80th OREGON LEGISLATIVE ASSEMBLY--2019 Regular Session

Senate Bill 818

Sponsored by Senators KNOPP, GOLDEN

SUMMARY

The following summary is not prepared by the sponsors of the measure and is not a part of the body thereof subject to consideration by the Legislative Assembly. It is an editor's brief statement of the essential features of the measure **as introduced.**

Establishes program to improve cybersecurity of systems used to administer elections by encouraging independent technical experts, in cooperation with state election officials, local government election officials and election service providers, to identify and report election cybersecurity vulnerabilities.

A BILL FOR AN ACT

Relating to election cybersecurity.

Be It Enacted by the People of the State of Oregon:

SECTION 1. Section 2 of this 2019 Act is added to and made a part of ORS chapter 254.

SECTION 2. (1) As used in this section:

(a) "Election cybersecurity vulnerability" means any security vulnerability that affects an election system.

(b) "Election service provider" means any person, including a contractor or vendor, who provides, supports or maintains an election system on behalf of the state or a local government.

(c) "Election system" means any system used for the management, support or administration of an election for state office or local office, including:

(A) Voting machines;

(B) The vote tally system;

(C) The electronic voter registration system described in ORS 247.019;

(D) Elector registration databases; and

(E) The electronic mail system used by state election officials or local government election officials.

(d) "Security control" means the management, operational and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity and availability of an election system or its information.

(e) "Security vulnerability" means any attribute of hardware, software, process or procedure that could enable or facilitate the defeat of a security control.

(2) The Secretary of State by rule shall establish a program to improve the cybersecurity of the election systems in this state. The program shall encourage independent technical experts, in cooperation with state election officials, local government election officials and election service providers, to make assessments to identify and report election cybersecurity vulnerabilities. The secretary may award competitive contracts as necessary to manage the program established under this section.

(3) The program established under this section shall include:

NOTE: Matter in **boldfaced** type in an amended section is new; matter [*italic and bracketed*] is existing law to be omitted. New sections are in **boldfaced** type.

(a) A recurring competition that allows independent technical experts to assess Oregon's election systems for the purpose of identifying and reporting election cybersecurity vulnerabilities;

(b) An expeditious process by which independent technical experts can qualify to participate in the competition;

(c) A schedule of awards, either monetary or nonmonetary, for reports of previously unidentified election cybersecurity vulnerabilities discovered by independent technical experts during the competition;

(d) A process for local government election officials and election service providers to voluntarily participate in the program by designating specific election systems, periods of time and circumstances for assessment by independent technical experts;

(e) A method for promptly notifying state election officials, local government election officials and election service providers about relevant election cybersecurity vulnerabilities discovered through the competition; and

(f) A method for promptly providing technical assistance in remedying any election cybersecurity vulnerabilities discovered through the competition.

(4)(a) State election officials shall participate in the program established under this section.

(b) Local government election officials and election service providers may participate in the program established under this section, but are not required to participate.

(c) In developing the program established under this section, the Secretary of State shall solicit input from, and encourage participation by, local government election officials.

(5) Notwithstanding any other provision of law, and except as provided in subsection (6) of this section, a person may not be found to have violated any laws of this state by taking an action necessary to discover an election cybersecurity vulnerability if the person:

(a) Acts in compliance with the rules of the program established under this section; and

(b) Reports the election cybersecurity vulnerability to the Secretary of State.

(6) Subsection (5) of this section does not apply to a person who:

(a) Acts outside the scope of the program established under this section;

(b) Exploits an election cybersecurity vulnerability; or

(c) Publicly exposes an election cybersecurity vulnerability before:

(A) Reporting the vulnerability to the Secretary of State; and

(B) Receiving permission from the secretary to publicly expose the vulnerability.