Policy Resolution 2019-02

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. 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, healthcare and public health, information technology, transportation, and water and wastewater systems.

3. Addressing cybersecurity needs across critical infrastructure sectors is further complicated by the increasing interdependency and interconnectedness of our nation's data systems to 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.

4. 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.

5. 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.

6. The Office of Management and Budget and Department of Homeland Security (DHS) 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.

7. 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 cybersecurity education, training, and recruitment programs and encourage the private sector to do the same through effective policy.

B. GOVERNORS' POLICY STATEMENT

1. Western Governors urge Congress to improve coordination of congressional oversight and legislative activity on cybersecurity. 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.

2. Federal agencies must engage in early, meaningful, substantive, and ongoing consultation with Governors or their designees on all aspects of cybersecurity. The federal government must also 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.

3. The increasing number and inconsistency of federal security regulations puts an unnecessary burden on state governments and is an inefficient use of often-constrained security resources. The federal government should establish a working group with representatives from states and federal agencies, as well as restore the position of the White House cybersecurity coordinator, to harmonize disparate agency regulations.

4. 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 DHS's Office of Cybersecurity and Communications, with which state chief information officers regularly interact.

5. 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.

6. The federal government should use the full range of economic tools, including travel and financial sanctions, to deter cyberattacks organized or supported by nation-states.

7. The public and private sectors must take steps to mitigate global supply chain risks (e.g. installation of malicious software or hardware). Government and industry should also increase the cybersecurity awareness of government and private employees through training and education.

8. 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. The federal government should also expand the CyberCorp: 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.

9. Western Governors support 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.

10. 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.

Western Governors enact new policy resolutions and amend existing resolutions on a bi-annual basis. Please consult westgov.org/resolutions for the most current copy of a resolution and a list of all current WGA policy resolutions.