Washington State
House of Representatives
Office of Program Research

BILL ANALYSIS

State Government, Elections & Information Technology Committee

HB 1421

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

Sponsors: Representatives Smith, Hudgins and Stanford.

Brief Summary of Bill

- Prohibits state agencies from storing payment credentials.
- Provides waivers to agencies in specified circumstances.
- Requires a compliant third-party institution to accept and store payment credentials.

Hearing Date: 2/1/17

Staff: Megan Palchak (786-7105).

Background:

In 2016, the Office of the Attorney General indicated in its Data Breach Report that financial account information was the most frequently compromised type of information. At the time of report, data breaches, such as malicious cyber security attacks, unintentional breaches, and unauthorized access, had impacted fewer than 10,000 consumers in Washington State. Cybersecurity attacks cause most breaches.

The Consolidated Services Technology Agency (CSTA), or WaTech, is required to establish security standards and policies to ensure the confidentiality and integrity of information transacted, stored, or processed in the state's information technology systems and infrastructure. Each state agency must develop an information technology security program.

The Office of Privacy and Data Protection (OPDP) is a point of contact for state agencies on policy matters involving data privacy and protection. The OPDP conducts annual privacy

---

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.

reviews, trains agencies and employees, articulates privacy principles and best practices, coordinates data protection in cooperation with the CSTA, and participates with the Office of the State Chief Information Officer in the review of major state agency projects involving personally identifiable information.

Summary of Bill:

State agencies are prohibited from storing payment credentials on state data systems. Payment credentials include: (1) the full magnetic stripe or primary account number of a credit or debit card combined with cardholder name, expiration date or service code, or (2) personally identifiable credentials allowing the state to receive incoming payments for services, excluding account information required for making outgoing payments, distributions, and transfers. The CTSA must develop policy to minimize retention of personally identifiable information.

Payment data must be eliminated from state systems by July 1, 2020. Waivers may be granted in instances where transitioning payment credentials off state data systems presents special difficulty, or where holding payment credentials is required for day-to-day agency business of the agency or by law.

Payment credential data must be accepted and stored by a third-party institution that is fully compliant with industry standards, which must be liable for security breaches if out of compliance with standards.

Appropriation: None.

Fiscal Note: Available.

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