

HOUSE BILL REPORT

HB 1469

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

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: Representatives Hudgins, Magendanz, Stanford, Ormsby and Tarleton.

Brief History:

Committee Activity:

General Government & Information Technology: 1/30/15, 2/10/15 [DPS].

Brief Summary of Substitute Bill

- Prohibits state agencies from holding payment credentials on state data systems.
- Allows agencies to transfer collected payment credentials to third-party institutions compliant with industry leading security standards if credentials must be stored.
- Places financial liability of data breaches on third-party institutions holding 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).
- 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

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.

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).

Background:

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.

Summary of 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. If payment credentials collected by state agencies must be stored, the data may be transferred and stored with a third-party institution that is compliant with industry leading security standards. Such an 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.

Substitute Bill Compared to Original Bill:

The substitute bill provides a definition for "payment credentials," and replaces all instances of the term "cardholder data" in the original bill with "payment credentials." All references to the "Payment Card Industry Security Standards," a specific set of payment card industry security standards, are removed in the substitute bill; instead, agencies are directed to store data with "third-party institutions" compliant with "industry leading security standards," where applicable. The requirement that payment credentials held on state data systems be transferred to a single secure storage system administered by the Consolidated Technology

Services agency, where applicable, is removed. Language directing the OCIO to develop a policy for "removing" sensitive information from state networks is revised; instead, the OCIO is directed to develop a policy for "minimizing retention" of such information, and any ongoing retention must be justified.

Appropriation: None.

Fiscal Note: Available. New fiscal note requested on February 6, 2015.

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) 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.

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.