HOUSE BILL REPORT
HB 1466

As Reported by House Committee On:
General Government & Information Technology

Title: An act relating to encryption of data on state information technology systems.

Brief Description: Establishing data classification and encryption standards for state agencies.

Sponsors: Representatives Hudgins, Magendanz, Stanford, Smith, S. Hunt and Ormsby.

Brief History:
Committee Activity:
General Government & Information Technology: 1/30/15, 2/6/15 [DPS].

Brief Summary of Substitute Bill

- Establishes a data classification schedule as part of the information technology security standards set by the Office of the Chief Information Officer (OCIO).
- Directs the OCIO to adopt encryption standards for each data category.
- Requires state agency data to be categorized according to the schedule and encrypted according to the standards. Certain agencies are required to submit a plan for implementing the encryption policy to the OCIO for approval.
- Allows the OCIO to grant waivers to the established encryption policy.

HOUSE COMMITTEE ON GENERAL GOVERNMENT & INFORMATION TECHNOLOGY

Majority Report: The substitute bill be substituted therefor and the substitute bill do pass. Signed by 7 members: Representatives Hudgins, Chair; Senn, Vice Chair; MacEwen, Ranking Minority Member; Caldier, Assistant Ranking Minority Member; McCabe, Morris and Takko.

Staff: Derek Rutter (786-7157).

Background:

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not a part of the legislation nor does it constitute a statement of legislative intent.

Office of the Chief Information Officer.
The Office of the Chief Information Officer (OCIO) was created in 2011 within the Office of Financial Management (OFM). The OCIO is responsible for the preparation and implementation of a strategic information technology (IT) plan and enterprise architecture for the state. The OCIO works toward standardization and consolidation of IT infrastructure and establishes IT standards and policies, including state IT security policies. The OCIO also prepares a biennial state performance report on IT, evaluates current IT spending and budget requests, and oversees major IT projects.

OCIO Data Security Policies.
The OCIO has established policy for classifying and securely managing state agency data. According to this policy, agencies must classify data into categories based on the sensitivity of the data. There are four categories defined in the current policy: public information (category 1), sensitive information (category 2), confidential information (category 3), and confidential information requiring special handling (category 4). The policy requires category 3 and category 4 data to be encrypted using industry standard encryption methods validated by the National Institute of Standards and Technology. It also defines standards for sharing and transferring data in these categories.

Summary of Substitute Bill:

A data classification schedule is established in the information technology standards maintained by the Office of the Chief Information Officer (OCIO). State agencies must classify all data stored on state data networks or elsewhere according to the schedule. Agencies storing or transmitting data falling in the most sensitive classes must encrypt these data or develop a plan for encryption, depending on where the data are transmitted or stored. In the cases where agencies must develop an encryption plan, the OCIO must review and approve these plans. The OCIO is also directed to adopt and annually update data encryption standards appropriate to each data category and may grant individual waivers to this policy.

Substitute Bill Compared to Original Bill:

The substitute bill clarifies that data passing to, through, or from state data networks must be classified. Specific data category definitions were stricken from the original bill; the substitute instead refers to the information technology standards maintained by the Office of the Chief Information Officer (OCIO), which includes category definitions. The substitute also adds the following: a requirement that agencies classify state data stored in locations other than state data systems; a requirement that high-sensitivity agency data not stored or transmitted within the state network be encrypted; a requirement that agencies storing or transmitting high-sensitivity data on or within the state network submit a plan for implementing encryption to the OCIO; a requirement for the OCIO to review, approve, and report plans to the Legislature; and a new definition for "encryption." Language in the original bill allowing the OCIO to grant waivers specifically when encryption was "unreasonably costly" was removed.

Appropriation: None.

Fiscal Note: Available.

Effective Date of Substitute Bill: The bill takes effect 90 days after adjournment of the session in which the bill is passed.

Staff Summary of Public Testimony:

(In support) None.

(With concerns) There is nothing more important to cybersecurity than knowing where your data is and what type it is so that it can be properly protected. There were technical nuances in the original bill that raised concerns about runaway costs, but the substitute appears to have addressed the issues. Encrypting data on legacy systems will present challenges and high costs. Data collection minimization is also an important consideration in moving forward with enhancing state information-technology security.

(Opposed) None.

Persons Testifying: Michael Cockrill, Office of the Chief Information Officer; and Rob St. John, Consolidated Technology Services.

Persons Signed In To Testify But Not Testifying: None.