SB 542

Department of Legislative Services

Maryland General Assembly
2015 Session

FISCAL AND POLICY NOTE

Senate Bill 542 (Senator Lee, *et al.*)
Finance

Maryland Cybersecurity Council - Establishment

This bill establishes the Maryland Cybersecurity Council, which is tasked with working with the National Institute of Standards and Technology (NIST), as well as other federal agencies, private-sector businesses, and private cybersecurity experts to meet specified goals related to cybersecurity in the State.

On or before July 1, 2016, the council must submit a report of its initial activities to the General Assembly, and beginning July 1, 2017, and every two years thereafter, the council must submit a report of its activities to the General Assembly.

The bill takes effect July 1, 2015.

Fiscal Summary

State Effect: Any expense reimbursements for task force members and staffing costs for the University of Maryland, University College (UMUC) are assumed to be minimal and absorbable within existing resources. Revenues are not affected.

Local Effect: The bill does not directly affect local governmental finances or operations.

Small Business Effect: None.

Analysis

Bill Summary:

Composition of the Maryland Cybersecurity Council

The 30-member council must consist of several Executive department secretaries and directors (or their designees), as well as representatives appointed by the Attorney General from businesses and companies around the State. In addition to the 30 required members of the council, the President of the Senate and the Speaker of the House of Delegates may each appoint two legislative members to serve on the council. Finally, the Attorney General must also invite specified directors and secretaries of federal security agencies to serve on the council. The council must be chaired by the Attorney General or the Attorney General's designee.

A member of the council may not receive compensation as a member of the council but is entitled to reimbursement for travel expenses. UMUC must provide staff for the council.

Maryland Cybersecurity Council Responsibilities

The Maryland Cybersecurity Council must work with NIST, as well as other federal agencies, private-sector businesses, and private cybersecurity experts to:

- for critical infrastructure not covered by federal law or Executive Order 13636, review and conduct risk assessments to determine which local infrastructure sectors are at the greatest risk of cyber attacks and need the most enhanced cybersecurity measures;

- use federal guidance to identify categories of critical infrastructure as critical cyber infrastructure if cyber damage or unauthorized cyber access to the infrastructure could result in catastrophic consequences;

- assist infrastructure entities that are not covered by the executive order in complying with federal cybersecurity guidelines;

- assist private-sector cybersecurity businesses in adopting, adapting, and implementing the NIST cybersecurity framework of standards and practices;

- examine inconsistencies between State and federal laws regarding cybersecurity;

- recommend a comprehensive State strategic plan to ensure a coordinated and adaptable response to and recovery from cybersecurity attacks; and

- recommend any legislative changes considered necessary by the council to address cybersecurity issues.

Current Law: The Secretary of Information Technology is responsible for developing a statewide information technology master plan (better known as ITMP) that:

- serves as the basis for the management and direction of information technology (IT) within the Executive Branch;
- includes all aspects of State IT, including telecommunications, data processing, and information management;
- considers interstate transfers as a result of federal legislation and regulation;
- works jointly with the Secretary of Budget and Management to ensure that IT plans and budgets are consistent; and
- ensures that State IT plans, policies, and standards are consistent with State goals, objectives, and resources, and represent a long-range vision for using IT to improve the overall effectiveness of State government.

State agencies may not purchase, lease, or rent IT unless it is consistent with the master plan.

Background: In February 2013, President Obama's Executive Order 13636 directed the Secretary of Commerce to enlist NIST in developing a "framework to reduce cyber risks to critical infrastructure." The framework was to include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address the risk of cyber attacks.

In February 2014, NIST released its official first version of the framework, as well as a companion roadmap that discussed next steps and identified key areas of cybersecurity development, alignment, and collaboration. NIST advises that the framework was created through collaboration between industry and government, and it consists of standards, guidelines, and practices to promote the protection of critical infrastructure. In February 2015, in its most recent update regarding the framework, NIST discussed (1) the feedback it has received regarding the framework, including methods to improve specific aspects of the framework and (2) its next planned steps, including partnering with other organizations to raise awareness of cybersecurity issues and the framework.

Additional Information

Prior Introductions: None.

Cross File: None.

Information Source(s): Office of the Attorney General (Consumer Protection Division), University System of Maryland, National Institute of Standards and Technology, Department of Legislative Services

Fiscal Note History: First Reader - March 13, 2015
md/mcr

Analysis by: Richard L. Duncan

Direct Inquiries to:
(410) 946-5510
(301) 970-5510