Published on *The National Law Review* https://natlawreview.com

Governors of 38 States Join a Cybersecurity Compact

Article By:

Gregory Bautista

On July 16, 2016, the chair of the National Governors Association (NGA), Governor Terry McAuliffe (D-VA), unveiled his 2016?2017 initiative, Meet the Threat: States Confront the Cyber Challenge. Over the past year, the initiative has raised awareness of cybersecurity issues on a state level, held roundtables to address industry-specific cybersecurity issues, and held regional summits to bring together policy leaders and private-sector experts. The initiative also has published resources specifically tailored to assist and educate governors and state legislators, including memos comparing and contrasting states' cybersecurity governance bodies and cybersecurity centers; breakdowns of various state cybersecurity response plans; surveys of state cybersecurity budgets; and recommendations to address the cybersecurity of critical infrastructure ? including health care infrastructure, energy infrastructure, and election infrastructure ? the electric grid and public safety.

Since the launch of the initiative, "more than 30 governors have signed an executive order, legislation or announced a cybersecurity initiative," McAuliffe said. "This has resulted in a dozen executive orders, 14 signed bills and 17 initiatives."

On July 14, 2017, the initiative culminated with 38 governors signing A Compact to Improve State Cybersecurity. In a press release, McAuliffe stated that the NGA has "successfully engaged governors and their states on strengthening their cyber protocols and recognizing that cybersecurity is a technology issue, but it's also a health issue, an education issue, a public safety issue, an economic issue and a democracy issue."

With this compact, the 38 governors committed to review and move toward implementation of key recommendations "to protect their residents from cybersecurity threats" in three areas:

- First, the governors agreed to enhance state cybersecurity governance, including the creation of a cybersecurity governance structure through executive order or legislation, development of a statewide cybersecurity strategy, and implementation of a risk assessment to identify vulnerabilities and threats.

- Second, the governors agreed to prepare and defend their states from cybersecurity events through the creation of statewide response plans, organization of an information-sharing framework, incorporation of procedures for the use of the National Guard's cyber capabilities and the development of public communications plans.

- Third, the governors committed to growing the nation’s cybersecurity workforce, as the underpinning to successful cybersecurity policy is a competent and robust workforce. This includes partnering with colleges and universities to seek National Security Agency certification as Centers of Academic Excellence and to increase the availability of two-year cybersecurity degrees, creating an internship program for qualified college students to state agencies and placing veterans into cybersecurity certification programs or open positions within state agencies.

The commitment of 38 governors to the NGA’s cybersecurity goals demonstrates that states will continue to be a driving force in the evolution of U.S. data privacy and security laws and best practices, especially where the federal government has refrained from outlining a clear strategy at the state level. These changes to state governments and their cybersecurity practices will inevitably shape the industries related to critical infrastructure, which include the health care, energy, financial and telecommunications industries. Such businesses will need to navigate and comply with an increasing number of federal and state laws, standards and practices.

Businesses that work directly with state governments or otherwise rely on government contracts as a source of business should anticipate that any new cybersecurity initiatives may directly impact those contractual relationships. This could include, for example, imposition of greater corporate privacy policies and technical standards, legal liability for cybersecurity events, the requirement to maintain cyber liability insurance, and compliance with new and evolving consumer protection laws and regulations.

National Law Review, Volume VII, Number 227