Shirley N. Weber, Ph.D.
California Secretary of State
Office of Voting Systems Technology Assessment
1500 11th Street, 6th Floor | Sacramento, CA 95814 | 916.695.1680 | votingsystems@sos.ca.gov

August 27, 2025

County Clerk/Registrar of Voters (CC/ROV) Memorandum #25073

TO: All County Clerks/Registrars of Voters

FROM: /s/ Rodney Rodriguez
Information Technology Supervisor II, OVSTA

RE: Statewide Special Election: Voting Technology Security

California's voting technologies are developed and implemented with security as a fundamental principle. Accordingly, the following are important reminders regarding our security processes and procedures:

- Any modifications to a voting system or remote accessible vote by mail system must be authorized by the Secretary of State (Elec. Code, §§ 19216, 19217, 19218, and 19291).
- Any modifications to a certified electronic poll book must be authorized by the Secretary of State (Cal. Code Regs., tit. 2 § 20159)
- Any change to the equipment, procedures, or facility of a certified ballot printer, or the equipment or procedures of a certified ballot on demand system, must be authorized by the Secretary of State (Cal. Code Regs., tit. 2, §§ 20230 and 20267).
- Tampering with, interfering with, or attempting to interfere with a voting system, or portion thereof, is a felony (Elec. Code, § 18564).
- California conducts source code review, penetration testing, open-ended vulnerability testing, and operational testing to validate system performance to ensure vulnerabilities are identified and addressed prior to certification and use.
- Registered voters receive a paper ballot, ensuring voters can review their choices prior to ballot casting, establishing a voter-verified paper audit trail, and providing elections officials an auditable record to confirm the accuracy of tabulation.

- California voting systems and tabulators are never connected to the internet, do not electronically transmit or receive election data through an external network, nor do they contain modems or hardware that could be remotely "activated."

- California voting technologies are equipped with physical security controls and safeguards to prevent unauthorized access or tampering.

- California voting systems are installed exclusively using the trusted build software provided by the Secretary of State.

- Before each election, every county must validate that the voting system is identical to the Secretary of State supplied trusted build, either by 1) reinstalling the trusted build, or 2) utilizing the Secretary of State trusted build cryptographic hash algorithms (a digital fingerprint that uniquely identifies software and firmware) to ensure it has not been modified.

- Ballot printers are certified by our office and regularly inspected.

- Vendors and county elections officials follow strict physical security and chain of custody requirements for all voting technology software, firmware, and hardware.

- If the chain of custody to any part or component of a certified voting technology has been compromised, breached, or attempted to be breached, the Secretary of State must be notified immediately, and investigation, verification, and sanitization procedures must be followed (Elec. Code, § 17603(b)).

- County election officials follow specific role-based permissions following the principle of least privilege, administrative and management controls, access controls, security procedures, operating procedures, and personnel screening.

- Minimum password complexity, length, strength, and lockout policies for failed attempts are required. Under no circumstances may default passwords be used.

- For every election, each county must perform the required, voting technology specific, pre-election logic and accuracy testing.

- For every election, each county must conduct a post-election audit by manual tally to identify and resolve any discrepancies.

Questions regarding this CCROV should be submitted to the Office of Voting Systems Technology Assessment (OVSTA) at VotingSystems@sos.ca.gov or (916) 695-1680.