Department of Legislative Services
Maryland General Assembly
2013 Session

FISCAL AND POLICY NOTE

House Bill 1276   (Delegate Hough, *et al.*)

Health and Government Operations

Statewide Information Technology Master Plan - Security Policy

---

This bill requires that the statewide information technology master plan (ITMP) include a policy that requires a vendor selling an information technology (IT) product or piece of equipment to the State to establish that it is safe from embedded security threats. It also requires the plan to develop steps that establish that products or pieces of equipment are safe from embedded security threats.

Fiscal Summary

State Effect: Although the Department of Information Technology (DoIT) can make the necessary changes to the ITMP with existing resources, it is not feasible to achieve the bill's goal of ensuring that all IT products purchased and used by the State are free from embedded security threats. Any attempt to do so is cost-prohibitive.

Local Effect: None.

Small Business Effect: Meaningful for small businesses that sell IT products to the State. They have to certify that all products are free from embedded security threats, which is not feasible.

Analysis

Current Law/Background: The Secretary of Information Technology must develop a statewide ITMP. With some exceptions, primarily for public institutions of higher education, each unit of State government must develop and submit an information technology plan and annual project plans to the Secretary. Information technology

developed, purchased, and used by State agencies must be consistent with the statewide ITMP.

The fiscal 2014 ITMP reaffirms "three perpetual objectives of consolidation, interoperability, and standardization."

State Fiscal Effect: DoIT and the Office of Information Systems within the Department of Legislative Services advise that the bill's objectives cannot be met because both the cost and technical aspects of ensuring that a device is free from embedded security threats are prohibitive. Indeed, DoIT advises that it is impossible to "completely mitigate the risk of embedded security risks in products received and implemented in the State." Any effort to do so, it advises, would likely double the cost of technology products purchased by the State and require a level of staffing expertise that is not currently available in State government. The State currently spends at least $102 million annually to purchase IT hardware and software. Enforcement of such a requirement would also require regular inspections and/or an ongoing State presence in manufacturing plants that produce IT equipment and products sold to the State.

Additional Information

Prior Introductions: None.

Cross File: None.

Information Source(s): Department of Information Technology, Department of General Services, Maryland Department of Transportation, University System of Maryland, Department of Legislative Services

Fiscal Note History: First Reader - March 4, 2013
mm/rhh

Analysis by: Michael C. Rubenstein

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