April 10, 2024

The Honorable Ron Wyden
Chair
Subcommittee on Water and Power
Committee on Energy and Natural Resources
United States Senate
304 Dirksen Senate Building
Washington, DC 20510

The Honorable James E. Risch
Ranking Member
Subcommittee on Water and Power
Committee on Energy and Natural Resources
United States Senate
304 Dirksen Senate Building
Washington, DC 20510

Dear Chair Wyden and Ranking Member Risch:

In light of the Subcommittee's April 10, 2024, hearing, Cyber Threats to and Vulnerabilities of Critical Water Infrastructure in our Energy Sector, attached please find Western Governors' Association (WGA) Policy Resolution 2022-05, Cybersecurity. The resolution provides recommendations to address threats to critical infrastructure and calls for improved agency coordination.

I request that you include this document in the permanent record of the hearing, as it articulates Western Governors' policy positions and recommendations related to this urgent issue.

Thank you for your attention to this matter and your consideration of this request. Please contact me if you have any questions or require further information.

Sincerely,

Jack Waldorf
Executive Director

Attachment

Policy Resolution 2022-05

Cybersecurity

A. BACKGROUND

1. In the age of automation, digitization, big data, artificial intelligence, and machine-to-machine learning, the United States' capabilities to prevent, detect and respond to cyberattacks are of ever-growing importance to our society. The cybersecurity of our nation is an all-of-government and industry-wide endeavor.

2. Aging information technology (IT) infrastructure and systems pose serious cybersecurity risks and increase vulnerabilities for government and organizations. Due to the longstanding financial and national security implications of prior cybersecurity breaches resulting in data theft and other adverse outcomes, modernizing these systems to help prevent successful cyberattacks and better safeguard our data is imperative.

3. The COVID-19 pandemic has transformed society and accelerated the shift to a virtual environment, further increasing vulnerabilities across systems as threat actors become more complex and widespread. Ransomware attacks, a type of malicious software attack that threatens to publish sensitive information or impedes access to data or computer systems until the victim pays a ransom to the attacker, have grown by 148 percent due to the rise in remote activities. These attacks can shut down public and private sector operations, posing particular challenges to critical infrastructure functions.

4. Cybersecurity is especially imperative for critical infrastructure, which includes the nation's electric grid, energy resource supply and delivery chains, finance, communications, election systems, the chemical industry, commercial facilities, critical manufacturing, defense industrial base, emergency services, food and agriculture, government facilities, health care and public health, information technology, transportation, and water and wastewater systems. Large-scale cyber incidents, including the SolarWinds and Colonial Pipeline attacks, demonstrate the risk cybercrime now presents to national security.

5. Addressing cybersecurity needs across critical infrastructure sectors is further complicated by the increasing interdependency and interconnectedness of our nation's data systems to a myriad of non-critical infrastructure systems and a dynamic threat environment. Effective cybersecurity programs require strategic and functional relationships and information sharing between federal, state and local levels of government, and the public and private sectors.

6. The cybersecurity of their states and the nation is a high priority of Western Governors. State governments are responsible for securing public networks, the state's digital assets, and citizen data, as well as coordinating their cybersecurity efforts with federal agencies and potentially-affected private entities (e.g., utilities, financial institutions, transportation, and health). Governors lead efforts to plan and implement state cybersecurity programs, respond to cyberattacks, and investigate intrusions.

7. National Guard cyber protection teams, serving in 59 cyber units, provide invaluable assistance to states across the country with threat assessment and cyber incident response and remediation. Currently, states can mobilize Guard members through State Active Duty (SAD) and Title 32 of the U.S. Code. Supported by state funds, Governors can activate SAD for disasters or homeland defense, although state constitutions or statutes often constrain deployment of the Guard to state emergencies. Title 32 gives Governors the authority to order the Guard to duty, using federal funds, with the approval of the President or the Secretary of Defense. However, this process can create barriers to rapid and nimble action in the face of cyberattacks. While both of these functions are vital resources, potential exists to further leverage the capabilities of the National Guard for the cybersecurity posture of states.

8. Although state and local governments remain significant targets for cyberattacks, they often lack adequate funding to address these issues and modernize their systems. According to a study by Deloitte and the National Association of State Chief Information Officers, state cybersecurity budgets comprise less than 3 percent of their overall IT budgets.

9. Prior to the passage of Public Law 117-58, the Infrastructure Investment and Jobs Act, the Homeland Security Grant Program was the primary federal mechanism to provide cybersecurity funding to state, local, territorial, and Tribal governments. Over the years, less than 4 percent of that funding was allocated to cybersecurity. Such low levels of funding have been insufficient for states to meet their pressing, and rapidly growing, cybersecurity needs. The Infrastructure Investment and Jobs Act sought to address this issue by establishing a much-needed standalone cybersecurity grant program for state and local governments, marking a huge increase in federal support for state and local cybersecurity efforts.

10. The $1 billion program will be administered by the Federal Emergency Management Agency (FEMA) for four years, with the Cybersecurity and Infrastructure Security Agency (CISA) serving in an advisory role. Funding will be distributed to states, tribes, and territories, who must allocate about 80 percent to their localities. States must also meet varying match requirements to share the financial burden and account for cybersecurity costs in their budgets.

11. State election systems remain targets of foreign interference. As Governors, we remain committed to protecting our states' election systems. There is nothing more fundamental to the enduring success of our American democracy, and we take seriously our responsibility to protect the integrity and security of our elections. This is an imminent national security threat that transcends party lines. This is a matter of protecting and preserving fair elections – the underpinning of our democracy.

12. The Office of Management and Budget and Department of Homeland Security May 2018 Federal Cybersecurity Risk Determination Report and Action Plan concluded that 71 of 96 federal agencies are at risk or high risk of cyber intrusions. It also determined that federal agencies are not equipped to determine how threat actors seek to gain access to their information. This deficiency results in ineffective allocations of the agencies' limited cyber resources.

13. Currently, there is a severe deficit of cyber workers, especially in government. Our nation cannot defend itself without a well-trained, experienced cyber workforce. The public sector must dedicate resources to "K through gray" cybersecurity education, training, work-based learning and apprenticeships, and recruitment programs and encourage the private sector to do the same through effective policy.

14. While investments in workforce development and human capital are a key component in addressing workforce shortages, states can leverage other tools to meet the scale of these challenges. Technology and innovation will be needed to alleviate workforce strains and keep pace with a wide range of attacks while also reducing burdens associated with operational functions.

B. GOVERNORS' POLICY STATEMENT

1. Western Governors urge Congress to improve coordination of congressional oversight and legislative activity on cybersecurity, including by reducing the number of committees in Congress that have jurisdiction over this issue.

2. Western Governors support modernizing our systems to be more resilient to minimize vulnerabilities and protect against unauthorized access to information and data theft. We request that FEMA and CISA work collaboratively with Governors in executing the newly created state and local cybersecurity grant program to ensure the funds are administered in a flexible and measurable manner to all states, Tribes, and territories. Designated, flexible, and measurable cybersecurity funding would help ensure that states, Tribes, and territories have resources to build resilient systems and meet growing cybersecurity challenges.

3. The federal government has a responsibility to provide adequate funding for states to meet election security needs. Western Governors encourage Congress and the Administration to work cooperatively with states in developing election security legislation and mandates, and to fully fund implementation.

4. Federal agencies must engage in early, meaningful, substantive, and ongoing consultation with Governors or their designees on all aspects of cybersecurity. Western Governors advise the federal government to clearly define the roles for state representatives in CISA's recently established Joint Cyber Defense Collaborative.

5. Western Governors recommend that the federal government continue the DHS State, Local, Tribal, and Territorial Engagement Program, which provides cybersecurity risk briefings and resources to Governors and other officials. The Governors also support CISA Central, with which state chief information officers regularly interact.

6. The federal government must continue to clarify the roles and responsibilities of federal agencies in preventing, preparing for, and responding to cyberattacks. Centralized authority, points of contact, and formalized communication pathways are necessary to address increasingly complex threats. In addition, these pathways must occur at each level within government and other organizations.

7. The federal government must also improve agency coordination to use often-constrained security resources more efficiently and harmonize disparate regulations that put an

unnecessary burden on state governments. Western Governors urge Congress to provide appropriations for the Office of the National Cyber Director commensurate with the importance of the office's position in leading federal coordination efforts.

8. The National Institute for Standards and Technology (NIST) Cybersecurity Framework and other standards can facilitate effective, consistent, and risk-based decision making in government and industry. Real-world simulations of attacks on critical infrastructure are essential to prepare our nation for potential threats.

9. The federal government should build a stronger international framework for cybercrime and use the full range of economic tools, including travel and financial sanctions, to deter cyberattacks organized, supported, or harbored by nation-states.

10. Western Governors recognize the need for states, Tribes, and territories to work together to address gaps or vulnerabilities in these systems to reduce disruptions. The public sector, particularly the federal government, must take steps to mitigate global supply chain and national critical infrastructure risks (e.g. ransomware) in collaboration with the private sector.

11. Western Governors implore Congress and the Administration to reduce bureaucratic burdens and change restrictive guidance related to deploying the National Guard under USC Title 32 for cybersecurity prevention, detection, and response activities. Clarifying the use of the National Guard for these purposes and streamlining the approval process would improve state capacity to confront cyberattacks, contain threats, and help protect neighboring jurisdictions. Western Governors also support efforts to develop civilian cybersecurity reserves, which help alleviate workforce shortages and augment National Guard forces.

12. The Administration should propose, and Congress should provide, long-term authorization and sufficient appropriations for high-quality cybersecurity education and workforce development programs to grow and sustain the cybersecurity workforce, including those that target underrepresented populations, those that include rotational components to retain personnel, and work-based learning opportunities such as apprenticeships. The federal government should also expand the CyberCorps: Scholarship for Service program and continue to support educational initiatives, such as NIST's Initiative for Cybersecurity Education and National Centers of Academic Excellence in Cyber Defense.

13. Government and industry should increase the cybersecurity awareness of government and private employees through training and education. Western Governors encourage the federal government to develop a national cybersecurity literacy and awareness campaign to educate citizens about how to stay safe online and prevent effective cyberattacks.

14. Western Governors support incentives for the creation of and participation in programs that encourage information sharing across all levels government, industry verticals, and regions. We also support other policies that incentivize the private sector to improve cybersecurity and share information regarding cyber threats as early as possible, including policies to improve access to information or create common standards for information-sharing. The federal government should emphasize the benefits of information sharing, while alleviating private sector concerns with this essential communication. The federal

government and states should continue to investigate liability protections, such as safe harbor provisions, for entities that report cyber intrusions.

15. Our nation requires innovation in detecting, preventing, and responding to continually evolving cyber threats. More research is required to understand the use of blockchain and encryption by perpetrators and its utility for defense against cyber threats, and address vulnerabilities of other emerging technologies, including connected vehicles and Internet of Things devices. The federal government should provide funding and technical assistance for these and other types of cybersecurity research and development.

C. GOVERNORS' MANAGEMENT DIRECTIVE

1. The Governors direct WGA staff to work with congressional committees of jurisdiction, the Executive Branch, and other entities, where appropriate, to achieve the objectives of this resolution.

2. Furthermore, the Governors direct WGA staff to consult with the Staff Advisory Council regarding its efforts to realize the objectives of this resolution and to keep the Governors apprised of its progress in this regard.

This resolution will expire in December 2024. Western Governors enact new policy resolutions and amend existing resolutions on a semiannual basis. Please consult http://www.westgov.org/resolutions for the most current copy of a resolution and a list of all current WGA policy resolutions.