NCSL
NATIONAL CONFERENCE OF STATE LEGISLATURES

Brian Patrick Kennedy
Speaker Pro Tempore
Rhode Island General Assembly
President, NCSL

Sabrina N. Lewellen
Deputy Director - Senate
Assistant Secretary of the Senate
Arkansas General Assembly
Staff Chair, NCSL

Tim Storey
Chief Executive Officer
NCSL

Statement for the Record

On behalf of

National Conference of State Legislatures

Hearing on

Cybersecurity Issues for Local Governments and Municipal Authorities

Provided to

Pennsylvania State Senate Joint Local Government and Communications and Technology Committees

Jan. 31, 2024

Susan Parnas Frederick
Senior Federal Affairs Counsel
National Conference of State Legislatures

Thank you Chair Pennycuick, Minority Chair Dillon, Chair Brown and Minority Chair Kearney for having me here today. My name is Susan Parnas Frederick, and I am the senior federal affairs counsel at the National Conference of State Legislatures (NCSL) in our Washington, D.C. office. NCSL is a bipartisan organization representing the legislatures of the nation's 50 states, five territories and Washington, D.C. NCSL's mission is to strengthen the institution of the legislatures, provide connections between the states and serve as the voice of state legislatures in the federal system of government. I am pleased to provide the joint committee with the following statement for the record on current federal and state cybersecurity initiatives and legislation.

While the 117th and 118th Congress have seen many bills related to cybersecurity introduced in both chambers, no federal legislation has passed both and become law. However, it is instructive to see where Congress has placed its cybersecurity priorities through legislation it has introduced. Two bills are illustrative.

In the Senate, the priority is on protecting critical infrastructure, and S. 3600, the "Strengthening American Cybersecurity Act of 2022" was a bipartisan bill that passed the Senate in March 2022. It required the Cybersecurity and Infrastructure Agency (CISA) to perform ongoing and continuous risk assessments of federal agency cybersecurity protocols and required entities that own or operate critical infrastructure to promptly report to the federal government any cybersecurity incidents, including ransomware attacks.

The House of Representatives passed H.R. 4502 in October 2023 and it is currently awaiting action in the Senate. This bipartisan bill focuses on bolstering our national cyber workforce. If it becomes law, it will modify educational requirements for federal cybersecurity jobs by shifting federal hiring standards away from traditional education such as a four-year college degree and toward two-year associate degrees or certification programs offered by private sector companies.

Although the Senate and the House have not yet coalesced around any cybersecurity legislation, the Cybersecurity and Infrastructure Security Agency (CISA) has moved forward on several initiatives to protect our critical infrastructure. In its 2023 "Year in Review," CISA outlined its major accomplishments in cybersecurity. These included a revised paper instructing software manufacturers to update their design and development programs and stressed three core principles of top-down leadership, transparency and accountability, and "owning customer security outcomes." Through its pre-ransomware notification initiative, CISA has been able to assist organizations by warning them of potential ransomware attacks. CISA documents more than 1,200 pre-ransomware notifications in various sectors such as water and wastewater entities, K-12 school districts and transportation system entities.

With respect to water and wastewater system sectors (WWS), CISA published an Incident Response Guide in collaboration with the FBI and the Environmental Protection Agency. It also solicited input from state and local government stakeholders and other industry and nonprofit organizations. This document provides guidance and strategies to improve the cybersecurity of WWS systems nationwide. It describes the four stages of incident response and discusses how CISA's free cybersecurity vulnerability scanning can assist state and local governments and WWS facilities to better prepare for a cyber incident.

States have also been active in introducing and passing cybersecurity legislation. In 2023, At least 40 states, Guam, Puerto Rico and Washington, D.C., introduced or considered more than 500 bills or resolutions that addressed cybersecurity issues. Thirty-nine states and Washington, D.C. passed cybersecurity legislation, enacted at least 130 bills and adopted 10 resolutions in 2023.

Multifactor authentication was an emerging topic in state legislatures last year. Maryland and Utah passed legislation in this area. Several states such as New Jersey and Rhode Island passed legislation addressing state agency cyber incident reporting requirements and Indiana and Washington passed bills establishing advisory boards to establish best cybersecurity practices. Overall, states have been very active in the cybersecurity space, and we expect to see many more bills passed in the 2024 legislative sessions.

Thank you for your time. Please contact me or any member of my team with any questions you may have.