SHIRLEY N. WEBER, Ph.D.
CALIFORNIA SECRETARY OF STATE
Office of Voting Systems Technology Assessment | 1500 11th Street, 6th Floor
Sacramento, CA 95814 | **Tel** 916.695.1680 | www.sos.ca.gov

May 6, 2022

County Clerk/Registrar of Voters (CC/ROV) Memorandum # 22105

TO: All County Clerks/Registrars of Voters

FROM: /s/ Susan Lapsley
Deputy Secretary of State, HAVA Director and Counsel

RE: OVSTA: Voting Technology Security

Security is layered into every aspect of California's voting technology. Our office, in partnership with county election offices, take election security very seriously. The following are reminders regarding security processes and procedures:

- California conducts source code review and evaluation, hardware and software security penetration testing, open ended vulnerability testing, operational testing to validate system performance and functioning under normal and abnormal conditions and more to identify any vulnerabilities and have our voting systems resolve or mitigate them.

- Every California registered voter receives a paper ballot – which creates a voter-verified paper audit trail that provides voters an opportunity to review their choices when casting their paper ballot and provides elections officials with a means to confirm the accuracy of tabulation.

- California voting systems and tabulators - ARE NOT connected to the internet, nor do they have modems or hardware in them that could be remotely "activated."

- California voting systems have physical intrusion prevention security controls and safeguards.

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

- Every county must validate - before every election - that the voting system is identical to the Secretary of State supplied trusted build by reinstalling the trusted build or utilizing the Secretary of State trusted build cryptographic HASH (essentially a digital fingerprint of the software and firmware) to ensure it matches the approved version and has not been modified.

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

- Vendors and county officials follow strict physical security and chain of custody requirements for all voting technology software, firmware and hardware which meet or exceed federal guidance including that of the Justice Department, the Cybersecurity and Infrastructure Security Agency and the Election Assistance Commission.

- If chain of custody has been compromised or attempted to be breached, the Secretary of State must be notified immediately, and investigation, verification, and sanitization (e.g. NIST Media Sanitization guidelines https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final) procedures be followed.

- County election officials must follow specific role-based permissions, administrative and management controls, access controls, security procedures, operating procedures, physical facilities and arrangements controls, and organizational responsibilities and personnel screening.

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

- Every county performs logic and accuracy testing.

- For every election, each county must conduct an audit by manual tally or risk limiting auditing to identify and resolve any discrepancies.

Chain of Custody

The Secretary of State mandates voting system vendors, security consultants and county officials follow strict chain of custody requirements for voting system software, firmware and hardware throughout testing, certification, and operation. Voting system software, firmware and hardware is used at the jurisdiction in a process-controlled environment where chain of custody and software integrity is strictly controlled.

Counties must adhere to the security and chain of custody requirements in the certified Use Procedures, Certification document, and state law. If the chain of custody of voting technology has been breached, jurisdictions are required to notify the Secretary of State immediately.

Further, pursuant to California Elections Code Sections 19216,19217 and 19218, any modifications to a voting system, including additions, and/or deletions of certified firmware, software, or hardware, must be authorized by the Secretary of State. No addition and/or deletion of voting system components are allowed unless authorized and provided by our office.

Below are additional California Elections Code sections and California Code of Regulation sections that further protect voting systems from unauthorized access:

- Pursuant to Elections Code section 18564.5, tampering with a voting system is prohibited.

- Pursuant to California Code of Regulations section 20820 (e), during recounts, unauthorized parties are prohibited from “touching any voting system components, ballots, tally sheets, or other special recount board materials.”

We are in regular contact with and work closely with federal and state law enforcement and intelligence agencies to ensure we protect our elections. Should anyone attempt to interfere with our election, we will work with state and federal law enforcement agencies to prosecute them to the full extent of law and hold them accountable.