State Governors Sign Cybersecurity Compact

07.27.2017

The National Governors Association (NGA), recently announced that 38 governors had signed “A Compact to Improve State Cybersecurity.” In announcing the Compact, Virginia Governor Terry McAuliffe, outgoing chair of the NGA, cited its three core principles:

- Building cybersecurity governance
- Preparing and defending the state from cybersecurity events
- Growing the nation’s cybersecurity workforce

The Compact highlights the attention that states are paying to cybersecurity and includes several key recommendations for each of the three principles. As is to be expected, many of these recommendations are primarily governmental in nature. For example, one recommendation is to reclassify state job descriptions for cybersecurity positions to align with private sector practices. Another is to develop a public communications plan for cyber events.

However, given the connectivity between IT networks, and the nature of cyberthreats, others will have a direct impact on businesses. For example, one of the recommendations is to develop “a statewide cybersecurity strategy that emphasizes protecting the state’s IT networks [and] defending critical infrastructure.” Such strategies will impact companies of all sizes and types that do business with state agencies. Moreover, many businesses are connected, directly and indirectly, to industries generally considered to be critical infrastructure, such as energy, communications, financial services and health care.

In the past, the federal government has taken the lead on cybersecurity requirements. However, as initiatives such as the Compact indicate, states are taking more of an active role in protecting their assets, infrastructure and citizens from cyber threats. As Governor McAuliffe stated: “[s]ince the launch of my initiative [as chair of NGA, to strengthen states’ cybersecurity efforts], more than 30 governors have signed an executive order, legislation or announced a cybersecurity initiative . . . [resulting] in a dozen executive orders, 14 signed bills and 17 initiatives.” As a result, it will become increasingly important for businesses to understand and comply with cybersecurity requirements at the state as well

as the federal level.

Related People

- Kevin D. Pomfret – 703.760.5204 – kpomfret@williamsmullen.com

Related Services

- Data Protection & Cybersecurity