H-3308.1

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

**HOUSE BILL 2278**

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

**State of Washington 65th Legislature 2018 Regular Session**

**By** Representatives Morris, Hudgins, Smith, Slatter, Tharinger, Macri, Young, Kloba, and Appleton

AN ACT Relating to enhancing personal information privacy protections in government entities; amending RCW 42.56.420; adding a new section to chapter 19.215 RCW; and adding a new chapter to Title 40 RCW.

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

NEW SECTION. **Sec.**  (1) Each department or other agency of the state government must designate an agency privacy officer. In coordination with the state office of privacy and data protection, the agency privacy officer must:

(a) Develop an agency personal information minimization policy to reduce the use and retention of personal information wherever possible;

(b) Create a work plan that uses a Gantt chart or similar project planning tool for the following, including the estimated costs of execution:

(i) An inventory of all personal information prepared, owned, used, or retained by the agency, that would include the specific type of information, the purpose for its collection, and the extent to which the information is protected from unauthorized access; and

(ii) A map of the physical or digital location of all personal information collected by the agency, that would be indexed to the inventory created in (b)(i) of this subsection; and

(c) Report the work plan created under (b) of this subsection to the state office of privacy and data protection no later than December 15, 2018.

(2) Agency privacy officers designated under subsection (1) of this section must complete a training course provided by the state office of privacy and data protection on privacy best practices. The training course must be completed no later than sixty days after assuming responsibilities as an agency privacy officer, and at intervals of no more than four years as long as they maintain the designation.

(3) Any inventory or data map records created under subsection (1)(b) of this section that reveal the location of personal information or the extent to which it is protected may not be disclosed under the public records act, chapter 42.56 RCW.

(4) For purposes of this section, "personal information" has the same meaning as in RCW 42.56.590(5).

NEW SECTION. **Sec.**  A new section is added to chapter 19.215 RCW to read as follows:

A governmental entity is prohibited from selling:

(1) Personal financial and health information; and

(2) Personal identification numbers issued by a government entity.

**Sec.**  RCW 42.56.420 and 2017 c 149 s 1 are each amended to read as follows:

The following information relating to security is exempt from disclosure under this chapter:

(1) Those portions of records assembled, prepared, or maintained to prevent, mitigate, or respond to criminal terrorist acts, which are acts that significantly disrupt the conduct of government or of the general civilian population of the state or the United States and that manifest an extreme indifference to human life, the public disclosure of which would have a substantial likelihood of threatening public safety, consisting of:

(a) Specific and unique vulnerability assessments or specific and unique response or deployment plans, including compiled underlying data collected in preparation of or essential to the assessments, or to the response or deployment plans; and

(b) Records not subject to public disclosure under federal law that are shared by federal or international agencies, and information prepared from national security briefings provided to state or local government officials related to domestic preparedness for acts of terrorism;

(2) Those portions of records containing specific and unique vulnerability assessments or specific and unique emergency and escape response plans at a city, county, or state adult or juvenile correctional facility, or secure facility for persons civilly confined under chapter 71.09 RCW, the public disclosure of which would have a substantial likelihood of threatening the security of a city, county, or state adult or juvenile correctional facility, secure facility for persons civilly confined under chapter 71.09 RCW, or any individual's safety;

(3) Information compiled by school districts or schools in the development of their comprehensive safe school plans under RCW 28A.320.125, to the extent that they identify specific vulnerabilities of school districts and each individual school;

(4) Information regarding the public and private infrastructure and security of computer and telecommunications networks, consisting of security passwords, security access codes and programs, access codes for secure software applications, security and service recovery plans, security risk assessments, and security test results to the extent that they identify specific system vulnerabilities, and other such information the release of which may increase risk to the confidentiality, integrity, or availability of security, information technology infrastructure, or assets;

(5) The system security and emergency preparedness plan required under RCW 35.21.228, 35A.21.300, 36.01.210, 36.57.120, 36.57A.170, and 81.112.180; ((~~and~~))

(6) Personally identifiable information of employees, and other security information, of a private cloud service provider that has entered into a criminal justice information services agreement as contemplated by the United States department of justice criminal justice information services security policy, as authorized by 28 C.F.R. Part 20; and

(7) Personal information inventory or data map records created under section 1(1)(b) of this act, that reveal the location of personal information or the extent to which it is protected.

NEW SECTION. **Sec.**  Section 1 of this act constitutes a new chapter in Title 40 RCW.

**--- END ---**