Testimony

Brandon Wales
Acting Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

FOR A HEARING ON

"*State and Local Cybersecurity:*
***Defending our communities from cyber threats amid COVID-19*"**

BEFORE THE
UNITED STATES SENATE

Committee on Homeland Security and Governmental Affairs
Subcommittee on Federal Spending Oversight & Emergency Management

December 2, 2020

Washington, DC

Chairman Paul, Ranking Member Hassan, and members of the Subcommittee, thank you for the opportunity to testify regarding the Cybersecurity and Infrastructure Security Agency's (CISA) mission to secure cyberspace and critical infrastructure. Our mission is to defend against the threats of today while working with partners across all levels of government and in the private sector to secure against the evolving risks of tomorrow – "Defend Today, Secure Tomorrow."

As the Nation's risk advisor, CISA leads the Nation's efforts to ensure the cybersecurity, physical security, and resilience of our critical infrastructure. CISA operates at the intersection of the Federal Government, state and local governments, the private sector, international partners, law enforcement, intelligence, and defense communities. By bringing together partners from across the critical infrastructure landscape, we enable the collective defense against cybersecurity risks, improve incident response capabilities, enhance information sharing of best practices and cyber threats, strengthen our resilience, and facilitate safety.

We share timely and actionable classified and unclassified information as well as provide training and technical assistance, and we do this in ways that prioritize the protection of privacy, civil liberties, and confidentiality. Specifically for State, Local, Tribal and Territorial (SLTT) Governments – which is the topic of today's hearing - the technical assistance and guidance provided can be used to secure networks, systems, assets, information, and data by reducing vulnerabilities, ensuring resilience to cyber incidents, and supporting their holistic risk management priorities. CISA's regional personnel are deployed in all States and territories to provide advisory services and assist the private sector and State and local government in improving their risk posture. With the support of this committee, CISA is in the process of hiring an advisor to serve in each State as a primary point of contact to improve State and local government cybersecurity.

As we continue to understand and support the management of the largest cyber threats facing our SLTT partners, a snapshot into what we have seen over the recent past could be grouped into three areas of focus: COVID-19 pandemic response and the mass shift to remote work and learning; cyber threats from ransomware; and election security. Independently, each of these threats is significant; taken together, they have the potential to stress systems and networks to the brink and we are working tirelessly to help SLTT leaders to defend today and secure tomorrow.

COVID-19 Response

Due to the global pandemic, the risk landscape shifted dramatically over the last eleven months. In March, CISA launched an effort to provide enhanced cybersecurity support to high-risk entities in the healthcare sector. When the Administration established Operation Warp Speed, CISA joined the interagency effort to offer cybersecurity services. In addition, CISA is leveraging its relationships with interagency and industry partners to facilitate greater communication and information sharing between the private sector, SLTT partners and the Federal government through coordinated alerts, guidance, and recurring engagement calls since the beginning of March.

CISA has been focused on understanding the impact of this shift and identifying organizations that are most critical to the response. Through our cybersecurity defensive services, our vulnerability scanning, and our information-sharing mechanisms, we are engaging with these critical organizations to assist them in establishing a strong defense today as well as a culture of resilience moving forward. In addition, we continue to assess the national critical functions, which allows us to identify and mitigate risk before it impacts critical infrastructure.

Support to Operation Warp Speed

Throughout Operation Warp Speed (OWS), CISA has focused on securing end-to-end COVID-19 vaccine production from research and development to manufacturing, and distribution, including countermeasures. Almost overnight, a set of American companies and institutions became indispensable, especially test labs, vaccine developers, and personal protective equipment manufacturers. CISA quickly began working with the Department of Health and Human Services (HHS), the Department of Defense (DoD), and the pharmaceutical industry to identify these entities and ensure they directly received necessary additional cybersecurity support, such as vulnerability scanning services, information sharing, and incident response.

CISA is working with its interagency partners on defensive activities, leveraging its relationships with government and industry partners to facilitate greater communication, coordination, prioritization and information-sharing between the private sector and the government through various alerts and guidance. We are also building cyber capacity by providing guidance for consumers and companies to increase cybersecurity maturity and awareness CISA's specific cyber defense/response activities include:

- Conducted 6 independent or joint notifications to OWS entities, covering open critical vulnerabilities, observed advanced persistent threat (APT) targeting or activity, or compromise.
- Provided 4 advanced warnings of state-sponsored cyber threats, which identified 2 additional entities targeted by APT 29 for information collection and 2 organizations potentially vulnerable to Chinese offensive activities.
- Provided notification of 8 critical vulnerabilities, helping to ensure that organizations patch appropriately to the risk level and where there may be increased risk of intrusion/affect from adversary cyber activities.
- Published 2 cyber advisory alerts highlighting APTs targeting OWS and 3 indicator bulletins.
- Conducted 6 incident investigations, including engagement with victims through initial forensics, malware and threat analysis.

CISA has also increased adoption of its Cyber Hygiene, which is a standard service offering that performs recurring scans of an organizations public facing IP addresses for known vulnerabilities with automated reporting to the organization, this service is available to all Federal agencies and designated critical infrastructure sectors. Cyber Hygiene services have increased from 5% of the

most important OWS entities to 62%, with 100% coverage of all OWS prime entities directly responsible for delivering vaccines.

CISA has also partnered with the Intelligence Community on the Overwatch service to better correlate existing intelligence collection to the infrastructure of key entities. This is a temporary intelligence and warning offering for OWS and related COVID response entities monitors threats involving the entities name, domains, and IP addresses. Overwatch adoption has gone from 0% to 62% with 100% coverage of the primes. CISA has also pledged to deliver monitoring services to up to 15 companies, with multiple companies currently going through the adoption and onboarding process and 17 separate detailed cyber vulnerability and architecture assessments and 10 field-based physical security assessments.

Essential Critical Infrastructure Workforce Guidance

Beginning in March, CISA released the Essential Critical Infrastructure Workers Guidance (ECIW), providing assistance and guidance to States and jurisdictions as they considered how to prioritize and support essential workers to operate safely while supporting ongoing infrastructure operations across the Nation. The guidance is advisory and seeks to identify, through analysis and coordination with Government Coordinating Councils and Sector Coordinating Councils, those critical infrastructure sectors, workers, and functions that should continue to work safely during the COVID-19 response across all jurisdictions. Through several updates issued throughout the Spring and Summer, CISA was able to account for the changing landscape of the Nation's COVID-19 response to support SLTT decision makers.

Early versions of the guidance were primarily intended to help officials and organizations identify essential work functions in order to allow them access to their workplaces during times of community restrictions. CISA's final release, Version 4.0, highlighted additional essential workers and specialized risk management strategies to ensure that personnel can work safely as States re-open. CISA will continue to work with our partners in the critical infrastructure community to update this advisory list if necessary, as the Nation's response to COVID-19 evolves.

CISA COVID – 19 Resources and Alerts

In addition, CISA is providing a one-stop-shop of cybersecurity and critical infrastructure resources from across Federal, private sector, and international partners to raise their security posture in this new landscape. Some of these resources include:

- *Cyber Essentials Toolkit*: A set of modules designed to break down the CISA Cyber Essentials into actions for IT and C-suite leadership to work toward full implementation of each Cyber Essential element.
- *CISA Trusted Internet Connections 3.0 Interim Telework Guidance*: Focuses on remote Federal employees connecting to private agency networks and cloud environments in a secure manner.

- *Best Practices for Industrial Control Systems*: Released with the Department of Energy, and the UK's National Cyber Security Centre (NCSC).
- *COVID-19 Recovery CISA Tabletop Exercise Package*: Developed to assist private sector stakeholders and critical infrastructure owners and operators in assessing short-term, intermediate, and long-term recovery and business continuity plans related to COVID-19.
- *Critical Infrastructure Operations Centers and Control Rooms Guide for Pandemic Response*: The guide provides considerations and mitigation measures for operation centers and control rooms but can be applied further to any critical node that is required to continue functioning in a pandemic environment.
- *CISA Insights: Risk Management for Novel Coronavirus (COVID-19)*: Provides executives a tool to help them think through physical, supply chain, and cybersecurity issues that may arise from the spread of Novel Coronavirus, or COVID-19.
- *Security and Resiliency Guide – Healthcare and Public Health Facility Annex:* This resource provides information to assist stakeholders with performing counter-improvised explosive device activities specifically applicable to healthcare and public health facilities.
- *Physical Security Considerations for the Healthcare Industry During COVID-19 Response:* Is a jointly developed product among CISA, Health and Human Services (HHS), and Federal Bureau of Investigation (FBI). It provides information regarding potential physical threats posed to the healthcare community during the pandemic.

Since the outbreak of COVID-19 in March 2020, and in collaboration with domestic and foreign partners, CISA provides up-to-date cyber threats and COVID-19 alerts. Some of our more recent alerts include:

- *Ransomware Activity Targeting the Healthcare and Public Health Sectors:* This joint cybersecurity advisory was coauthored by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS). This advisory describes the tactics, techniques, and procedures (TTPs) used by cybercriminals against targets in the Healthcare and Public Health (HPH) Sector to infect systems with ransomware.
- *Chinese Targeting of COVID-19 Research Organizations*: CISA and FBI Joint Alert warning that the People's Republic of China (PRC) is likely targeting organizations researching COVID-19.
- *Cyber Warning for Key Healthcare Organizations in the UK and USA*: The UK's National Cyber Security Centre and CISA have exposed malicious cyber campaigns targeting organizations involved in the coronavirus response.
- *COVID-19 Exploited by Malicious Cyber Actors, Joint UK, and US Alert*: This alert provides information on exploitation by cybercriminals and advanced persistent threat (APT) groups of the current coronavirus disease 2019 (COVID-19) global pandemic.
- *Enterprise VPN Security Alert*: Alert encouraging organizations to adopt a heightened state of cybersecurity when considering alternate workplace options for their employees.

To address the increased risk introduced by expanded telework during the COVID-19 pandemic, CISA has built an online portal for telework, addressing an array of issues, including remote patching, securing sensitive and proprietary data, and incorporating virtual collaboration tools. The Telework Center of Excellence portal brings together in one place products from

across the Federal government and private sector, including CISA, the Office of Personnel Management (OPM), National Institute of Standards and Technology (NIST), Cyber Readiness Institute, National Cyber Security Alliance, and the Global Cyber Alliance. Key recent releases include:

- *Cybersecurity Recommendations for K-12 Schools Using Video Conferencing Tools and Online Platforms*: A video conferencing product for a school district and campus IT administrators and staff charged with securing their IT networks, as well as end-users, such as teachers, to help them think through their cybersecurity issues.
- *Video Conferencing: Guidelines to Keep You and Your Students Safe*: A one-page tip sheet for schools using video conferencing.
- *Guidance for Securing Video Conferencing*: A product for organizations and individual users leveraging video conferencing tools, some of whom are remotely working for the first time.
- *Cybersecurity Recommendations for Federal Agencies Using Video Conferencing*: A product for executives charged with securing Federal agency networks, and for Federal employees to help them think through related cybersecurity and physical issues.
- *Cybersecurity Recommendations for Critical Infrastructure Using Video Conferencing*: A product for executives charged with securing critical infrastructure networks and for critical infrastructure employees to help them think through related cybersecurity and physical issues.
- *Telework Best Practices with CISA and NSA*: A joint-seal product from CISA and NSA featuring "Do's" and "Don'ts" for teleworking.
- *Tips for Video Conferencing*: A tip sheet with top recommendations on how to safely videoconference, with tips such as: 1) Only Use Approved Tools; 2) Secure Your Meeting; 3) Secure Your Information; and 4) Secure Yourself.

Additional resources and alerts can be found at https://www.cisa.gov/coronavirus.

COVID-19 Emergency Communications – Assistance and Alerts

Throughout the COVID-19 response, our Nation's public safety communications across the Federal and SLTT landscape have been tested as never before with the nationwide shift to a virtual environment. Emergency communications need to work the first time, every time, during all threats and hazards that threaten lives and property.

A decade of emergency communications interoperability preparations and planning was critical in mitigating impacts of COVID-19 and the stress placed on emergency communications. CISA's work with long-standing partners, including SAFECOM, the National Council of Statewide Interoperable Coordinators (NCSWIC), and Federal department and agencies, provided a clear understanding of emerging requirements and the ability to act decisively. Together with the Statewide Interoperability Coordinators (SWICs), CISA was able to operationalize the National Emergency Communications Plan to support an evolving ecosystem and those on the front line; increase connectivity to priority networks for essential workers to

mitigate network contestation, seeing a dramatic increase of Priority Telecommunication Services (PTS) use, expedited over 70,000 PTS activations, and support to several major hospitals, medical centers, and critical infrastructure manufacturers; and, developed critical emergency communications policies, guides, advisories, and technical standards, including:

- *Guidelines for Executives: 911 Center Pandemic Recommendations:* Emphasizes the importance of communication centers, accentuates the particular risk of a pandemic to resiliency of 911 operations, communicates executive-level action, and describes available guidance for 911 administrators.
- *Guidelines for 911 Centers: Pandemic Planning:* Highlights governance, resource planning, and contingency considerations from a holistic perspective during a pandemic.
- *Guidelines for 911 Centers: Pandemic Operating Procedures:* Recommends how to organize, train, and care for personnel while operating during a pandemic.
- *Guidelines for 911 Centers: Cleaning and Disinfecting During a Pandemic:* Presents cleaning and disinfecting guidance specific to public safety and resources for 911 centers during a pandemic.

Ransomware

Cybersecurity threats are all around us, and ransomware is a specific malicious 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 can be devastating to an individual or an organization in the form of disrupting critical public safety services, placing personal information at risk, and potentially losing millions of dollars financially. Ransomware continues to be a significant threat facing U.S. critical infrastructure, SLTT, and the private sector.

Ransomware has rapidly emerged as the most visible cybersecurity risk playing out across our Nation's networks. In just the past few months, several hospital systems across the country and the globe were affected by ransomware. In October, the University of Vermont Health Network was reported to the targeted of a ransomware attack that impacted a variety of patient services, including access to medical records. The network has restored access to electronic medical records, but is still in the process of restoring all its services.[1]

Additionally, multiple hospital systems and healthcare providers across the U.S. have incurred ransomware attacks creating varying degrees of impact. In October, CISA, in coordination with the FBI and HHS issued a joint cybersecurity advisory warning the Healthcare and Public Health (HPH) Sector of increased and imminent threats to healthcare providers from ransomware attacks.[2]

[1] "University of Vermont Medical Center Continuing Cyber Attack Recovery." Insurance Journal. December 1st, 2020. Accessed here.
[2] Alert AA20-302A, Ransomware Activity Targeting the Healthcare and Public Health Sector, Cybersecurity and Infrastructure Security. October 28, 2020. Accessed here.

CISA has several tools, products, and services to help protect against cybersecurity risks and vulnerabilities, like ransomware, including:

- *Joint CISA/ MS – ISAC Ransomware Guide:* A one-stop product for Ransomware Prevention Best Practices and includes a Ransomware Response Checklist, information on available risk management services from CISA, and explains how to request analysis and response assistance from the Federal Government.
- *CISA Insights: Ransomware Outbreak:* Provides stakeholders an understanding of how ransomware attacks unfold and what steps organizations can take to better defend their systems.
- *Protecting your Center from Ransomware:* Provides comprehensive information to stakeholders on how to protect public safety answering points (PSAPs) and emergency communications centers (ECCs) from ransomware.
- *Cyber Risks to Next Generation (NG911) white paper*: Provides an overview of the cyber risks that will be faced by NG911 systems.
- *NG911 Readiness Self-Assessment Tool*: The NG911 Self-Assessment Tool helps ECC/PSAP administrators and oversight personnel evaluate a system's NG911 maturity state and understand the next steps necessary to continue NG911 deployment progress.
- *Cyber Risks to 911: Telephony Denial of Service Fact Sheet:* This fact sheet familiarizes public safety communications partners with Telephony Denial of Service (TDoS) threats to 911.
- *Cyber Assessments:* Based on NIST 800-53 framework; reviews processes and procedures and areas of improvement.
- *Ransomware Awareness/Education Brief for PSAP, 911 and LMR Operations*: Provides best practices for secure use of technologies in daily operations, including interactive webinar with PSAP/9-1-1/LMR operations staff.

Election Security

CISA leads DHS efforts to secure our nation's election infrastructure. CISA, our Federal partners, state and local election officials, and the private sector prepared for the 2020 elections for nearly four years. Due to the exceptional efforts of the election community, at this time there is no evidence that any voting system deleted or lost votes, changed votes, or was in any way compromised. Since 2016, CISA has led a voluntary partnership of Federal Government and election officials who regularly share cybersecurity risk information. CISA has engaged directly with election officials—coordinating requests for assistance, risk mitigation, information sharing, and incident response. To ensure a coordinated approach to assisting election officials with protecting the election infrastructure they manage, CISA has convened stakeholders from across the Federal Government through CISA's Election Security Initiative. CISA and the Election Assistance Commission (EAC) have convened Federal government and election officials regularly to share cybersecurity risk information and to determine an effective means of assistance. Since 2017, the Election Infrastructure Subsector (EIS) Government Coordinating Council (GCC) has worked to establish goals and objectives, to develop plans for the EIS partnership, and to create an EIS Sector-Specific Plan. Participation in the council is voluntary and does not change the fundamental role of state and local jurisdictions in overseeing elections.

CISA and the EAC have also worked with election equipment and service vendors to launch, in 2017, an industry-led Sector Coordinating Council (SCC), a self-organized, self-run, and self-governed council with industry leadership designated by SCC members. The SCC serves as the industry's principal entity for coordinating with the Federal Government on critical infrastructure security activities related to sector-specific strategies. The SCC has helped CISA further its understanding of election systems, processes, and relationships.

CISA, through the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC), now provides threat alerts to all 50 states and more than 2800 local and territorial election offices. In addition, all 50 states, 250 localities, three territories and DC now have intrusion detection sensors. These sensors are operated and monitored by EI-ISAC as part of the Multi-State Information Sharing and Analysis Center's (MS-ISAC) Albert intrusion detection system. DHS shares intelligence and other cyber threat information with EI-ISAC for use in Albert, which assists with identifying specific threats to election infrastructure networks.

For most of the year, COVID-19 has provided an additional layer of complexity to the work of state and local election officials. CISA and the EAC have worked closely with the election community to provide the necessary services and resources throughout the primaries, in the run-up to the general election, and during the voting and post-election periods. At the beginning of the outbreak, the EIS GCC and SCC created a Joint Working Group consisting of government and industry representatives, to analyze aspects of different voting methods and to provide written resources to state and local officials seeking to mitigate exposure to COVID-19 while administering elections. The Joint Working Group has to date produced numerous guidance documents, addressing such issues as voter education about administrative changes and the importance of accurate voter data when expanding absentee voting. CISA has also hosted calls through the spring and summer between the election community and the Centers for Disease Control and Prevention (CDC), the United States Postal Service (USPS), and other relevant Federal partners, to help ensure that election officials have the most up-to-date information and advice from the experts at these agencies regarding COVID-19 response.

CISA continues to build national resilience against foreign influence operations through public education and awareness to help Americans better understand the threat of foreign influence and simple steps they can take to avoid amplifying foreign influence operations. CISA has developed innovative methods to help Americans recognize and avoid foreign disinformation operations targeting our democracy, which includes the #WarOnPineapple campaign to help educate Americans on the tactics of malicious foreign influence campaigns. CISA also coordinates closely with social media platform counterparts to enable election officials to report mis- and disinformation from these platforms.

CISA has worked directly with our Federal, state, and local partners on these and other issues through a number of exercises. In July 2020, we hosted our third iteration of Tabletop the Vote, a nationwide exercise that engaged more than 1,750 participants. The exercise enabled participants to explore and assess issues related to voter confidence, voting operations, and the integrity of elections in response to simulated cyber and physical threats impacting the 2020 election. CISA also works directly with Federal, state, local, and critical infrastructure partners to

exercise their plans and procedures in tailored exercises. In Fiscal Year 2020, we have conducted 22 of these direct partner exercises focused on elections security. These events not only build the capabilities of our partners, but also strengthen the relationships and information sharing among the community to enhance our collective preparedness.

On Election Day, CISA hosted an in-person classified and unclassified operations center, bringing together Federal agencies with private sector organizations, including both major political parties, social media companies, election technology companies, and other organizations. CISA also stood up a virtual National Cybersecurity Situational Awareness Room, an online portal for state and local election officials and their private sector partners to share real-time information and support as needed. CISA will remain in an enhanced coordinated posture until after all election results have been certified and will continue to remain vigilant to protect against attempts by foreign actors to target or disrupt this process.

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 government networks and critical infrastructure. The threat environment is complex and dynamic, with interdependencies that add to the challenge. CISA contributes unique expertise and capabilities around cyber-physical risk and cross-sector critical infrastructure interdependencies.

I recognize and appreciate the Subcommittee's 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 Subcommittee today, and I look forward to your questions.