Department of Legislative Services

Maryland General Assembly
2013 Session

FISCAL AND POLICY NOTE
Revised

Senate Bill 676 (Senator Pugh)(Commission on Maryland Cybersecurity Innovation and Excellence)

Education, Health, and Environmental Affairs Health and Government Operations

Governmental Procedures - Security and Protection of Information

Thi s bill establishes, for units of and local State government (not including legislative or judicial agencies), specified requirements with regard to the protection of an individual's private information from unauthorized access.

The bill takes effect July 1, 2014.

Fiscal Summary

State Effect: Potential significant increase in State expenditures (all funds) for units of State government that are not already in compliance with the bill's security and notice requirements.

Local Effect: Potential significant increase in local government expenditures for units of local government to comply with the bill's security and notice requirements. **This bill imposes a mandate on a unit of local government.**

Small Business Effect: Minimal.

Analysis

Bill Summary: The bill does not apply to personal information that (1) is publicly available information that is lawfully made available to the general public from federal, State, or local government records; (2) an individual has consented to have publicly disseminated or listed; or (3) with specified exceptions, records disclosed in accordance with specified provisions of federal law.

A unit of State or local government that collects an individual's personal information must – to protect personal information from unauthorized access, use, modification, or disclosure – implement and maintain reasonable security procedures and practices appropriate to the nature of the information collected and the nature of the unit and its operations. Similarly, a unit that uses a nonaffiliated third party as a service provider (and discloses personal information about an individual) must require that the third party implement and maintain reasonable security procedures and practices, as specified by the bill.

If a government unit that collects computerized data that containing an individual's personal information discovers (or is notified of) a breach of the security system, the unit must conduct, in good faith, a reasonable and prompt investigation to determine whether the unauthorized acquisition of personal information has resulted in (or is likely to result in) the misuse of the information – in which case the unit (or the nonaffiliated third party, if authorized under a written contract or agreement) generally must notify the individual of the breach, as specified by the bill. The bill also requires a unit to provide notice of a breach of security to the Office of the Attorney General (OAG), the Department of Information Technology (DoIT), and consumer reporting agencies under specified conditions.

Similarly, a nonaffiliated third party that maintains computerized data containing personal information provided by a unit generally must notify the unit, as specified by the bill, of a breach of the security of a system if the unauthorized acquisition of the individual's personal information has occurred or is likely to occur.

Notice to an individual must include specified information and may be given by written notice, telephonic notice, or (under specified circumstances) electronic mail. Substitute notice may be given if the unit demonstrates that the cost of providing notice would exceed $100,000 or that the affected class of individuals to be notified exceeds 175,000 (or if the unit does not have sufficient contact information to give regular notice).

A unit of State or local government is required to – in destroying an individual's records containing personal information – take reasonable steps to protect against unauthorized access to, or use of, the personal information. In doing so, the unit must take into account the sensitivity of the records, the nature of the unit and its operations, the costs and benefits of different destruction methods, and available technology.

A government unit or nonaffiliated third party that complies with specified federal laws and guidelines must be deemed to be in compliance with the bill.

The bill's provisions are exclusive and preempt any provision of local law.

Current Law/Background:

Commission on Maryland Cybersecurity Innovation and Excellence

Chapters 250 and 251 of 2011 (SB 557/HB 665) established the Commission on Maryland Cybersecurity Innovation and Excellence to (1) review current federal and State laws, standards, and policies for inconsistencies and preemption issues; (2) provide recommendations regarding strategic plans to promote cybersecurity innovation and recover from attacks on cybersecurity; and (3) recommend methods of promoting innovation through public-private partnerships, the education system, research and development, and selection of a State agency suitable to implement a pilot program. University of Maryland University College was tasked to provide staff support for the commission, which held an introductory meeting on November 22, 2011, before submitting its interim report to the Governor and the General Assembly on December 23, 2011. The commission is required to submit its final findings and recommendations to the Governor and the General Assembly by September 1, 2014.

Recent Legislative Audit of DoIT and Selected State Agencies

State agencies maintain significant volumes of personally identifiable information (such as Social Security numbers) that relate to income taxes, medical assistance program claims histories, criminal backgrounds, public assistance, and driver's licenses. In a recent legislative audit – which was presented to the Commission on Maryland Cybersecurity Innovation and Excellence – of DoIT and selected State agencies, the Office of Legislative Audits (OLA) recommended that State agencies ensure that they (1) comply with DoIT policies for evaluating and documenting the security categories for their systems and establish security measures commensurate with data sensitivity and risk; (2) develop agency-specific information security policies that address DoIT's required components of an information security program; (3) develop and implement a risk management process for all critical systems and periodically update or reevaluate the risk assessments; (4) provide timely security awareness training to all employees; and (5) ensure that confidential information on portable devices is encrypted, and that data loss prevention, vulnerability scanning, and penetration testing tools are used as feasible.

OLA further recommended that DoIT (1) address the protection of personally identifiable information in the custody of State agencies via legislation or policy; (2) address the notification of affected individuals and other appropriate parties in the event of a breach; (3) implement a process to monitor and enforce State agencies' compliance with DoIT's information security policies; (4) establish more thorough security incident response guidance; and (5) enhance its security policies and guidance in other areas identified in the audit report, including emerging technologies.

DoIT initially cited insufficient resources as an obstacle to implementing some of OLA's recommendations, but ultimately stated that it would (1) require each State agency under its jurisdiction (*i.e.*, executive agencies only) to submit an annual information system data security plan as well as perform an annual information system data security self-audit; (2) conduct an annual data security awareness and training session for all agency chief information officers; (3) conduct data security compliance assessments with selected agencies throughout the year; and (4) dedicate on additional full-time employee to support these activities.

Security Breaches and Identity Fraud Generally

In February 2012, the Federal Trade Commission and the Consumer Sentinel Network (CSN), a consortium of national and international law enforcement and private security entities, released the *Consumer Sentinel Network Data Book* for calendar 2011. In calendar 2011, CSN received 279,156 identity fraud complaints. In calendar 2010, the number of identity fraud complaints was 251,105. In Maryland, residents reported 4,980 instances of identity fraud in 2011, or 86.3 complaints per 100,000 population, ranking Maryland ninth in the nation for identity fraud. In a shift from the last several years, the most common type of identity fraud was government documents or benefits fraud in Maryland, which comprised 33% of all complaints. The second most prevalent type of identity fraud involved phone and utilities fraud and represented 13% of all complaints.

Any business that retains consumer records is required by Maryland law to notify a consumer who is a resident of Maryland if his or her information is compromised. The business is also required to notify OAG. According to OAG, there were 218 security breaches in fiscal 2012.

State Expenditures: While some State agencies report that they are already in compliance with the requirements established by the bill, other agencies advise that additional staffing and/or contractual services are needed to implement the bill – particularly with regard to security procedures and practices. Agencies anticipate further costs associated with the provision of notice to affected individuals in the event of the breach. The Department of Legislative Services (DLS) advises that costs associated with the bill's security and notice requirements depend on several factors – including the content of the regulations ultimately adopted under the bill, the extent to which an agency is already in compliance, and the number and extent of any subsequent security breaches – and cannot be reliably estimated at this time. However, given the expansiveness of the bill's requirements, the number of agencies affected, the amount of personal information that is stored by State agencies, and the number of individuals that could be affected by a security breach, DLS advises that expenditures could be significant.

Local Expenditures: Units of local government are affected in the same manner as the State with regard to the bill's security and notice requirements. As discussed above, expenditures may increase significantly.

Additional Information

Prior Introductions: None.

Cross File: HB 959 (Delegate Lee, *et al.*) (Commission on Maryland Cybersecurity Innovation and Excellence) - Health and Government Operations.

Information Source(s): Maryland Department of Information Technology, Maryland State Archives, Department of Budget and Management, Maryland State Department of Education, Maryland Higher Education Commission, Department of Health and Mental Hygiene, Comptroller's Office, Judiciary (Administrative Office of the Courts), Maryland Association of Counties, Maryland Municipal League, Department of State Police, Department of Public Safety and Correctional Services, Maryland Department of Transportation, Federal Trade Commission – *Consumer Sentinel Network Data Book for January-December 2011*, Department of Legislative Services

Fiscal Note History: First Reader - February 18, 2013
mc/lgc Revised - Senate Third Reader - April 6, 2013

Analysis by: Jennifer A. Ellick

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