Governor's Association (NGA) and the National Association of State Chief Information Officers (NASCIO) with three simple, actionable steps to increase state and local resilience against ransomware. These steps included, Back Up Your System; Reinforce Basic Cybersecurity Awareness and Education; and Revisit and Refine Cyber Incident Response Plans.

In the fall of 2019, CISA released several resources aimed at assisting its stakeholders in raise the level of their cybersecurity practices. These resources include:

- ***CISA Insights - Ransomware Outbreak*****:** The Insights document focuses on Ransomware and building a better understanding of how attacks are taking place and what actions can be done to mitigate such attacks. The document includes elements like: backing-up data, system images, and configurations and keep the backups offline; updating and patching systems; reviewing and exercising incident response plans; and asking for help from CISA, the FBI, or the Secret Service.

- ***CISA's Cyber Essentials***: The Essentials document is a guide for leaders of small and medium businesses as well as leaders of state, local, tribal and territorial government agencies to develop an actionable understanding of where to start implementing organizational cybersecurity practices.

- ***Ransomware Cyber Tabletop Exercise Package:*** Commonly referred to as "exercise in a box," the Exercise Package is as a resource for state, local, and private sector partners that includes template exercise objectives, scenario, and discussion questions, as well as a collection of ransomware and cybersecurity references and resources. Partners can use the exercise package to initiate discussions within their organizations about their ability to address the threat of ransomware, which is impacting the community with increasing frequency.

CISA Insights, Cyber Essentials and other materials, including a webinar on Ransomware, viewed over 4,000 times, are available online at www.us-cert.gov/ransomware to assist state and local governments, and small and medium-sized businesses.

At CISA, we believe that there are six key attributes of a successful cyber program. Two strategic attributes are leadership engagement and a culture of security. Two technical attributes are knowing what is on your network and knowing who is on your network. Finally, the two tactical attributes are being able to recover after an incident, utilizing backups that have been tested and having a plan in place that includes outreach to employees, public, etc. CISA actively coordinates with our state and local stakeholders to better understand the support they need to defend their systems from a ransomware attack. CISA utilizes a layered approach to supporting SLTTs through direct assistance, indirect assistance, and self-service capabilities to raise their level of cyber resilience. CISA funds the MS-ISAC, that not only provides a range of free services, but also serves as a network where SLTT agencies can share best practices and lessons learned with each other. Additionally, our partnerships with the private sector are essential. Private sector companies are regularly called in to help victims rebuild systems. We need partnerships and input from them as we continue to build out and strengthen our incident efforts.

CISA will continue to raise awareness of the threat, sharing key actions that make organizations harder, more resilient targets. Additionally, we have come together with our other interagency partners to build-up a ransomware campaign working through the FBI's National Cyber Investigative Joint Task Force (NCIJTF).

CISA Cybersecurity Operations

CISA provides entities with information, technical assistance, and guidance that they can use to secure their networks, systems, assets, information, and data by reducing vulnerabilities, ensuring resilience to cyber incidents, and supporting their holistic risk management priorities. CISA also does allied tasks in the physical critical infrastructure and communications coordination mission areas. CISA operates at the intersection of the Federal Government, state and local governments, the private sector, international partners, law enforcement, intelligence, and defense communities. The *Cybersecurity Act of 2015* (P.L. 114-113) established DHS as the Federal Government's central hub for the sharing of cyber threat indicators and defensive measures. By focusing on rapid sharing of the technical features that permit network defenders to identify and respond to threats while minimizing the receipt of personally identifiable information, CISA's automated indicator sharing capability allows the Federal Government and private sector network defenders to share technical information at machine speed. This sharing provides greater situational awareness for all sectors and entities across an ever-evolving threat landscapes.

CISA, our government partners, and the private sector are all engaging in a more strategic and unified approach towards improving our nation's overall defensive posture against malicious cyber activity. In May of 2018, the Department published the *DHS Cybersecurity Strategy*, outlining a strategic framework to execute our cybersecurity responsibilities during the next five years. The *National Cyber Strategy*, released in September 2018, reiterates the criticality of collaboration and strengthens the government's commitment to work in partnership with industry to combat cyber threats and secure our critical infrastructure. Together, the *National Cyber Strategy* and *DHS Cybersecurity Strategy* guide CISA's efforts.

The National Cybersecurity Incident Response Plan (NCIRP), required by Presidential Policy Directive 41, outlines how the US government will respond to a significant cyber incident. The plan addresses the various roles of the private sector, state and local governments, as well as multiple federal agencies. DHS, acting through CISA, is the lead for asset response during a significant cyber incident. CISA's asset response activities include providing technical instance to affected entities, mitigating vulnerabilities and impacts of a cyber incident. CISA is also responsible for identifying additional entities that may be affected and assessing risks of cascading impacts. Lastly, CISA is responsible for facilitating information sharing and operational coordination.[9]

Conclusion

In the face of increasingly sophisticated threats, CISA employees stand on the front lines of the Federal Government's efforts to defend our Nation's federal networks and critical infrastructure. The threat environment is complex and dynamic with interdependencies that add to the challenge. As new risks emerge, we must better integrate cyber and physical risk in order to effectively secure the Nation. CISA contributes unique expertise and capabilities around cyber-physical risk and cross-sector critical infrastructure interdependencies.

I recognize and appreciate the committees strong support and diligence as it works to understand this emerging risk and identify additional authorities and resources needed to address it head on. We at CISA are committed to working with Congress to ensure our efforts cultivate a safer, more secure, and resilient Homeland through our efforts to defend today and secure tomorrow.

Thank you for the opportunity to appear before the Committee today, and I look forward to your questions.

[9] National Cyber Incident Response Plan, Department of Homeland Security, December 2016.