Election Security Safeguards

The Coalition of Bay Area Election Officials partnered with the Cybersecurity and Infrastructure Security Agency (CISA) to implement resources for securing all aspects of election infrastructure.

Securing **NETWORKS**

- Vote counting system is not connected to the internet
- Networks in high-security locations only
- Robust backup and patching policies
- Password policy
- Ports on systems are sealed to prevent access
- Multi-factor authentication
- Cybersecurity awareness, phishing and other trainings for all staff
- Cyber hygiene vulnerability scans
- Internal/external system testing
- Monitor and track system changes
- Apply principal of least privilege access
- Hardened networks
- Multiple firewalls, network segmentation
- Intrusion detection system (active intercept)
- VoteCal Statewide database

Securing **FACILITIES**

- Physical security assessment
- Designated high security areas
- Staff only access areas they need to do their jobs
- ID badges, access control, log
- Alarm systems and/or 24/7 video surveillance
- Partnerships with local law enforcement
- Security and ADA assessments of all voting locations
- Separate entrances for staff and public observers
- Visitors and observers escorted
- Tamper evident seals / security features
- VBM ballot drop boxes (bolted to concrete)

Securing **PROCESSES**

- Elections designated as “critical infrastructure” by Homeland Security
- Always two people with the ballots
- Chain of custody protocols, access management
- Voting systems must be certified by the SOS prior to being used at any election
- “Trusted build” version of software must be reloaded before each election
- Paper-based, digitally scanned vote system
- Pre-election logic and accuracy testing
- Post-election audits to confirm equipment operated correctly
- Paper ballots stored for 22 months
- VBM ballot security, bar codes, signatures verified, signature cure process
- E-poll books — real time access to registration data and voter history
- Conditional Voter Registration

Securing **PEOPLE**

- Oaths of Allegiance and/or background checks of all staff
- Training and supervision on safety, security, election codes, and procedures
- Staff only access those systems they need to do their job
- Periodic training on phishing and cybersecurity best practices
- Two-people are always with ballots and voting equipment
- Observers and tours — transparency of our processes
- Emergency planning — prepare for fire, flood, PSPS, earthquake, etc.
- Visitors and observers identified with unique badges
- Observers must review and agree to observer rules prior to access
- Staff follow standard uniform operating procedures across the department

CISA Resources

#TrustedInfo2022

- Election Security Snapshot
- Physical Security Walkthrough
- EI-ISAC Membership
- Election Emergency Response Guide
- Risk and Vulnerability Testing
- Vulnerability Scanning
- Remote Penetration Testing
- Albert Sensors