H-0470.1

HOUSE BILL 1466

State of Washington 64th Legislature 2015 Regular Session

By Representatives Hudgins, Magendanz, Stanford, Smith, S. Hunt, and Ormsby

Read first time 01/21/15. Referred to Committee on Gen Govt & Info Tech.

AN ACT Relating to encryption of data on state information technology systems; and adding a new section to chapter 43.41A RCW.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

NEW SECTION. **Sec. 1.** A new section is added to chapter 43.41A RCW to read as follows:

(1) A classification schedule for data stored on or passing through state data networks is established with the following categories based on the sensitivity of the data:

(a) "Category 1" means information that may be released to the public.

(b) "Category 2" means information that may not be specifically protected from disclosure by law, but is for official use only. Category 2 information is generally not released to the public unless specifically requested.

(c) "Category 3" means information that is specifically protected from disclosure by law.

(d) "Category 4" means information that is specifically protected from disclosure by law, and for which especially strict handling requirements are dictated, such as by statutes, regulations or agreements. Category 4 includes information the unauthorized disclosure of which could result in serious consequences, such as threats to health and safety, or legal sanctions.

(2) State agencies must classify all data stored on state data systems according to the schedule established under subsection (1) of this section.

(3) Agencies storing Category 3 and Category 4 information must select and apply encryption to these data while at rest, using industry standard algorithms or cryptographic modules validated by the national institute of standards and technology.

(4) Agencies transmitting Category 3 and Category 4 information off the state governmental network must encrypt these data, using industry standard algorithms or cryptographic modules validated by the national institute of standards and technology, such that:

(a) All manipulations or transmissions of data during the exchange are secure;

(b) If intercepted during transmission, the data cannot be deciphered; and

(c) When necessary, confirmation is received when the intended recipient receives the data.

(5) Agencies not on the state governmental network must follow the standards established in subsection (4) of this section when transmitting Category 3 and Category 4 information outside the agency's secure network.

(6) The office shall adopt data encryption standards with which all state agencies must comply. The standards must include technical requirements for encryption beyond those specified in subsections (3), (4), and (5) of this section that are appropriate to each data classification established under subsection (1) of this section.

(7) The office shall update and distribute the encryption standards to state information technology directors annually, by the end of each fiscal year, to reflect the changing state of information technology. The annual distribution must include a timeline for phase-in of any new technologies required under the updated standards.

(8) The office may grant individual waivers to the policies established under subsections (3), (4), (5), and (6) of this section in cases where encryption is deemed unreasonably costly.

--- END ---