HB 804

Department of Legislative Services

Maryland General Assembly
2014 Session

FISCAL AND POLICY NOTE

House Bill 804 (Delegate Lee, *et al.*)
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 State IT master plan can be performed by the Department of Information Technology with existing budgeted resources. Implementation by State agencies of the cybersecurity framework required by the bill may involve expenditure of additional resources for 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. NIST released an exposure draft of the framework in October 2013 and invited public comments on the draft during a 45-day comment period. It is currently in the process of reviewing those comments and assessing the need for adjustments to the framework.

Additional Information

Prior Introductions: None.

Cross File: SB 197 (Senator Pugh, *et al.*) - Finance.

Information Source(s): Board of Public Works, Department of Information Technology, Department of Legislative Services

Fiscal Note History: First Reader - February 6, 2014
ncs/ljm

Analysis by: Michael C. Rubenstein

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