CONTRA COSTA COUNTY
ELECTIONS DIVISION
www.cocovote.us
ContraCostaElections

FACT SHEET

Topic: Election Security

Four Pillars of Election Security

- Securing Facilities
- Securing Networks
- Securing People
- Securing Processes

Facilities

- Physical security assessments are conducted regularly.
- Designated high security areas have limited access to only authorized employees; proximity access cards are used to limit access to necessary staff.
- Election areas are secured with alarm systems with limited access and 24/7 motion-detection video surveillance.
- Access to the voting system is password-protected and all activity is logged by the voting system. Administrative passwords are only known by designated elections officials.
- The Elections Division maintains positive partnerships with security agencies and law enforcement at the Federal, State, and local levels to provide safe, secure, and transparent elections for our residents and jurisdictions.
- Observers and other members of the public are escorted and supervised at all times.
- Emergency and disaster planning is conducted to ensure ballots and equipment are secure in the event of an emergency.

Networks

- Multi-factor Authentication is present on all systems and a robust password policy is in place.
- Cybersecurity awareness, phishing, and other cyber trainings are required for all staff.
- Voting systems are NEVER connected to the internet or the county network; internet capabilities are deactivated at the BiOS level. Computers within a voting system are only connected to one another.
- USB Ports on systems are sealed to prevent access.
- The voting system is physically restricted under lock and key and only authorized personnel are allowed access; proper chain of custody protocols are observed.
- The “Trusted Build” – the certified software and firmware which controls the voting system and is required to conduct an election - is received directly from the Secretary of State and reinstalled before each election.
- Firewalls, virus blocking software, and active monitoring are used on all systems connected to the VoteCal Statewide Voter Registration Database.

People

- All Elections staff, both permanent and temporary, must take an Oath of Allegiance and pass a background check with fingerprinting. ID Badges must be worn at all times.
- All staff are trained and supervised in safety, security, election code, policy and procedures, and best practices.
- Chain of custody policies are followed by requiring a two-person rule at all times with all ballots and voting equipment.
- Observers are identified with unique ID badges, are escorted by staff, and are never left unsupervised. Observers must acknowledge and follow all Observer Rules and shall not interfere with the election process.
- Staff follow standard uniform operating procedures throughout the department.
- Election officials remain vigilant with security, staying abreast of emerging trends/threats, and continuing with ongoing efforts to safeguard their voting systems and election operations.

Processes

- Elections are designated as “critical infrastructure” by the Department of Homeland Security.
- Adherence to California Elections Code, administrative regulations, and local ordinances are strictly enforced and followed.
- Voting systems that counties use to count ballots must be certified by the California Secretary of State under one of the most strenuous testing and certification programs in the country.
- Voting system security is a multi-layered process with multiple factors, multiple checkpoints, multiple people, and multiple systems that makes systematic fraud nearly impossible.
- Voting systems are a paper-based, optical scan ballot system.
- Election staff ensure that specific procedures for programming, deployment, and use of voting equipment during elections are met.
- Strict chain of custody procedures, two-person teams, and ballot inventory controls are required.
- E-pollbooks at polling places have real-time access to the voter database, ensuring a voter is only able to vote once.
- Vote-by-Mail ballots go through a signature verification process for ballot security; a voter is given the opportunity to “cure” his or her signature if a signature is missing or declared a mismatch to the voter’s registration record.
- Mandatory pre-election Logic and Accuracy testing ensure tabulation equipment is counting ballots accurately, and a post-election 1% Manual Hand Tally ensure the paper ballots have been properly tabulated and reported.
- Ballots and other canvass materials must be kept secure for 22 months after the election.