A Compact to Improve State Cybersecurity

The foremost duty of every governor is to safeguard the public safety and welfare of its residents; that includes protecting citizens from cybersecurity threats. Cyber threats pose serious risks to the core interests of all states and territories. Recent cyber intrusions have stolen volumes of confidential data, exposed critical services to disruption and resulted in significant economic impacts to states.

States are attractive targets because they collect and store massive amounts of personal and financial data. They also own, control and regulate critical infrastructure. Yet all states struggle to defend agencies against cybersecurity threats. Some of the most sophisticated cyber hacking tools—once the sole purview of militaries and intelligence agencies—are now widely available to anyone with an Internet connection. States are on the front lines of cybersecurity, and adversaries will continue to target them.

Governors are focused on this threat. Most states and territories have awakened to these concerns, and governors across the nation are taking steps to enhance their resiliency. But cybersecurity policy is difficult. Solutions require vast coordination and deconfliction between state agencies, localities, tribal entities, federal partners, private companies and citizens, as well as the flexibility to rapidly change with emerging technologies.

Moreover, a state's cybersecurity interests extend far beyond defending public networks. Governors must prepare for significant consequences resulting from disruptions of critical infrastructure. They are responsible for identifying, pursuing and prosecuting cyber criminals. Businesses also depend on governors to be prepared for the consequences of cyberattacks, both virtual and physical. Yet, the underpinning to successful cybersecurity-policy is having a competent and plentiful workforce. Therefore, governors must lead the creation of school curricula that ensure individuals are getting the necessary skills to compete in an economy where cybersecurity is a core business concern.

In short, cybersecurity is a whole-of-state concern that requires high-level executive engagement.

With this compact, the undersigned commit to review and implement key recommendations to protect their residents from cybersecurity threats by:

Building cybersecurity governance, which may include:

- Creating a cybersecurity governance structure, whether through executive order, legislation or ad-hoc formation, and selecting members of the body based on their ability to implement change;

- Developing a statewide cybersecurity strategy that emphasizes protecting the state's IT networks, defending critical infrastructure, building the cybersecurity workforce and enhancing private partnerships; and

- Conducting a risk assessment to identify cyber vulnerabilities, cyber threats, potential consequences of cyberattacks and resources available to mitigate such threats and consequences.

Preparing and defending the state from cybersecurity events, which may include:

- Creating and exercising cybersecurity disruption response plans that emphasize a whole-of-state approach;

- Organizing a framework for information sharing by introducing state IT, homeland security and emergency management officials to managers of key critical infrastructure operators;

- Incorporating procedures for using the National Guard's cyber capabilities into cyber response plans and working with the legislative branch to expand the circumstances under which the Guard can be activated, if necessary; and

- Developing a public communications plan for cyber events.

Growing the nation's cybersecurity workforce, which may include:

- Reclassifying state job descriptions for cybersecurity positions to align with private sector practices;

- Encouraging colleges and universities to seek National Security Agency certification as a Center of Academic Excellence;

- Placing veterans into cybersecurity certification programs or open positions within state agencies;

- Partnering with community colleges to increase the availability of transferable, two-year cybersecurity degrees; and

- Creating a program to assign qualified college students to state agencies as low-cost, skilled cybersecurity interns.