July 24, 2019

The Honorable Cory Gardner
U.S. Senate
354 Russell Senate Office Building
Washington, D.C. 20510

The Honorable Mark Warner
U.S. Senate
703 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Derek Kilmer
U.S. House of Representatives
1410 Longworth House Office Building
Washington, D.C. 20515

The Honorable Michael T. McCaul
U.S. House of Representatives
2001 Rayburn House Office Building
Washington, D.C. 20515

Dear Senators Gardner and Warner and Representatives Kilmer and McCaul:

On behalf of the nation's states, cities and counties, we write to you in appreciation of your efforts, and in support of the State Cyber Resiliency Act (S.1065 and H.R. 2130). Our members believe this legislation would strengthen the nation's cybersecurity posture through state and local cybersecurity grants administered by the U.S. Department of Homeland Security (DHS).

The State Cyber Resiliency Act would provide increased and dedicated funding to help develop and implement innovative cybersecurity practices, help to build resources and human capital, as well as help to increase intergovernmental partnerships. The public and private sectors share a responsibility to ensure the resiliency and investments necessary to maintain a robust cyber infrastructure, and the State Cyber Resiliency Act will help state and local governments better dedicate resources to this shared mission.

Our global economy, society, infrastructure and daily life are more interconnected and increasingly dependent upon the security and reliability of communications technology and digital infrastructure. The potential for a cyber incident to move to the physical realm, impacting human safety, looms large for state and local governments. The rise of complex cyber incidents, intrusions and disruptions highlights the critical need to establish and support a comprehensive approach to protecting sensitive information and technology systems at all levels of government.

This includes innovative partnerships to further effective policies and processes; develop better detection and information sharing practices; clarify roles and responsibilities; and develop response and recovery plans to mitigate disruptions. A comprehensive strategy also requires investment in resiliency and a stable and competent cyber workforce.
We believe that the federal government and the private sector should view state and local governments as key partners in cybersecurity efforts. Federal, state and local governments should develop and implement government-wide, holistic cyber resiliency plans that incorporate and implement strategic initiatives identified in their cybersecurity strategies.

However, states and localities are stretching finite homeland security and information technology resources to meet these evolving threats to critical infrastructure, communications systems, financial systems, sensitive databases and election security. This necessitates innovative and adaptable strategies and planning, as well as increased funding to deploy comprehensive security resources and recruit and retain a capable cyber workforce.

The 2018 Deloitte-NASCIO Cybersecurity Study stressed the evolving role of cybersecurity over the past 10 years, noting that most states now have formally approved governance processes and guidelines across the state enterprise. But acquiring adequate resources and workforce to carry out these requirements continues to challenge. As a result, states allocate between 0 and 3 percent of their overall IT budget on cybersecurity of their state networks. Similarly, cybersecurity spending within existing grant programs- such as the Homeland Security Grant Program - can prove a challenge in the face of declining federal allocations, increased allowable uses, and a strong desire to maintain existing capabilities that states have spent years building.

For these reasons, the National Governors Association (NGA), the National Association of State Chief Information Officers (NASCIO), the Governors Homeland Security Advisors Council (GHSAC) and the National Conference of State Legislatures (NCSL) applaud the introduction of this legislation. The new grant program authorized by the State Cyber Resiliency Act would prioritize best practices at all levels of government and help participating state and local governments coordinate resources, better respond to threats, and plan for a strong and resilient cyber future. Overall, and most importantly, efforts such as these will help to ensure the safety and security of our citizens, our economy and our nation.

Thank you for your leadership on this issue. We look forward to our continued partnership. If you have any questions, please do not hesitate to contact our staff: Mary Catherine Ott (NGA/GHSAC) at mcott@NGA.org; 202.719.2667, Matt Pincus (NASCIO) at mpincus@NASCIO.org; and Susan Frederick (NCSL) at susan.frederick@ncsl.org.

Sincerely,

Nikki Guilford
Interim Executive Director
National Governors Association

Doug Robinson
Executive Director
National Association of State Chief
Information Officers

Tim Storey
Executive Director
National Association of State
Legislatures

Kevin Klein
Chairman
Governors Homeland Security Advisors
Council