State of Minnesota

HOUSE OF REPRESENTATIVES

NINETY-FIRST SESSION

H. F. No. 4084

03/04/2020 Authored by Nash
The bill was read for the first time and referred to the Committee on Government Operations

A bill for an act

relating to elections; providing for election technology and cybersecurity assessment, maintenance, and enhancement; requiring certain election security notifications; amending Minnesota Statutes 2018, sections 201.022, subdivision 1; 204B.27, subdivisions 5, 10; 206.57, subdivision 6; proposing coding for new law in Minnesota Statutes, chapters 5; 209.

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

Section 1. **[5.42] TECHNOLOGY AND CYBERSECURITY FUND.**

Subdivision 1. **Definitions.** For the purposes of this section, the terms defined in this subdivision have the meanings given them:

(1) "information and telecommunications technology systems and services" has the meaning given in section 16E.03, subdivision 1, paragraph (b); and

(2) "cybersecurity" has the meaning given in section 16E.03, subdivision 1, paragraph (e).

Subd. 2. **Special revenue fund.** (a) The secretary of state may retain two percent of all statutory fees collected by the secretary of state for costs to maintain and enhance the secretary of state's information and telecommunications technology systems and services and for cybersecurity.

(b) Money received under this subdivision must be deposited in an account in the special revenue fund and is appropriated to the secretary of state for purposes of this subdivision.

Sec. 2. Minnesota Statutes 2018, section 201.022, subdivision 1, is amended to read:

Subdivision 1. **Establishment.** The secretary of state shall maintain a statewide voter registration system to facilitate voter registration and to provide a central database containing voter registration information from around the state. The system must be accessible to ~~the~~ any county auditor ~~of each county in the state~~ who has completed any required training established under section 204B.27, subdivision 10. The system must also:

(1) provide for voters to submit their voter registration applications to any county auditor, the secretary of state, or the Department of Public Safety;

(2) provide for the definition, establishment, and maintenance of a central database for all voter registration information;

(3) provide for entering data into the statewide registration system;

(4) provide for electronic transfer of completed voter registration applications from the Department of Public Safety to the secretary of state or the county auditor;

(5) assign a unique identifier to each legally registered voter in the state;

(6) provide for the acceptance of the Minnesota driver's license number, Minnesota state identification number, and last four digits of the Social Security number for each voter record;

(7) coordinate with other agency databases within the state;

(8) allow county auditors and the secretary of state to add or modify information in the system to provide for accurate and up-to-date records;

(9) allow county auditors, municipal and school district clerks, and the secretary of state to have electronic access to the statewide registration system for review and search capabilities;

(10) provide security and protection of all information in the statewide registration system and ensure that unauthorized access is not allowed;

(11) provide access to municipal clerks to use the system;

(12) provide a system for each county to identify the precinct to which a voter should be assigned for voting purposes;

(13) provide daily reports accessible by county auditors on the driver's license numbers, state identification numbers, or last four digits of the Social Security numbers submitted on

voter registration applications that have been verified as accurate by the secretary of state; ~~and~~

(14) provide reports on the number of absentee ballots transmitted to and returned and cast by voters under section 203B.16~~.~~; and

(15) require all users to use a multifactor authentication method approved by the secretary of state to access the system.

The appropriate state or local official shall provide security measures to prevent unauthorized access to the computerized list established under section 201.021.

Sec. 3. Minnesota Statutes 2018, section 204B.27, subdivision 5, is amended to read:

Subd. 5. **Conferences for county auditors.** Before each state primary the secretary of state shall conduct conferences with county auditors to instruct them on the administration of election laws, election security and best practices, and the training of local election officials and election judges.

Sec. 4. Minnesota Statutes 2018, section 204B.27, subdivision 10, is amended to read:

Subd. 10. **Training for county auditors; training materials.** The secretary of state shall develop a training program in election administration for county auditors and shall certify each county auditor who successfully completes the training program. The secretary of state shall provide each county auditor with materials for use in training local election officials and election judges. The training program and materials for use in training local election officials must include training on election security and best practices. The secretary of state may require additional training for an election official before providing the election official access to the statewide voter registration system.

Sec. 5. Minnesota Statutes 2018, section 206.57, subdivision 6, is amended to read:

Subd. 6. **Required certification testing.** (a) In addition to the requirements in subdivision 1, a voting system must be certified by an independent testing authority accredited by the Election Assistance Commission or appropriate federal agency responsible for testing and certification of compliance with the federal voting systems guidelines at the time of submission of the application required by subdivision 1 to be in conformity with voluntary voting system guidelines issued by the Election Assistance Commission or other previously referenced agency. The application must be accompanied by the certification report of the voting systems test laboratory. A certification under this section from an independent testing authority accredited by the Election Assistance Commission or other previously referenced agency meets the requirement of Minnesota Rules, part 8220.0350, item L.

(b) A vendor must provide a copy of the source code for the voting system to the secretary of state. The secretary of state may facilitate assessments of the voting system, the source code, and the voting system's cybersecurity protections by an independent third-party evaluator, in cooperation with the vendor, to identify and report election security vulnerabilities. An independent technical expert must promptly notify the secretary of state and vendor about any relevant cybersecurity vulnerabilities discovered through the assessment and provide technical assistance in remedying the vulnerabilities.

(c) A chair of a major political party ~~or the secretary of state~~ may select, in consultation with the vendor, an independent third-party evaluator to examine the source code to ensure that it functions as represented by the vendor and that the code is free from defects. A major political party that elects to have the source code examined must pay for the examination.

(d) Except as provided by this subdivision, a source code that is trade secret information must be treated as nonpublic information, according to section 13.37. A third-party evaluator must not disclose the source code to anyone else.

(e) Before completing a purchase agreement for a voting system with a county or municipality, a vendor must provide the county or municipality with end-of-life and end-of-support dates for systems, devices, or products containing software or upgradable firmware. The vendor must provide timely security updates to a voting system provided to a county or municipality during the agreed-upon period for use of the voting system to maintain the voting system's certification under this section.

Sec. 6. **[209.96] VENDOR NOTIFICATIONS.**

Subdivision 1. **Definitions.** (a) For the purposes of this section, the terms defined in this subdivision have the meanings given.

(b) "Cybersecurity incident" means an event that may indicate that an organization's systems or data have been compromised or that measures put in place to protect them have failed.

(c) "Information security incident" means a targeted attempt or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

(d) "Vendor" means any person or entity that provides, programs, supports, or maintains election services or infrastructure on behalf of the state or unit of local government.

Subd. 2. **Cybersecurity and information security incidents.** (a) If a vendor becomes aware of the possibility of an election cybersecurity incident, including breaches of component suppliers, the vendor must promptly assess whether an election cybersecurity incident has occurred.

(b) If a vendor has reason to believe that an election cybersecurity incident may have occurred, or that an information security incident related to the role of the vendor as an election service provider may have occurred, including breaches of component suppliers, the vendor must notify the secretary of state of the incident in the most expedient time possible and without reasonable delay but in no event may the notice be provided to the secretary of state more than three calendar days after discovery of the possible incident.

(c) If a local election official becomes aware of the possibility of an election cybersecurity incident or information security incident that impacts election data, systems, or infrastructure, the election official must immediately notify the secretary of state.

Subd. 3. **Ownership.** A vendor must notify the secretary of state of any foreign national that directly or indirectly owns or controls a vendor, as well as any material change in ownership resulting in ownership or control by a foreign national.

Sec. 7. **SECURITY EXPERT.**

The secretary of state must engage a security expert to conduct an assessment of the secretary of state's data exchange partnerships with counties, cities, the Department of Public Safety, the Social Security Administration, the State Court Administrator's Office, and organizations governed by Minnesota Statutes, section 201.13, subdivision 3, paragraph (d). The security expert must notify the secretary of state of the assessment's findings and recommend any necessary improvements to increase security and accuracy of data being exchanged.