HB 1306

Department of Legislative Services

Maryland General Assembly
2014 Session

FISCAL AND POLICY NOTE

House Bill 1306 (Delegates Szeliga and Hough)
Health and Government Operations

State Government - Functionality and Security of Web Sites - Certification

This bill specifies that, if a website elicits, collects, or stores personally identifiable information (PII) and is accessible to the public, a governmental unit may not make the website available to the public unless specified conditions, including certification from a third-party private entity, are met. An exception is made for specified websites designed for testing and development purposes. If a website was made available to the public before October 1, 2014, the governmental unit must obtain a third-party certification before November 1, 2014. If the governmental unit does not obtain the required certification, the governmental unit must notify and work with the Secretary of Information Technology to make any changes necessary.

Fiscal Summary

State Effect: State expenditures (all funds) increase by *at least* $13.3 million in FY 2015 and by *at least* $3.0 million annually thereafter. Of that amount, $12.5 million in FY 2015 and $2.5 million annually thereafter reflects the cost of certification for websites as required by the bill. Remaining expenditures, approximately $848,200 in FY 2015, reflect full-time regular and contractual staff necessary for the Department of Information Technology (DoIT) to implement the bill. Out-year expenditures reflect annualization, inflation, and the termination of one-time costs and contractual positions. This estimate does not reflect any additional positions that may be required by other governmental units or expenditures related to required background checks for specified employees, both of which could be significant. Revenues are not affected.

($ in millions)	FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Revenues	$0	$0	$0	$0	$0
GF Expenditure	.8	.5	.3	.3	.3
GF/SF/FF Exp.	12.5	2.5	2.5	2.5	2.5
Net Effect	($13.3)	($3.0)	($2.8)	($2.8)	($2.8)

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

Local Effect: The bill does not directly affect local governmental operations or finances.

Small Business Effect: Potential meaningful. Some private small business entities in the State may meet the bill's requirements to perform security certifications on State websites.

Analysis

Bill Summary: The bill defines "fully functional" as a website that can fully support the activities for which it is designed or intended with regard to the elicitation, collection, or storage of PII, including handling the volume of queries expected. The bill defines "governmental unit" as an instrumentality of the State. The bill defines "PII" as information that can be associated with one individual through a Social Security number, a taxpayer identification number, a State identification number, or any other identifier; it does not include information necessary to contact an individual.

If a website elicits, collects, or stores PII and is accessible to the public, with exception for specified websites designed for testing and development purposes, a governmental unit may not make the website available to the public unless:

- the Secretary of Information Technology has been notified of the governmental unit's intent to make a website available to the public;
- an appropriate third-party private entity has evaluated the website and certified that it is fully functional and secure; and
- the certification has been submitted to the Secretary.

If a website was made available to the public before October 1, 2014, the governmental unit must obtain a third-party certification before November 1, 2014. If the governmental entity is unable to obtain the third-party certification required before November 1, 2014, the governmental unit must notify the Secretary. The Secretary must then work with the governmental unit to ensure that any issues preventing the website from being certified are addressed and any necessary changes to the website are made.

A website may not be certified as secure unless the website (1) has security features that meet a standard acceptable for banking purposes and (2) ensures that PII elicited, collected, or stored in connection with the website is captured at the latest possible step in a user input sequence. A website may also not be certified as secure unless the governmental unit:

- has named an overall security leader who has a comprehensive view of the security posture for the website and who has supervised a complete end-to-end security test;
- has taken reasonable efforts to minimize domain name confusion, including registering additional domain names and instituting a program to educate consumers on how to spot fraudulent websites;
- requires all personnel who have access to PII in connection with the website to undergo a background check and sign a nondisclosure agreement with respect to PII;
- takes proper precautions to ensure that only trustworthy persons can access PII; and
- maintains ample personnel to respond in a timely manner to issues relating to the proper function and security of the website and to monitor on an ongoing basis existing and emerging security threats to the website.

Current Law: DoIT provides information technology leadership to the Executive Branch agencies and commissions of State government so that key State information technology resources may be effectively managed. This leadership encompasses the establishment and management of technology standards, ensuring efficient procurement of information technology services and products, fostering cross agency collaboration for the mutual benefit of all agencies, and serving as an industry liaison. It is also the mission of DoIT to identify and promulgate opportunities for State agencies to become more efficient, reduce costs, and better serve the citizens of Maryland. The Governor's proposed fiscal 2015 operating budget includes $102.8 million for DoIT.

Chapter 452 of 2010 established that, after June 1, 2010, a department or an independent unit in the State, to the extent practical, may not publicly post or display an individual's personal information on a website maintained or paid for by the department or independent unit. Additionally, a person whose personal information is contained in a public record or report may request that the information be masked on the Internet version of the public record. An official custodian must then mask the public record within 30 days of the request and give the requestor a written notice of the action taken.

Background: In recent years, technological advancements to networks, electronic devices, and other forms of information technology have expanded and improved communications, travel, and data analysis. The U.S. Department of Homeland Security reports that cyber intrusions and attacks have also increased dramatically over the last decade, exposing sensitive personal and business information, disrupting critical operations, and imposing steep economic costs. Recognizing the importance of network and cyber security, in 2011, the U.S. Department of Defense named cyberspace as a new domain of warfare.

Cyber intrusions and attacks are a common occurrence in the United States for both the private- and public-sector entities. In December 2013, retailer Target revealed that its systems were hacked into and customer information was stolen from the servers. This included names, mailing addresses, email addresses, and financial information. In February 2014, the University of Maryland, College Park database system was breached and student, faculty, and staff information related to name, Social Security number, and date of birth was accessed.

Many State entities operate websites and servers that collect and contain PII. For example, the University of Maryland, College Park system contains data on more than 300,000 faculty, staff, and students; the State Ethics Commission collects and keeps personal information related to State officials' financial disclosures; the Department of Labor, Licensing, and Regulation collects and stores personal information related to business licensing; the Department of Natural Resources collects financial information through its website to allow reservations for campsites and park facilities; and the Maryland Health Benefit Exchange collects PII to allow Maryland residents to obtain health care online.

The bill is modeled after the Safe and Secure Federal Websites Act of 2013, which prohibits federal agencies from deploying websites until specified certifications are met relating to the functionality and security of the website.

State Expenditures: Expenditures (all funds) increase significantly in all years as a result of various provisions in the bill, as discussed below.

Certification Requirements for Governmental Unit Websites

DoIT estimates that at least 50 websites run by governmental units deal with PII in the manner specified by the bill and likely require certification before November 1, 2014. Due to the frequency with which many websites are updated or changed, DoIT also estimates that there will need to be approximately 10 additional certifications per year in future years across State agencies. DoIT notes that this is a conservative estimate, and it is possible that more websites that will require certification are currently in existence and more websites may require certification in future years.

DoIT reports that the certification process costs approximately $250,000 for each website, and as such, expenditures (all funds) increase by at least $12.5 million in fiscal 2015 and at least $2.5 million per year in future years to certify the websites. If there are more websites that require certification, expenditures increase accordingly.

Required Staff for DoIT

To meet the bill's extensive responsibilities and requirements for DoIT, the agency needs at least three additional full-time regular staff who specialize in cyber security, as well as additional contractual web programmers, systems analysts, and security subject matter experts, all of whom will manage and assist governmental units with website security needs. Contractual staff are only needed in fiscal 2015 and part of fiscal 2016 to assist DoIT in ensuring all existing websites meet the bills requirements. The scope of work, which requires DoIT to verify the security of existing and new websites and to assist governmental units in ensuring websites are fully secure and operational, requires oversight functions and validation of governmental entity systems once PII is collected. As such, DoIT general fund expenditures increase by $848,298 in fiscal 2015, which accounts for the October 1, 2014 effective date of the bill, to hire the required staff. Future year expenditures reflect inflation, employee turnover, annualization, and the elimination of one-time costs and contractual positions.

Regular Positions	3
Contractual Positions	7
Salaries and Fringe Benefits	$800,248
Start-up Costs	43,700
Ongoing Operating Expenses	4,350
Total FY 2015 State Expenditures	**$848,298**

Required Website Security Leader

Many governmental units in the State do not have information technology personnel on staff and may need additional staff to meet the bill's requirements that each governmental unit name an overall security leader with specified knowledge and responsibilities before the unit's websites may be certified as secure. The exact number of governmental units that need to hire an additional person for this position, as well as any related expenditure increase, cannot be reliably estimated at this time.

Required Background Checks for Employees

Because the bill does not specify the type or extent of the background check required for employees who have access to PII in connection with a website, and it is unclear how many employees will require the background checks, any related expenditures cannot be reliably estimated at this time.

Additional Information

Prior Introductions: None.

Cross File: None.

Information Source(s): Department of Business and Economic Development; Department of Budget and Management; Department of Human Resources; Department of Natural Resources; Department of Information Technology; Maryland State Department of Education; Maryland Department of the Environment; State Ethics Commission; Department of Housing and Community Development; Maryland Higher Education Commission; Department of Health and Mental Hygiene; Maryland Insurance Administration; Judiciary (Administrative Office of the Courts); Department of Juvenile Services; Department of Labor, Licensing, and Regulation; Department of State Police; Maryland Department of Transportation; University System of Maryland; U.S. Department of Defense; U.S. Department of Homeland Security; Department of Legislative Services

Fiscal Note History: First Reader - March 11, 2014
ncs/mcr

Analysis by: Richard L. Duncan

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