HOUSE BILL REPORT
2SHB 1469

As Passed House:
June 11, 2015

Title: An act relating to the removal of payment credentials and other sensitive data from state data networks.

Brief Description: Addressing removal of payment credentials and other sensitive data from state data networks.

Sponsors: House Committee on Appropriations (originally sponsored by Representatives Hudgins, Magendanz, Stanford, Ormsby and Tarleton).

Brief History:
Committee Activity:
General Government & Information Technology: 1/30/15, 2/10/15 [DPS];
Appropriations: 2/25/15, 2/26/15 [DP2S(w/o sub GGIT)].
Floor Activity:
Passed House: 3/11/15, 98-0.
Second Special Session
Floor Activity:
Passed House: 6/11/15, 89-0.

Brief Summary of Second Substitute Bill

- Prohibits state agencies from storing payment credentials on state data systems.
- Requires payment credentials collected on behalf of state agencies to be accepted and stored by a third-party institution compliant with industry leading security standards.
- Places financial liability of data breaches on third-party institutions storing the compromised payment credentials if the institution is found not to have been compliant with industry leading security standards at the time of the breach.
- Directs state agencies to remove currently stored payment credentials from state data systems by 2018 unless granted a waiver from the Office of the Chief Information Officer (OCIO).

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.

- Directs the OCIO to develop a policy for minimizing retention of social security numbers and other sensitive data on state data systems.

HOUSE COMMITTEE ON GENERAL GOVERNMENT & INFORMATION TECHNOLOGY

Majority Report: The substitute bill be substituted therefor and the substitute bill do pass. Signed by 6 members: Representatives Hudgins, Chair; Senn, Vice Chair; MacEwen, Ranking Minority Member; McCabe, Morris and Takko.

Staff: Derek Rutter (786-7157).

HOUSE COMMITTEE ON APPROPRIATIONS

Majority Report: The second substitute bill be substituted therefor and the second substitute bill do pass and do not pass the substitute bill by Committee on General Government & Information Technology. Signed by 33 members: Representatives Hunter, Chair; Ormsby, Vice Chair; Chandler, Ranking Minority Member; Parker, Assistant Ranking Minority Member; Wilcox, Assistant Ranking Minority Member; Buys, Carlyle, Cody, Condotta, Dent, Dunshee, Haler, Hansen, Hudgins, G. Hunt, S. Hunt, Jinkins, Kagi, Lytton, MacEwen, Magendanz, Pettigrew, Sawyer, Schmick, Senn, Springer, Stokesbary, Sullivan, Taylor, Tharinger, Van Werven, Walkinshaw and Fagan.

Staff: Derek Rutter (786-7157).

Background:

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.

Summary of Second Substitute Bill:

State agencies are prohibited from holding payment credentials on state data systems. Payment credentials are defined to include credit and debit card data, but exclude data required for outgoing payments, distributions, or transfers. Payment credentials collected on behalf of state agencies must be accepted and stored, the data may be transferred and stored with a third-party institution that is compliant with industry leading security standards. Agencies that currently store payment credentials must work with the OCIO to eliminate these data from state systems by 2018, but may be given a waiver to this requirement from the OCIO. A third-party institution is financially liable for damages resulting from a data

security breach if it is found not to have been compliant with industry leading standards at the time of the breach.

State agencies currently holding payment credentials must work with the OCIO to eliminate these data by July 2018, though the OCIO may grant a waiver to this requirement where payment credentials must be held for day-to-day agency operation or by law.

The OCIO is also directed to develop a policy for minimizing retention of social security numbers and other sensitive, personally identifiable information on state data networks, with which all state agencies must comply. Ongoing retention of such information must be justified as part of the policy.

Appropriation: None.

Fiscal Note: Available.

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

Staff Summary of Public Testimony (General Government & Information Technology):

(In support) None.

(With concerns) Technology moves much faster than the Legislature can keep up. The state acts as a merchant, and not long ago, merchants regularly held cardholder data. Today, that poses an unacceptable level of risk for merchants, as those data represent a "honeypot," or target for hackers. There is no longer any good business reason for the state to hold that honeypot. Getting it off our network is one of the best things we can do to make the state a less attractive target. This will cost a significant amount of money, but is a long-term investment worth making.

The bill also deals with social security numbers and other sensitive data. It is more likely that a waiver would be given to allow agencies to hold these data, as the cost of removing these data is likely much higher than the cost of removing payment credentials.

The term "payment credentials" is preferable to "cardholder data" because it covers a wider variety of payment mechanisms. Many of the concerns with the original bill have been fixed in the substitute.

(Opposed) None.

Staff Summary of Public Testimony (Appropriations):

(In support) This is one of the most important things that can be done to lower the financial risk that the state has and make the state a less attractive target; it is high on the priority list in terms of lowering the state's overall risk profile.

With regard to implementation, a new, modern payment system that stores payment information should not be built, and most modern systems that do store this information should be easy to update so that they do not. The bigger operational challenge comes from old, legacy systems. Taking the payment information out of those may be difficult, which is one of the reasons the three-year timeframe is allowed in the bill. Risk and cost are always traded off, and older systems should be looked at individually to evaluate the cost of mitigating the system in place against the cost of just replacing the system.

(Opposed) None.

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

Persons Testifying (Appropriations): Representative Hudgins, prime sponsor; and Michael Cockrill, Office of the Chief Information Officer.

Persons Signed In To Testify But Not Testifying (General Government & Information Technology): None.

Persons Signed In To Testify But Not Testifying (Appropriations): None.