Department of Legislative Services

Maryland General Assembly
2017 Session

FISCAL AND POLICY NOTE
First Reader - Revised

House Bill 435 (Delegate Stein)
Health and Government Operations

Governmental Procedures - Security of Computerized Data - Encryption of Personal Information

This bill requires a unit of State or local government (which does not include the Legislative or Judicial Branch of State government) to secure any personal information that it collects in electronic or optical form using encryption.

Fiscal Summary

State Effect: State expenditures (all funds) increase significantly for units of State government to meet the bill's encryption requirements. As discussed below, significant costs have been identified by the Department of Information Technology (DoIT) and the Comptroller's Office, and additional significant costs are anticipated for other State agencies that are not already in compliance with the bill's encryption requirements and that host their own networks and data storage. Revenues are not affected.

Local Effect: Local government expenditures increase significantly for units of local government that are not already in compliance with the bill's encryption requirements, as discussed below. Revenues are not affected. **This bill imposes a mandate on a unit of local government.**

Small Business Effect: Minimal.

Analysis

Current Law/Background:

Definitions

"Encryption" means the protection of data in electronic or optical form, in storage or in transit, using a technology that is certified to meet or exceed specified federal standards and renders the data indecipherable without an associated cryptographic key necessary to enable decryption of such data. "Personal information" means an individual's first name (or first initial) and last name, personal mark, or unique biometric or genetic print or image, in combination with one of a number of specified data elements such as the individual's Social Security number or driver's license number.

National Institute of Standards and Technology – the Utility of Encryption

The National Institute of Standards and Technology generally advises that cryptographic techniques should be considered for the protection of data that is sensitive, has a high value, or is vulnerable to unauthorized disclosure or undetected modification during transmission or while in storage. In today's environment of increasingly open and interconnected systems and networks and the use of mobile devices, network and data security are essential for the optimum safe use of this information technology.

Personal Information Protections Established by Chapter 304 of 2013

State agencies maintain significant volumes of personally identifiable information (PII, such as Social Security numbers) that relate to income taxes, medical assistance program claims histories, criminal backgrounds, public assistance, and driver's licenses.

Chapter 304 of 2013 requires a unit of State or local government (except for the Legislative and Judicial branches of State government) that collects an individual's personal information to 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.

If a government unit that collects computerized data that contains 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. If so, the unit (or the nonaffiliated third party, if authorized

under a written contract or agreement) generally must notify the individual of the breach. A unit must also provide notice of a breach of security to the Office of the Attorney General, DoIT, and consumer reporting agencies under specified conditions.

Legislative Audits – Personal Information Protection Concerns in Government

In a recent legislative audit bulletin, the Office of Legislative Audits (OLA) noted that nine audit reports issued during calendar year 2016 identified findings related to the inadequate safeguarding of sensitive PII on State agency databases. For example, in the February 2016 report of the Maryland Longitudinal Data System Center, OLA described several instances of improperly stored sensitive PII. More than 2.2 million unique individual names and Social Security numbers were stored in clear text in a database on the server, despite the database software being capable of data encryption.

State Expenditures: State expenditures (all funds) increase significantly for units of State government that are not already in compliance with the bill's encryption requirements. Even though the total effect across all State agencies cannot be reliably estimated, significant costs have been identified by DoIT and the Comptroller's Office.

Department of Information Technology

DoIT is able to provide a *partial* estimate of the effect for a number of State agencies. Specifically, DoIT advises that ensuring the encryption of stored data for the Executive Branch agencies for which DoIT provides information technology (IT) services is likely to cost *at least* (1) $22.4 million in fiscal 2018 for software licensing and hardware upgrades and (2) $8.7 million annually thereafter for ongoing licensing and maintenance costs. These costs reflect DoIT's proposed approach of consolidating all PII in one-third of its servers in order to minimize costs. To the extent that this approach is not feasible or otherwise not implemented, costs could be considerably higher to secure all 120 of DoIT's servers.

Under one scenario, however, the software licensing costs for DoIT may be able to be mitigated (by as much as $7.0 million in fiscal 2018) because DoIT recently signed a Statewide Enterprise Agreement with Microsoft to standardize on the Microsoft Cloud platform as part of its statewide consolidation initiative. As part of the agreement, DoIT may be upgrading some of its Microsoft SQL database servers, which is also necessary to implement the bill. Even so, DoIT advises that the agreement primarily focuses on end-user productivity products and it is unclear to what extent the databases accessed by end users will be encrypted absent the bill. Under the agreement, DoIT advises that it has access to additional encryption services through Microsoft, but the department is still required to purchase licenses to use those services.

Regardless, the *total* cost for DoIT is expected to be significantly higher because DoIT's estimate does not address likely costs for (1) labor to upgrade or replace, and reintegrate, certain legacy applications (legacy systems are discussed in more detail below); (2) replacing noncustom applications used by agencies that do not support encryption; (3) any other software licenses needed to ensure that data is stored in an encrypted form; and (4) additional software and hardware upgrades needed to ensure the encryption of data in transit. Although a precise estimate of these additional costs could not be provided in time for this analysis, DoIT advises that they are expected to be significant as some of them may be in the tens of millions of dollars. Thus, the total cost for DoIT in fiscal 2018 could easily be double the first-year known cost identified above.

Comptroller's Office and Other State Agencies

Many other State agencies, including the Comptroller's Office, the Maryland Department of Transportation, the Department of State Police, and the University System of Maryland host their own networks and store their own data that includes PII and, therefore, are not covered in DoIT's preliminary estimate. These agencies also incur significant costs to meet the bill's encryption requirements. For example, the Comptroller's Office advises that the existing security measures for its tax processing system do not meet the bill's encryption requirements. Therefore, the Comptroller's Office estimates a cost of approximately $15.2 million in fiscal 2018, with ongoing annual expenses of about $1.0 million, for it to make the necessary upgrades and software purchases to encrypt all of its data, both while it is stored and while it is in transit. Additionally, the Comptroller's Office advises that updating the system in this manner is likely to delay implementation of its new tax processing system.

Some of the comments received by the Department of Legislative Services in response to the bill discussed the issue of legacy systems making implementation of the bill challenging and expensive. Legacy systems are outdated (and in some cases obsolete) computer and IT systems that have been used by State agencies and local governments for many years. Many legacy systems are not compatible with modern encryption software, which necessitates additional hardware upgrades before the government unit can purchase and install encryption software.

Local Expenditures: Units of local government are affected in the same manner as the State with regard to the bill's encryption requirements. Therefore, local government expenditures are expected to increase significantly for local governments that do not store personal data using encryption.

According to the Maryland Association of Counties, some local government entities (such as Baltimore County) currently use encryption for the storage of data and, therefore, already meet the bill's requirements. Expenditures for other local government entities that

do not use encryption for data storage increase significantly. For example, the City of Frederick estimates a cost of $270,000 in fiscal 2018 and $170,000 annually thereafter to ensure all of its personal data is encrypted. Montgomery County, which stores much more personal data, estimates as much as (1) $1.0 million to organize and catalog its existing data; (2) $15.0 million over 5 to 10 years to fully encrypt its numerous databases and systems; (3) $5.0 million to purchase additional hardware and software licenses; and (4) $1.0 million each year for ongoing licensing and compliance costs.

Additional Information

Prior Introductions: None.

Cross File: None.

Information Source(s): Department of Information Technology; Comptroller's Office; University System of Maryland; Montgomery and Garrett counties; Maryland Association of Counties; cities of Frederick and Havre de Grace; Maryland Municipal League; Judiciary (Administrative Office of the Courts); Department of Legislative Services

Fiscal Note History: First Reader - February 6, 2017
mm/mcr Revised - Updated Information - March 10, 2017

Analysis by: Richard L. Duncan

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