Department of Legislative Services

Maryland General Assembly
2015 Session

FISCAL AND POLICY NOTE

Senate Bill 544 (Senator Lee, *et al.*)
Finance Economic Matters

Statewide Information Technology Master Plan - Inclusion of Cybersecurity Framework - Requirement

This bill requires that the statewide information technology (IT) master plan include a cybersecurity framework. In developing the framework, the Secretary of Information Technology must consider materials developed by the National Institute of Standards and Technology (NIST).

Fiscal Summary

State Effect: The addition of a cybersecurity framework to the annual statewide IT master plan can likely be performed by the Department of Information Technology with existing budgeted resources by dedicating an existing staff member to the necessary activities. Implementation by State agencies of the cybersecurity framework required by the bill may involve expenditure for additional resources related to IT infrastructure and personnel, but any such impact cannot be assessed at this time.

Local Effect: None.

Small Business Effect: None.

Analysis

Current Law: The Secretary of Information Technology is responsible for developing a statewide IT master plan that:

- serves as the basis for the management and direction of 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: SB 197 of 2014 passed the Senate but received an unfavorable report from the House Economic Matters Committee. Its cross file, HB 804, also received an unfavorable report from the House Economic Matters Committee.

Cross File: None.

Information Source(s): Department of Budget and Management, Department of Information Technology, National Institute of Standards and Technology, Department of Legislative Services

Fiscal Note History: First Reader - March 13, 2015
mar/ljm

Analysis by: Michael C. Rubenstein

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