Washington State
House of Representatives
Office of Program Research

BILL ANALYSIS

General Government & Information Technology Committee

HB 1469

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

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

Brief Summary of Bill

- Prohibits state agencies from holding payment credentials on state data systems.
- Allows agencies to transfer collected payment credentials to PCI-compliant third-party institutions if credentials must be held.
- Places financial liability of data breaches on third-party institutions holding the compromised payment credentials if the institution is found not to have been PCI-compliant at the time of the breach.
- Directs state agencies to remove currently held payment credentials from state data systems by 2018 unless granted a waiver from the Office of the Chief Information Officer (OCIO).
- Requires payment credentials that must be held for day-to-day agency operations or by law to be held on a secure system administered by Consolidated Technology Services.
- Directs the OCIO to develop a policy for removing social security numbers and other sensitive data from state data systems by 2018.

Hearing Date: 1/30/15

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's duties include standardization and consolidation of IT infrastructure and establishment of 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.

Consolidated Technology Services
Consolidated Technology Services (CTS) was created in 2011 to provide technology-based services to state agencies and local governments, including server hosting and network administration, telephony, security administration, and email.

PCI Security Standards Council and the PCI Security Standards
The PCI Security Standards Council is a consortium founded in 2006 by five private global payment brands - American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc. - that is responsible for the development and management of the PCI Security Standards. The PCI Security Standards are industry standards relating to payment card data security, including methods for prevention, detection, and appropriate reaction to data breaches and payment cardholder data fraud. The payment brands that founded the PCI Security Standards Council have collectively adopted PCI Security Standards compliance (PCI-compliance) as the requirement for organizations that process, store, or transmit payment cardholder data. Enforcement of the standards is carried out by the individual payment brands through contracts.

Summary of Bill:

State agencies are prohibited from holding cardholder data or other payment credentials on state data systems. If payment credentials collected by state agencies must be held, the data may be transferred and stored with a third-party institution that is compliant with the PCI Security Standards. Such an institution is financially liable for damages resulting from a data security breach if it is found not to have been PCI-compliant 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. Payment credentials that must be held for day-to-day agency operation or by law must be transferred to a unified secure data storage system administered by Consolidated Technology Services by July 2018. The OCIO may grant waivers extending this deadline.

The OCIO is also directed to develop a policy for removing social security numbers and other sensitive, personally identifiable information from state data networks, with which all state agencies must comply.

Appropriation: None.

Fiscal Note: Requested.

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