SB 882

Department of Legislative Services

Maryland General Assembly
2018 Session

FISCAL AND POLICY NOTE
First Reader

Senate Bill 882 (Senator Lee)
Education, Health, and Environmental Affairs

Procurement - Telecommunication and Computer Network Access - Security Requirements

This bill prohibits a State agency, subject to a waiver process, from procuring services from an Internet service provider (ISP) that blocks specified content, impairs or degrades lawful Internet traffic in specified ways, or engages in commercial traffic preferencing, as specified by the bill. It also requires vendors of Internet-connected devices to submit, prior to being awarded a State contract, either (1) a written certification that the device does not have specified security vulnerabilities or defects and that it satisfies other security-related requirements or (2) an application for a waiver of that certification requirement. The Department of Information Technology (DoIT) must develop regulations to implement these provisions of the bill.

Fiscal Summary

State Effect: General fund expenditures increase by $119,300 to implement the security-related provisions for Internet-connected devices. Out-year costs reflect annualization, salary increases, and the termination of a contractual position. The Board of Public Works (BPW) and other agencies can implement the provisions related to procurement of ISPs with existing budgeted resources. No effect on revenues.

(in dollars)	FY 2019	FY 2020	FY 2021	FY 2022	FY 2023
Revenues	$0	$0	$0	$0	$0
GF Expenditure	119,300	75,200	77,400	80,200	83,100
Net Effect	($119,300)	($75,200)	($77,400)	($80,200)	($83,100)

Note:() = decrease; GF = general funds; FF = federal funds; SF = special funds; - = indeterminate increase; (-) = indeterminate decrease

Local Effect: None.

Small Business Effect: Potential meaningful.

Analysis

Bill Summary:

Internet Service Providers

The bill defines "reasonable network management" to mean a practice that primarily is used for and tailored to achieving a legitimate network management purpose, taking into account the particular network architecture and technology of the broadband Internet access service. It does not include other business practices.

A State agency may not procure services from an ISP that:

- blocks lawful content, applications, services, or nonharmful devices, subject to reasonable network management;
- impairs or degrades lawful Internet traffic on the basis of Internet content, application, or service, or use of a nonharmful device, subject to reasonable network management; or
- engages in commercial traffic preferencing, including specified actions, either in exchange for consideration from a third party or to benefit an affiliated entity.

BPW may establish a waiver process that includes a public hearing before the board and requires a majority vote of the members of the board. By November 1 of each year, BPW must report to the General Assembly on all waivers issued under the process.

Internet-connected Devices

An "Internet-connected device" is a physical object that is capable of connecting to and is in regular connection with the Internet and has computer processing capabilities that can collect, send, or receive data.

Before a State agency can award a procurement contract for an Internet-connected device, the vendor must submit a written certification that the device:

- does not contain, at the time that the bid or proposal is submitted, a hardware, software, or firmware component with a known security vulnerability or defect listed in the National Vulnerability Database of the National Institute of Standards and Technology (NIST) or any additional database selected by the Secretary of Information Technology;
- relies on software or firmware components capable of accepting properly authenticated and trusted updates from the bidder or offeror;

- uses only nondeprecated industry-standard protocols and technologies for functions; and
- does not include any fixed or hard-coded credentials used for remote administration, the delivery of updates, or communication.

Alternatively, the bidder or offeror may submit a written application for a waiver from the certification requirements for the purpose of disclosing a known vulnerability. The waiver application must identify the vulnerability and mitigating actions that may limit or eliminate the vulnerability, and it must include a justification for secure use of the device in spite of the vulnerability.

The bill specifies additional clauses that must be included in State contracts for Internet-connected devices, generally relating to the disclosure of defects and procedures for updating and replacing the devices.

If a State agency reasonably determines that procurement of an Internet-connected device that meets the certification requirements is not feasible or economically practical, the agency may petition DoIT for a waiver to purchase a noncompliant device. The petition must include specified documentation. If a waiver petition is granted, the head of the agency must sign a statement that the agency accepts the risks associated with use of the device. Also, if an agency uses a third-party security standard that is at least as strict as the one required by the bill, it can require vendors to meet that standard.

DoIT must adopt regulations that define a set of conditions under which agencies can use Internet-connected devices that do not comply with the security requirements, and it may adopt additional regulations for the management and use of noncompliant devices, as specified by the bill. The bill should not be construed to establish additional obligations or criminal penalties for individuals engaged in researching the cybersecurity of Internet-connected devices.

Current Law: The Secretary of Information Technology is responsible for, among other statutory duties:

- developing, maintaining, revising, and enforcing information technology (IT) policies, procedures, and standards;
- providing technical assistance, advice, and recommendations to the Governor and any unit of State government concerning IT matters; and
- reviewing the annual project plan for each unit of State government to make information and services available to the public over the Internet.

DoIT is also designated as the agency that controls State procurement of (1) information processing equipment and associated services and (2) telecommunications equipment, systems, or services. However, its control agency status terminates in October 2019.

Background:

Net Neutrality

In December 2017, the Federal Communications Commission (FCC) approved a repeal of existing "net neutrality" regulations that had been in place for two years and that barred ISPs from restricting Internet traffic on their services. The FCC also reclassified broadband Internet service as an "information service" rather than a "telecommunications service," thereby limiting the FCC's authority to regulate broadband service in the future. The order included a preemption clause that prevents states from adopting their own net neutrality rules, although some states dispute whether the preemption clause is valid. The repeal is scheduled to take effect April 23, 2018.

With the repeal of the net neutrality rules, ISPs can slow down or block access to some websites. They can also accept fees from companies to make their content load faster than other sites.

According to *Consumer Reports*, 26 states have introduced legislation to mitigate the effects of the repeal of net neutrality, and several governors have signed executive orders to enact their own net neutrality rules. As of February 28, 2018, Washington is the only state to successfully pass net neutrality legislation, which is awaiting the Governor's signature. The executive orders that have been signed in several states generally use the power of state contracting to require or pressure ISPs to abide by the principles of net neutrality in the respective states. In addition, the Attorneys General of 22 states (including Maryland) have filed a lawsuit seeking to block the FCC's order. That lawsuit is currently pending.

Security of Internet-connected Devices

NIST's National Vulnerability Database is a federal repository of standards-based vulnerability management data. It includes databases of security checklist references, security-related software flaws, misconfigurations, and more; and allows for the automation of vulnerability management for IT devices and software.

State Expenditures: Under the bill, DoIT is charged with:

- developing regulations to implement the security-related provisions of the bill;

- monitoring agency and vendor compliance with the security vulnerability provisions related to Internet-connected devices;
- developing and administering waiver and petition processes for those provisions; and
- assessing whether third-party security standards used by agencies are at least as rigorous as those required by the bill.

The development of regulations is a one-time occurrence, but the remaining tasks are ongoing and require additional staff to carry out. Therefore, general fund expenditures increase by $119,321 in fiscal 2019, which accounts for the bill's October 1, 2018 effective date. This estimate reflects the cost of hiring a procurement officer and a contractual assistant Attorney General to administer the bill's security-related procurement provisions and to promulgate regulations. It includes salaries, fringe benefits, one-time start-up costs, and ongoing operating expenses. The contractual position ends after nine months.

Regular Position	1
Contractual Position	0.75
Salary and Fringe Benefits	$108,603
Operating Expenses	10,718
Total FY 2019 State Expenditures	**$119,321**

Future year expenditures reflect a full salary with annual increases and employee turnover, the termination of the contractual position, and ongoing operating expenses.

This estimate does not include any health insurance costs that could be incurred for specified contractual employees under the State's implementation of the federal Patient Protection and Affordable Care Act.

The net neutrality-related provisions have no material effect on State operations or finances. BPW can implement the waiver process with existing budgeted resources.

Small Business Effect: IT companies, many of which are small businesses, will have to comply with all of the security-related provisions if they provide Internet-connected devices (including personal computers, smart phones, and much more) to the State. Complying with all the provisions, including possibly writing and submitting waiver requests, may pose an administrative burden on small businesses.

Additional Information

Prior Introductions: None.

Cross File: None.

Information Source(s): Department of Information Technology; Department of General Services; Board of Public Works; FastCompany.com; *Federal Register*; New York Attorney General's Office; *Consumer Reports*; Department of Legislative Services

Fiscal Note History: First Reader - March 1, 2018
mag/ljm

Analysis by: Michael C. Rubenstein

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