
**State Government, Elections &
Information Technology Committee**

HB 1479

Brief Description: Concerning encryption of data on state information technology systems.

Sponsors: Representatives Hudgins, Graves, Tarleton and Stanford.

Brief Summary of Bill

- Requires classification and encryption of data associated with state networks.

Hearing Date: 2/7/17

Staff: Megan Palchak (786-7105).

Background:

The Consolidated Services Technology Agency (CSTA), or WaTech, is required to establish security standards and policies to ensure the confidentiality, availability, and integrity of the 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 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 (Office) Officer in the review of major state agency projects involving personally identifiable information.

Summary of Bill:

The CTSA must establish a classification schedule for data on, or passing through, state data networks. State agencies must classify all data stored on state systems or elsewhere. Any

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.

agency not on the state governmental network must encrypt data. All data considered confidential and not stored or transmitted by the state governmental network must be encrypted, or protected, in electronic or optical form, while in transit or storage. Encryption technology utilized must meet standards, such as those adopted by the national institute of standards and technology.

Agencies must submit plans for storing or transmitting confidential data, no later than September 1, 2018. Plans must include a total cost estimate and timeline for implementation. The Office must: (a) review and approve, or work with agencies to modify plans to align with the Office policy; (b) submit a report summarizing the final approved plans to the Legislature by 2019, which must include agency cost estimates and implementation timeframes, and may exclude information exposing potential vulnerabilities; (c) adopt encryption standards for state agency compliance; (d) update and distribute standards to state information technology directors, annually by the end of each fiscal year, which include phase-in of any new technologies; and (e) grant individual waivers.

Appropriation: None.

Fiscal Note: Preliminary fiscal note available.

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