COALITION OF
BAY AREA ELECTION OFFICIALS

Website: www.bayareavotes.org
Facebook: Bay Area Votes

Voting Systems & Security

Election Security Overview

Election security is a major concern at all levels of government. Elections have been designated as critical infrastructure of this Country by Federal Homeland Security.

The end goal of election security is to deliver a process that is not only safe and secure, but also fair, accurate and accessible. In California, at both the state and county level, there are a multitude of layered security protocols in place.

What is a voting system and why should I trust it? (and other things my mother never told me about elections)

At its core, a voting system facilitates ballot design, ballot tabulation, and reporting of election results. It may also include ballot manufacturing or printing (commonly known as "ballot on demand"), and ballot marking technologies for voters with disabilities or voters in the military or living overseas. A voting system does not manage voter registration, candidate filing, incoming vote-by-mail processing, or signature checking, to name a few of the election-related responsibilities which are facilitated by other systems.

Voters should be aware that the systems counties use to count ballots are certified for use by the California Secretary of State. The state has developed one of the most strenuous voting systems testing and certification programs in the country. Voting technology in California, must be certified for use by the Secretary of State, prior to being sold and/or used in any California election. New voting systems applying for certification must undergo months of extensive testing before they can be used by counties to tally votes.

While the hardware is delivered from the voting system vendor to a county, the software which controls the system software and is used to conduct an election is delivered directly from the Secretary of State into the hands of the Elections Official; Only the Secretary of State-supplied "trusted build" (the certified version of the software and firmware) for any voting system shall be installed by counties and must be reinstalled prior to any election.

At the local level, California counties are required to abide by stringent sets of rules and regulations regarding implementation and use of a voting system. A few notable rules and regulations include:

- The voting system used is a paper-based, digital scan ballot system.
- The voting system is NEVER connected to the internet or county network.
- The voting system is physically restricted under lock and key; only authorized personnel are allowed in the area.
- Strict chain of custody procedures and ballot inventory controls are required.
- Access to the voting system is password-protected and all activity is logged by the voting system. Administrative passwords are only known by necessary elections officials.
- Election staff ensure specific procedures for programming, deployment, and use of voting equipment during elections are met.

- Prior to counting, counties are required to perform a logic and accuracy test of the ballots and voting system to ensure votes are tabulated accurately.
- After Election Day, counties are required to perform a 1% manual hand tally (audit) of the votes as part of our official canvass process, which confirms that the voting system accurately tabulated and reported votes cast.
- If any part or component of a voting system for which the chain of custody has been compromised, the security or information has been breached, or attempted to be breached, the Secretary of State requires immediate notification, and that an investigation, verification, and sanitization protocol be followed.

Saying that voting systems are impenetrable and impervious to vulnerabilities and bad actors is like saying that the Titanic is unsinkable. Election officials remain vigilant with security and employ many other safeguards to their voting systems and election operations.

<u>What other safeguards and security measures do county election offices use?</u>

After the 2016 Presidential Election, Elections were declared to be critical infrastructure by the Department of Homeland Security. Other critical infrastructure sectors include Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare and Public Health, Information Technology, Nuclear Reactors/Materials/Waste, Transportation Systems, and Water and Wastewater Systems.

As a result, the federal government is able to provide resources to support counties in their efforts to employ security measures during the course of an election. The Election Infrastructure subsector is part of the Government Facilities sector and covers a wide range of physical and electronic assets such as storage facilities, polling places, and centralized vote tabulations locations used to support the election process, as well as information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments.

Support is provided in four primary areas:

- Networks & Systems
- Facilities
- Processes
- People

Counties have worked with various agencies such as the FBI, DHS, Cybersecurity and Infrastructure Security Agency (CISA), and the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC), serving as national clearinghouses for counties across the nation to keep abreast of pertinent cybersecurity issues happening across the country. Recently, the federal DOJ has worked with election officials to report and investigate threats made to election officials. The California Secretary of State office has been instrumental in bringing awareness and sharing "best practices" with counties on physical security and cybersecurity.

County election offices are targets for intrusion by foreign actors or others attempting to subvert elections. While voting systems are never connected to the Internet, county networks are subjected to cyber-hygiene scanning and penetration testing for vulnerabilities, so systems can be hardened with multiple firewalls and monitoring tools to prevent unauthorized access by bad actors. Staff training is provided along with cybersecurity awareness training regarding emails with links and emails used to attack the local county network or website for ransomware payments.

In the same fashion, tried and true physical security measures are utilized to prevent authorized access to critical functions of the election. These include video monitoring, alarm systems, and card access systems. High security areas include the ballot tabulation room, where ballots are staged for voting locations, and where vote by mail (VBM) ballots are signature-checked and stored before and after counting. Check-in log sheets are completed and maintained for visitors, vendors, and observers when they visit or access the election office.

The majority of key election processes are regulated by state law and election code, whether it be performing voter registration duties, the voting system regulations and use procedures listed earlier, the processing of VBM ballots, checking voters in at a voting location on Election Day, chain of custody and ballot accounting processes, and ending with the official canvass before the election is certified. All of these contribute to the integrity of an election.

Lastly, elections involve people. Permanent and temporary staff must pass background checks before hire. They are given access only to their areas of responsibility and the two-person rule is utilized in the presence of ballots at all times. In this way, election workers are the eyes and ears to ensure that systems are not compromised, that buildings are secure, and that procedures are properly followed.

While a voting system with unfettered access could have vulnerabilities to be exploited, it is the combination of security of systems, facilities, processes, and people that greatly reduce the risk of unauthorized access.

Latest threats to elections: Mis-, Dis-, and Mal-Information (MDM)

Since the 2020 Presidential Election, election officials across the nation have contended with mis-, dis-, and mal-information regarding unfounded false claims regarding elections. These threats may erode public trust in our elections and the democratic process in how we elect our representative leaders. Truth, transparency, and trust in election are vital to the validity of results and transfers of leadership.

To respond to these false claims about elections, expanded voter education and outreach efforts are being made to bring greater awareness of the election processes and to make our operations ever more transparent for the public to observe.

Our message to the public: “Election officials, who are non-partisan and apolitical, are the trusted source of election information”. We want the public to reach out to us if they have questions or concerns about an election or election process.