2026 South Dakota Legislature

Senate Bill 215

Introduced by: ***Senator*** *Peterson (Sue)*

An Act to provide for a pilot program for the implementation of a secured cryptographically end-to-end verifiable voting system in certain jurisdictions.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF SOUTH DAKOTA:

Section 1. There is established the cryptographically end-to-end verifiable election pilot program for the purposes of testing and validating a secured cryptographically end-to-end verifiable voting system for absentee voters and voters under the Uniformed and Overseas Citizens Absentee Voting Act, 52 U.S.C. §§ 20301 to 20311, inclusive (January 1, 2023). No more than three election jurisdictions in this state may participate in the pilot program.

Section 2. Before a jurisdiction may participate in the pilot program, the person in charge of the jurisdiction's elections must receive the approval of the governing body of the jurisdiction. If the governing body approves of the jurisdiction's participation in the pilot program, the person in charge of a jurisdiction's elections must notify the secretary of state:

(1) That the jurisdiction will be implementing a secured cryptographically end-to-end verifiable voting system;

(2) Which system the jurisdiction has selected to implement; and

(3) Which laws may be incompatible with the implementation of the system.

If more than two jurisdictions notify the secretary of state of an intention to participate in the pilot program, the secretary shall determine which jurisdictions are to participate in the pilot program by the order in which the notifications were received.

Section 3. Upon receipt of the notice from the person in charge of the election, the secretary of state and the attorney general shall review the list of laws the person in charge of the elections has indicated may be incompatible with the implementation of the system. If the secretary of state and the attorney general determine that the person in charge of the jurisdiction's elections requests the waiver of a law that is not incompatible with the implementation of the system, the secretary of state and the attorney general must remove

the law from the list of laws to be waived. The secretary of state shall waive the laws that the secretary of state and the attorney general have identified as being incompatible with the implementation of the system within seven days of receiving the notice from the person in charge of the election.

Nothing in this section may be construed to permit the secretary of state the ability to void any of the provisions of this Act. Nothing in this Act may be construed to permit the secretary of state, the person in charge of a jurisdiction's election, or any other person the ability to void, waive, or otherwise suspend any provision of law pertaining to an individual's eligibility to vote, voter registration, citizenship requirements, the requirements for applying to vote by absentee ballot, or the requirements pertaining to the conducting of an election on election day.

Section 4. The secretary of state shall report to the Government Operations and Audit Committee the jurisdictions participating in the pilot program and the laws that have been waived. The secretary's report to the committee is open to public inspection and may not contain any confidential information.

Section 5. Any secured cryptographically end-to-end verifiable voting system must enable a voter to cast a vote for all offices and on all measures on which the voter is entitled to vote.

Section 6. Except for routine testing conducted prior to voting, the neither the person in charge of the jurisdiction's elections nor any other individual may decrypt the election results or ballot tabulation until after the polls have closed for the election conducted as part of the pilot program. A violation of this section is a Class 2 Misdemeanor.

Section 7. If a jurisdiction participates in the pilot program, pursuant to this act, the jurisdiction is not required to provide a paper ballot to any registered voter who applies to vote by absentee ballot.

Section 8. The person in charge of the jurisdiction's elections may not implement or test any system other than a secured cryptographically end-to-end verifiable voting system that uses a single, integrated, and cryptographically end-to-end verified digital system to:

(1) Accurately identify and authenticate each voter;
(2) Generate a voter's ballot;
(3) Encrypt each ballot when the ballot is generated;
(4) Deliver the generated and encrypted ballot to the voter;

(5) Accurately mark the voter's ballot;

(6) Transmit the voter's ballot to the person in charge of the election in a way that is secured and maintains the ballot's encryption;

(7) Provide to a voter a unique, verifiable record that allows the voter to independently confirm that the voter's ballot was received, recorded, and tabulated by the person in charge of the election, without disclosing the voter's selections;

(8) Decrypt each ballot only:

(a) For tabulating the ballot; and

(b) When authorized by the person in charge of the election and a member of the governing body of the jurisdiction in which the election is being conducted, as appointed by the governing body of the jurisdiction;

(9) Provide encryption and tabulation keys as part of the system's multi-party cryptographic security;

(10) Store all ballots transmitted to the person in charge of the election in a manner that maintains each ballot's encryption;

(11) Tabulate the ballots transmitted to the person in charge of the election;

(12) Produce a physical copy of every ballot that may be:

(a) Tabulated by the jurisdiction's automatic tabulating equipment; and

(b) Reviewed as part of the jurisdiction's post-election audit;

(13) Provide, without vendor representation, to the person in charge of the election, a candidate, and any authorized observer, the ability to independently verify the integrity of the election through direct technical and procedural evidence that demonstrates:

(a) That each ballot was not altered;

(b) That all ballots tabulated were generated by a registered voter whose identity was verified and matched to the voter's registration before the ballot was generated;

(c) That no additional ballots were added to the tabulation; and

(d) A complete and immutable chain of custody for each ballot from when the ballot was generated through the tabulation of the ballot; and

(14) Detect and report to the person in charge of the election any attempt by a registered voter to cast multiple ballots.

Section 9. Any entity that applies to have a secured cryptographically end-to-end verifiable voting system used in the cryptographically end-to-end verifiable election pilot program shall agree to:

(1) Host the system on the server infrastructure designated by the person in charge of the election;

(2) Relinquish to the person in charge of the election, ownership of all data and logs associated with the development of the system or generated by the system after the system's implementation and use;

(3) Allow the person in charge of the election the ability to review and audit the system's software source code;

(4) Provide, to the individuals authorized by the person in charge of the election, custody of all encryption and tabulation keys created as part of the system's multi-party cryptographic security; and

(5) Give the person in charge of the election control over the system configuration and activation, and all processes required to:

(a) Tabulate ballots;

(b) Certify the election results produced by the system; and

(c) Audit any election conducted through the system.

Section 10. The person in charge of the jurisdiction's elections may access a system's software source code only to inspect, verify, or conduct a forensic review of the source code, provided that the inspection, verification, or review:

(1) Does not require the ownership of the source code to transfer to the state;

(2) Takes place under controlled and confidential conditions; and

(3) Does not require public disclosure or other notification.

The person in charge of the jurisdiction's elections may not use any access to the system's software source code to develop, modify, or reverse engineer the system's software source code, to authorize any entity other than the owner of the system's software source code to analyze the system's software source code, or to use the system's software source code in any other way that may be construed as commercial exploitation. The person in charge of the jurisdiction's elections may not copy any portion of the system's software source code unless the copy is necessary to conduct an approved audit or forensic review of the system's software source code.

Section 11. The State Board of Elections shall promulgate rules, pursuant to chapter 1-26, to establish the process by which a jurisdiction participating in the pilot program, conducts absentee voting using a cryptographically end-to-end verifiable election system.

Section 12. Any waiver approved pursuant to section 3 of this Act applies only to the jurisdiction named on the waiver application and expires on December 31, 2028.

Section 13. This Act is effective beginning January 1, 2027.

Section 14. The provisions of this Act expire on December 31, 2028.