By Administrator
Tuesday, 28 October 2014 05:00 -

RALEIGH, (SGRToday.com) - The National Governors Association is focusing on workforce issues in a new paper focusing on ways for states to preapre to inprove cybersecurity.

"The Cybersecurity Workforce: States' Needs and Opportunities" examines factors to consider when creating a comprehensive state strategy to improve cybersecurity.

Cyber threats arise from a large and increasing number of adversaries seeking to threaten communications networks and systems; databases containing sensitive and private information; financial, payment and tax systems; and other critical cyber infrastructure. The core of a state's ability to manage, prevent and mitigate damage from those attacks is a workforce whose job it is to ensure the integrity and ongoing operation of the systems upon which government services have come to rely.

"People are the keystone of cybersecurity," said Maryland Gov. Martin O'Malley, co-chair of the NGA Resource Center for State Cybersecurity (Resource Center) in a statement. "In Maryland, we've worked aggressively to develop our highly skilled cyber workforce -- this will help address both the state's and the nation's cybersecurity challenges, and will also foster growth in our innovative and job-creating cybersecurity business sector."

The most direct challenge governors face is making sure that their states' systems are cyber secure. Hiring new employees, training or retraining current employees and contracting out for cybersecurity services are three ways that states can meet their needs. States are well advised to have a core of employees with cybersecurity expertise who are capable of assessing the state's specific needs and making decisions about what aspects and how much of a state's cybersecurity will be provided by state employees and what aspects of it are more cost effective to contract out.

Under any strategy, the statement says, a state will need a cyber workforce with a wide array of skills. To ensure a robust workforce, governors should develop a strategic understanding of their state's cybersecurity risk profile, including current threat environment, and ensure that their existing workforce has the requisite skills to protect and defend state networks and critical infrastructure. In the longer-term, that could require aligning state education and workforce programs to support training of cybersecurity workers.

The report also recommends governors look at the National Guard.

At the governor's direction, the National Guard's cyber expertise could be used to coordinate, train, advise and assist state agencies in performing vulnerability assessments of information networks and systems. The National Guard also is well-positioned to support cyber incident response and recovery operations.

The report can be found at http://nga.org/cms/center/hsps.