H-1287.2

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**SUBSTITUTE HOUSE BILL 1466**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**State of Washington 64th Legislature 2015 Regular Session**

**By** House General Government & Information Technology (originally sponsored by Representatives Hudgins, Magendanz, Stanford, Smith, S. Hunt, and Ormsby)

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.**  A new section is added to chapter 43.41A RCW to read as follows:

(1) A classification schedule for data stored on or passing to, through, or from state data networks is established in the information technology standards maintained by the office.

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

(3) State agency data falling in the most sensitive classes that are not stored on or transmitted within the state governmental network must be encrypted using industry standard encryption. For the purposes of this section, "encryption" means the protection of data in electronic or optical form, in storage or in transit, using:

(a) An encryption technology that has been adopted by an established standards-setting body including, but not limited to, the national institute of standards and technology that issues the federal information processing standards, which technology must render data indecipherable in the absence of associated cryptographic keys necessary to enable decryption; and

(b) Appropriate management and safeguarding of cryptographic keys to protect the integrity of encryption using guidelines promulgated by an established standards-setting body including, but not limited to, the national institute of standards and technology.

(4) Agencies storing or transmitting data in the most sensitive classes on or within the state governmental network must submit a plan to the office for encrypting these data. The plan must be submitted as soon as can reasonably be expected, but no later than September 1, 2016, and must include a timeline for implementation and a total cost estimate. The office must review and approve the plan or work with the agency to modify the plan to align with office policies. Agencies are encouraged to seek the advice of the office as early in the development of their plans as possible to facilitate expedient approval. The office must submit a report summarizing the final, approved plans to the appropriate committees of the legislature by the beginning of the 2017 legislative session. The report must include timelines and cost estimates, but may exclude information that could be used to identify specific vulnerabilities in the state's data systems.

(5) Agencies not on the state governmental network must follow the standards established in subsection (3) of this section when transmitting or storing information in the most sensitive classes 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 in this section.

**--- END ---**