SB 286

Department of Legislative Services

Maryland General Assembly
2017 Session

FISCAL AND POLICY NOTE
First Reader

Senate Bill 286 (Senator Lee)
Finance

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

This bill requires the statewide information technology (IT) master plan to 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 likely necessitates expenditures for additional resources related to IT infrastructure and personnel, but any such impact cannot be assessed at this time. Revenues are not affected.

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 U.S. 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 October 2015, NIST provided an update regarding the framework, discussing (1) its continued efforts to accept feedback and improve specific aspects of the framework and (2) the Critical Infrastructure Cyber Community Voluntary Program that helps organizations address and improve their cybersecurity risk management. In its most recent update in January 2017, NIST released a draft of the framework with proposed changes to address issues and concerns brought up in a cybersecurity workshop it hosted in 2016.

Additional Information

Prior Introductions: SB 412 of 2016 received an unfavorable report from the Senate Finance Committee. SB 544 of 2015 passed the Senate but received an unfavorable report from the House Economic Matters Committee. 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 Information Technology; National Institute of Standards and Technology; Department of Legislative Services

Fiscal Note History: First Reader - February 3, 2017
fn/mcr

Analysis by: Richard L. Duncan

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