**Washington State**
**House of Representatives**
**Office of Program Research**

# BILL ANALYSIS

# General Government & Information Technology Committee

# HB 1466

**Brief Description**: Establishing data classification and encryption standards for state agencies.

**Sponsors**: Representatives Hudgins, Magendanz, Stanford, Smith, S. Hunt and Ormsby.

**Brief Summary of Bill**

- Establishes a data classification schedule categorizing electronic data according to sensitivity and requires state agencies to classify data according to the schedule.
- Requires state agency data in the most sensitive categories to be encrypted at rest and in transit.
- Directs the Office of the Chief Information Officer (OCIO) to adopt encryption standards for each data category.
- Allows the OCIO to grant waivers to the established encryption policies where encryption would be unreasonably costly.

**Hearing Date**: 1/30/15

**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'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.

---

*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.*

OCIO Data Security Policies

The OCIO has established a policy for classifying and securely managing state agency data. According to this policy, agencies must classify data into categories based on the sensitivity of the data. There are four categories defined in the current policy: public information (category 1), sensitive information (category 2), confidential information (category 3), and confidential information requiring special handling (category 4). The policy requires category 3 and category 4 data to be encrypted using industry standard encryption methods validated by the National Institute of Standards and Technology (NIST). It also defines standards for sharing and transferring data in these categories.

**Summary of Bill**:

A data classification schedule is established in statute. State agencies must classify all data stored on state data networks according to the schedule. Agencies storing category 3 and 4 information must encrypt these data while at rest and in transit off the state governmental network. Agencies not on the state governmental network must encrypt category 3 and 4 data transmitted outside the agency's secure network. The OCIO is directed to adopt and annually update data encryption standards appropriate to each data category and may grant waivers in specific cases where encryption would be unreasonably costly.

**Appropriation**: None.

**Fiscal Note**: Requested.

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