House Bill 25-470

By Senator(s) Harrison
also Representative(s) Wood, Spencer, Jenkins, Vasquez

AN ACT

CONCERNING THE ADOPTION OF ONLINE VOTING

Be It Enacted by the General Assembly of the State of San Andreas:

SECTION 1. SHORT TITLE.
This Act shall be known and may be cited as the "Online Voting Implementation Act of 2025."

SECTION 2. FINDINGS AND PURPOSE.
The General Assembly finds and declares:
(a) That expanding access to elections is vital to democratic participation, and modern technology can facilitate more convenient access while maintaining integrity.
(b) That other jurisdictions and research (e.g. cryptographic voting systems, verifiable online voting designs) show that secure, end-to-end verifiable election systems are technically feasible (see e.g. "Towards end-to-end verifiable online voting" research).
(c) That implementing statewide online voting requires sufficient lead time, infrastructure, oversight, auditing, and transitional support.
(d) That beginning in November 2026 ensures that there is adequate time for testing, certification, public education, and fallback provisions.
(e) That the State has a compelling interest in ensuring voter security, fraud prevention, access (including for persons with disabilities), auditability, and public confidence in the electoral process.
(e) Therefore, the purpose of this Act is to require that all elections statewide include an option for secure online voting systems, with appropriate safeguards, audits, fallback options, and transition measures.

SECTION 3. DEFINITIONS.
In this Act, unless the context otherwise requires:
(a) "Election" includes all primary, general, coordinated, special, recall, and referendum elections held statewide under state or federal law.
(b) "Online voting" means the casting, submission, and receipt of votes over the internet or other digital networks by qualified electors.
(c) "Qualified elector" means a person eligible to vote in the state under existing law.
(d) "Election authority" means the Secretary of State and local county (or municipal) election officials.

Signed by Governor Isabel Payne and adopted into law on November 6, 2025

(e) “Verifiable voting system” means a cryptographic or algorithmic method by which each voter can verify that their vote was (a) recorded as cast, (b) included in the tally, and (c) counted correctly, while preserving ballot privacy and preventing double-voting.
(f) “Audit log” means a publicly viewable record or cryptographic commitment or hash chain that allows third parties to verify election integrity.
(g) “Fallback voting” means alternative secure voting means (e.g., in-person, paper ballot) to be used if system failure occurs.
(h) “Oversight commission” means the Online Voting Oversight Commission established under Section 6.
(i) “Certification” means the process by which a voting system is tested, certified, or approved by the Secretary of State (or designated independent testing authority) to meet security, reliability, accessibility, and verifiability standards.

SECTION 4. EFFECTIVE DATE AND TRANSITION.
(a) This Act takes effect immediately for the purposes of planning, rulemaking, budgeting, and preparations. Notwithstanding other provisions, the first statewide election held under this Act shall be the November 2026 general election.
(b) The Secretary of State, in collaboration with the oversight commission and local election authorities, shall adopt rules and standards no later than two (2) calendar months after this bill is signed by the Governor to implement the system.
(c) During the transition period (from enactment through November 2026), the State shall run pilot programs in selected counties (or districts) for prior elections (e.g. municipal or local) using the proposed online voting system to test and validate procedures, security, performance, and public acceptance.

SECTION 5. MANDATORY ONLINE VOTING IN ALL ELECTIONS.
(a) For all elections conducted on or after November 2026, all qualified electors shall have an option to cast their ballots via the online voting system, in addition to paper ballots, unless forced to use fallback procedures under system outage provisions (see Section 7).
(b) The Secretary of State shall provide to all voters:
(I) Secure login / credentialing (e.g. multi-factor authentication) to the online voting system;
(II) An interface (web, mobile) that is accessible (e.g. for voters with disabilities, blind/low-vision, etc.);
(III) A means by which the voter can verify that their vote was correctly recorded (e.g. voter receipt, cryptographic verification) without compromising ballot secrecy;
(IV) A mechanism to allow a voter to “challenge” or review their ballot before final submission;
(V) Public documentation of the system’s security architecture, audit logs, and open-source components where feasible (subject to security constraints).
(VI) The system design must ensure that no voter’s identity or credentials can be linked to their ballot once cast (i.e., preserve anonymity).
(VII) The system must prevent double-casting (i.e. prevent a voter from voting more than once) and detect and reject invalid votes.

(VIII) The results of the election shall be tabulated in a manner that allows external audit and verification (see Section 8).
(IX) Local election authorities shall coordinate with the Secretary of State to manage the online voting infrastructure (servers, networks, redundancy, cybersecurity) and provide support to voters (help lines, assistance, fallback voting centers, etc.).

SECTION 6. ONLINE VOTING OVERSIGHT COMMISSION.
(a) There is hereby established the Online Voting Oversight Commission (OVOC)
(b) Membership. The commission shall consist of:
(I) Two members appointed by the Governor (with at most one from the same party);
(II) Two members appointed by the President of the Senate;
(III) Two members appointed by the Speaker of the House;
(IV) One member appointed by the Chief Justice of the State Supreme Court;
(V) One member appointed by the Secretary of State (ex officio, nonvoting).
(VI) Must be equally divided between political party affiliations.
(b) The commission's duties include:
(I) Advising on system design, security, privacy, and accessibility;
(II) Reviewing and approving certification standards;
(III) Recommending rule amendments;
(IV) Overseeing independent audits and post-election reviews;
(V) Hearing and adjudicating disputes related to the online voting system;
(VI) Publishing periodic progress reports and audit summaries to the public.
(VII) The commission shall have the authority to engage independent cybersecurity, cryptography, and election technology experts to conduct reviews, penetration testing, and audits.
(c) Commission members shall serve for staggered terms, and may be reappointed, subject to conflict-of-interest rules.

SECTION 7. SYSTEM OUTAGE, FAILOVER, AND EMERGENCY VOTING.
(a) If, at any time during the voting period (or on election day), the online voting system suffers a partial or full outage, denial-of-service attack, or other failure that materially impairs access, local election authorities shall activate fallback voting procedures.
(b) Fallback voting shall include secure in-person voting centers (e.g. paper ballots, provisional ballots), supervised and connected to election officials, with extended hours as needed to compensate for lost online access time.
(c) Notification to the public of a system outage must be immediate (via email, SMS, state websites, press) and include instructions for fallback voting.
(d) An official incident report must be filed within 24 hours by the election authority, documenting the cause, mitigation, steps taken, and post-incident review.
(e) The oversight commission shall review all outages and recommend system hardening and improvements.

SECTION 8. AUDIT, VERIFICATION, AND TRANSPARENCY.

(a) After each election, the Secretary of State shall publish:

(I) Aggregate cryptographic commitments, hashes, or public audit logs;

(II) Summary reports showing total votes cast, participation metrics, rejected ballots, system performance metrics;

(III) A redacted (to maintain ballot secrecy) log that allows third-party verification of tallies.

(IV) At least one percent (1 %) of all ballots cast shall be independently audited via end-to-end verification, cross-checked with cryptographic receipts, and compared against system tallies.

(V) The oversight commission shall contract independent auditors (including academic or nonprofit election technology experts) to conduct penetration tests, source code inspection (if open-source), review incident reports, and issue audit certificates.

(b) The certification process (Section 10) must require that the system preserve all necessary logs, cryptographic proofs, and auditability features for a legally mandated retention period (e.g. 5 years).

(c) Any discrepancy or anomaly discovered during the audit must trigger an investigation. If system-wide error or fraud is confirmed, the oversight commission may order a partial or full election rerun under fallback (paper) procedures.

SECTION 9. VOTER EDUCATION, SUPPORT, AND ACCESSIBILITY.

(a) The Secretary of State shall conduct a statewide public education campaign (online, mailers, TV/radio, community outreach) at least 7 months prior to the first online voting election, to inform voters how to use the system, security features, fallback procedures, access assistance, and verification steps.

(b) Local election offices shall provide training to staff, help desks, drop-in support centers, and hotlines.

(c) The online voting interface shall comply with all accessibility requirements (e.g. Americans with Disabilities Act, Web Content Accessibility Guidelines [WCAG], screen-readers, adjustable text size, language translation).

(d) For voters without reliable internet access or devices, the election authority shall (during the voting period) provide in-person access centers (computers/tablets), staffed assistance, secure connections, and remote assistance.

SECTION 10. CERTIFICATION, STANDARDS, AND SECURITY.

(a) No online voting system may be used until it has been certified under standards promulgated by the Secretary of State (with oversight commission review).

(b) Certification standards must include:

(I) Resistance to tampering, hacking, denial-of-service, and insider attacks;

(II) End-to-end cryptographic verifiability;

(III) Ballot secrecy and unlinkability;

(IV) Protection against double-voting;

(V) Secure identity verification / authentication;

(VI) Secure key management, encryption in transit and at rest;

(VII) Source code inspection (where possible) or independent review;
(VIII) Disaster recovery, redundancy, backup systems, and failover design;
(IX) Penetration testing, code audits, continuous security review;
(X) Logging, cryptographic audit trails, tamper-evident records;
(XI) Secure infrastructure, monitoring, intrusion detection, network segmentation.
(XII) Certification must be renewed periodically (e.g. every 2 years) or after major updates.
(XIII) Any upgrades or patches to the system must undergo review and, if substantive, re-certification.
(c) The Secretary of State must maintain a list of pre-approved vendors, open-source solutions, and approved third-party components.
(d) The oversight commission has the authority to suspend use of the system if a certified system is found deficient or compromised, reverting temporarily to fallback voting until issues are resolved.

SECTION 11. FUNDING AND APPROPRIATIONS.
(a) The State shall appropriate necessary funds to the Secretary of State (and local election authorities) to design, build, test, certify, deploy, maintain, and support the statewide online voting infrastructure.
(b) Local election authorities shall receive grants or reimbursements for infrastructure upgrades (network, security, staffing, training, fallback facilities) to support the transition.
(c) The State may utilize federal grants or private-public partnerships (with strict oversight) to fund the implementation, provided no compromise of security or independence arises.
(d) The budget shall include funds for cybersecurity audits, third-party oversight, public education, and contingency reserves.

SECTION 12. LEGAL PROTECTIONS, LIABILITY, AND PENALTIES.
(a) The Secretary of State, oversight commission, vendors, contractors, and election authorities shall carry liability shields for good-faith operation, subject to gross negligence or willful misconduct.
(b) Any person who maliciously tampers with, hacks, or interferes with the online voting system shall be subject to criminal penalties consistent with election fraud statutes.
(c) Election records, logs, cryptographic proofs, and audit data shall be preserved for at least 5 years (or as required by state law), and shall be accessible to oversight commission and certified auditors.
(d) If an election is invalidated due to system failure or fraud, a court may order a rerun of the affected portion or entire election, using fallback voting, at the expense (where feasible) of responsible parties (vendor, contractor, or election authority).

SECTION 13. SEVERABILITY AND CONFLICT.
If any provision of this Act is held invalid or unconstitutional, such invalidity does not affect other provisions that can be given effect, and to that end the provisions of this Act are severable. If any provision conflicts with existing state constitutional or statutory provisions, the

constitutional provisions prevail, and the legislature or courts may revise or limit implementation as required.