Department of Legislative Services

Maryland General Assembly
2019 Session

FISCAL AND POLICY NOTE
First Reader

Senate Bill 553 (Senator Lee, *et al.*)
Finance and Education, Health, and Environmental Affairs

Security Feature for Connected Devices - Requirements, Procurement Preferences, and Reports

This bill establishes a regulatory framework for the manufacture and procurement of secure connected devices in the State. Among other things, the bill defines "secure connected device," prohibits the manufacturing of insecure connected devices, and generally requires each public body to require a contractor or subcontractor to use a secure connected device in the performance of a contract. **The bill takes effect January 1, 2020.**

Fiscal Summary

State Effect: State expenditures (all funds) increase beginning in FY 2020, potentially significantly, to the extent the bill results in additional contractor costs to ensure the use of secure connected devices. Otherwise, the bill's requirements can likely be handled using existing resources, assuming enforcement is complaint based. If the bill's intent is for proactive enforcement, general fund expenditures increase significantly, as discussed below. Potential minimal increase in general fund revenues due to the bill's penalty provisions.

Local Effect: Local expenditures increase beginning in FY 2020, potentially significantly, to the extent the bill results in additional contractor costs to ensure the use of secure connected devices. Revenues are not affected.

Small Business Effect: Potential meaningful.

Analysis

Bill Summary:

Definitions

"Connected device" means a physical object that is capable of connecting to the Internet, directly or indirectly, and assigned an Internet Protocol address or Bluetooth address. "Security feature" means an attribute of hardware, firmware, software, process, procedure, or combination of those factors that could prevent or lessen the failure or compromise of the confidentiality, integrity, or accessibility of a connected device or its stored information. "Insecure connected device" means a connected device that does not have the security features defined by the bill. "Secure connected device" means a connected device that is not an insecure connected device.

"Manufacturer" means a person who manufactures or assembles a new connected device for sale or distribution or contracts with another person to do so on that person's behalf. "Authentication" means a method of verifying the authority of a user, process, or connected device to access resources through an information system. "Unauthorized access" means any use, modification, disclosure, or destruction of any information stored within a connected device that is not authorized by the device's owner.

Security Features Required for Connected Devices

A manufacturer of a connected device must equip the device with a reasonable security feature that is:

- appropriate to the nature and function of the connected device;
- appropriate to the information the connected device collects, contains, or transmits; and
- designed to protect the connected device from unauthorized access, destruction, or modification.

A connected device is considered to have a reasonable security feature if it meets these requirements and is equipped with a means for authentication outside of a local area network that includes either (1) a preprogrammed password that is unique to each connected device or (2) a process that requires the user to generate a new means of authentication before the user is granted access for the first time.

The Attorney General may seek relief against a manufacturer that violates this requirement. For each connected device that does not have a reasonable security feature, the

manufacturer is subject to a separate civil penalty of $1,000; however, the manufacturer may not be fined more than $100,000 for violations arising from a single model of a connected device. The bill does not create or authorize a private right of action.

Reporting of Violations

The Department of Labor, Licensing, and Regulation (DLLR) must send a report of any violation of the bill's security feature requirement to the Maryland Cybersecurity Council. The report must include the name of the manufacturer responsible and the nature of the violation. The duties of the Maryland Cybersecurity Council are expanded to include taking these reports into account when performing its other duties.

DLLR must also report the make and model of the connected device to the Secretary of General Services. The Department of General Services (DGS) must then report the make and model of the device to specified units of State government that procure supplies under State procurement law.

Secure Connected Devices Required for Contractors

Each public body (which includes a unit of State government, a county, a municipality, a school district, and a special district) must require a contractor or subcontractor to use a secure connected device in the performance of a contract unless the head of the public body determines that:

- the price of a secure connected device exceeds the price of a similar insecure connected device by an unreasonable amount;
- a secure connected device is not available for purchase in reasonable quantities;
- the quality of a secure connected device is substantially less than the quality of a comparably priced, similar, and available insecure connected device; or
- the procurement of a secure connected device would be inconsistent with the public interest.

Limitations

The bill may not be construed to impose any duty on (1) a manufacturer of a connected device for an unauthorized access that arises from an unaffiliated third-party software or application that a user adds to a connected device; (2) a manufacturer to prevent a user from having full control over a connected device, including by allowing a user to modify the software or firmware running on the connected device; or (3) the operator of an electronic store, an electronic marketplace, or any other means of purchasing or downloading software or applications to enforce compliance with the bill.

Current Law/Background:

Department of Labor, Licensing, and Regulation

DLLR includes many of the State's agencies and boards responsible for licensing and regulating various businesses, professions, and trades. DLLR also administers a variety of federally funded employment service programs.

Procurement – Generally

Division II of the State Finance and Procurement Article and Title 21 of the Code of Maryland Regulations (COMAR) together provide the framework for procurement in Maryland. Statute authorizes the Board of Public Works (BPW), a constitutional entity consisting of the Governor, Treasurer, and Comptroller, to control procurement by State agencies by setting policy, adopting regulations, and establishing internal operational procedures. At the same time, however, statute authorizes BPW to delegate any of its procurement authority that it determines to be appropriate for delegation and requires BPW approval for specified procurement actions.

For specified services and product types, statute expressly authorizes other units of State government to establish standards and controls over the procurement process. For example, the Department of Information Technology is authorized to control the procurement of (1) information processing equipment and associated services and (2) telecommunication equipment, systems, or services.

Maryland Cybersecurity Council

Chapter 358 of 2015 established the Maryland Cybersecurity Council. The council is required to work with the National Institute of Standards and Technology (NIST), as well as other federal agencies, private-sector businesses, and private cybersecurity experts to address State issues. The council's responsibilities include (1) examining inconsistencies between State and federal cybersecurity laws; (2) assisting private-sector cybersecurity businesses in adopting, adapting, and implementing the NIST cybersecurity framework of standards and practices; and (3) recommending legislative changes to address cybersecurity issues.

The council consists of several Executive Department secretaries and directors (or their designees), as well as representatives appointed by the Attorney General from businesses and companies around the State. The council must be chaired by the Attorney General or the Attorney General's designee.

Office of the Attorney General

The Consumer Protection Division of the Office of the Attorney General is responsible for enforcing the Maryland Consumer Protection Act (MCPA) and investigating the complaints of aggrieved consumers. The division may attempt to conciliate the matter, issue a cease and desist order, or file a civil action in court. A merchant who violates MCPA is subject to a fine of up to $10,000 for each violation and up to $25,000 for each repetition of the same violation. In addition to any civil penalties that may be imposed, any person who violates MCPA is guilty of a misdemeanor and, on conviction, is subject to a fine of up to $1,000 and/or imprisonment for up to one year.

State Fiscal Effect:

Procurement Costs

State procurement costs (all funds) increase substantially to the extent that contractors must upgrade their technology to meet the bill's requirements and pass those costs on to the State. Even so, any such impact depends on numerous unknown factors, including the current standing of technology used by contractors that work with the State and, therefore, cannot be reliably estimated at this time.

Department of Labor, Licensing, and Regulation and Office of the Attorney General

Although the bill establishes a general prohibition against the manufacturing of insecure connected devices, it does not establish an enforcement or review mechanism for DLLR to make any determination on whether a device is secure or insecure. Furthermore, DLLR is not directly involved in, and has no experience with, the regulation of information technology (IT) or Internet-based devices or services. Therefore, DLLR advises that it plans to implement the bill's requirements using complaint-based enforcement in cooperation with the Office of the Attorney General (OAG). As it receives complaints, DLLR is only required to submit the information to the Maryland Cybersecurity Council and DGS, as appropriate, and can do so using existing budgeted resources. Under these circumstances, DGS and OAG can also likely handle the bill's requirements using existing resources, and general fund revenues may increase minimally due to the bill's penalty provisions.

To the extent that the intent of the bill is for DLLR and OAG to take a more proactive role in enforcement and to regularly examine and study connected devices in the State to ensure that they meet the bill's security requirements, general fund expenditures increase significantly beginning in fiscal 2020. Under these circumstances, DLLR would be required to establish a new division staffed with experts in IT and device security, and costs could easily exceed $300,000 annually to do so. Similarly, OAG may experience increased

costs from filing claims against manufacturers who produce insecure devices; the increase in litigation may also lead to significant general fund revenues as violators pay the penalty fines established by the bill.

Local Expenditures: Similar to the effect on State procurement costs, local government procurement costs increase substantially to the extent that contractors must upgrade their technology to meet the bill's requirements and pass those costs on to local governments.

Small Business Effect: Contractors for State and local government entities, many of which are small businesses, have to comply with the security requirements established by the bill for connected devices. Complying with these requirements could require a small business to replace and/or upgrade its technology in order to maintain a contract, and costs to do so could be significant.

Additional Information

Prior Introductions: None.

Cross File: HB 1276 (Delegate Carey) - Economic Matters and Health and Government Operations.

Information Source(s): Department of Information Technology; Maryland Association of Counties; Maryland Municipal League; Office of the Attorney General; Department of General Services; Department of Labor, Licensing, and Regulation; Department of Legislative Services

Fiscal Note History: First Reader - February 24, 2019
mm/mcr

Analysis by: Richard L. Duncan

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