SAN JOAQUIN COUNTY REGISTRAR OF VOTERS 2023 FACT SHEET

Mission Statement

- ☑ To facilitate voter registration and encourage participation among all eligible voters
- ☑ To conduct fair, impartial, accurate, secure, transparent, and accessible elections
- ☑ To serve every person with the highest level of integrity and efficiency
- ☑ To be stewards of public confidence and trust

Motto

Integrity Transparency Commitment Teamwork

The San Joaquin County Registrar of Voters staff strives for the highest standards in elections administration. For any questions about any material found within this guide, please contact our office by phone at (209) 468-VOTE (8683) or by email at Registrar@sjgov.org.

Disclaimer

This document and the information contained herein is provided as of May 24, 2023. The contents of this document are intended solely for informational purposes and should not be interpreted or used as legal advice. The information is based on the circumstances and legal principles in effect as of the date mentioned above.

Please note that laws, regulations, and circumstances can change frequently, and the document is not necessarily updated or revised in light of those changes. Consequently, the information may not reflect recent developments in the law. Before making any decisions based on the information provided in this document, we strongly recommend that you consult with a qualified legal professional or expert in the field relevant to your inquiry.

FACTSHEET

Topic: In-Person Voting

Be an Informed Voter

- San Joaquin County is a traditional polling place county and has not adopted the VCA model.
- Review your County Voter Information Guide. It includes detailed information concerning voting options, times and places.
- Go to the San Joaquin County Elections website at Registrar of Voters (sjgov.org)

Voters Still Have the Option to Vote in Person

- While AB37 and CA Elections Code § 3000.5 requires that all active registered voters receive Vote by Mail (VBM) ballots, voters still have the option of voting in person on Election Day.
- Voters can visit the County Elections Office beginning 29 days before the election and cast their ballots in person up to and including Election Day.
- Refer to the county voter information guide for more specific information.

Reasons a Voter May Want to Vote in Person

- Voter did not receive or lost their VBM ballot and needs a replacement ballot.
- Voter missed the registration deadline or recently moved into the county and must appear in person to complete Conditional Voter Registration, and/or vote provisionally.
- Voter has moved within the county and needs to update their residence address to vote on all the contests they are entitled to vote on.
- Voter desires to use the accessible voting equipment at voting locations to cast their ballot independently and confidentially.
- Voter needs language assistance.
- Voter wants to personally hand in his/her VBM ballot to an election worker at a voting location.
- Voter simply prefers to vote in person.

Main Differences Between Polling Place and Vote Center Operations

- Number of locations and days of operation. In general, there are more polling places than vote centers, but vote centers are open for multiple days before Election Day.
- Some vote centers are open 10 days before the election, with all vote centers open beginning 4 days before and including Election Day.
- Polling places are typically open on Election Day only, but counties may have early voting locations open on some days leading up to the election.
- While vote centers allow a voter to go to any voting location throughout the county, technology at polling places allow counties to have all ballot styles available electronically and the ability to check on a voter's VBM ballot status.

Similarities between Polling Places and Vote Centers

- All polling places and vote centers throughout the state are open from 7am to 8pm on Election Day.

- Polling places and vote centers are both subject to the same accessibility requirements to have accessible voting equipment for voters with disabilities.
- The assistive ballot marking device accommodates voters with visual impairments by presenting the ballot in audio format during an accessible voting session. Headsets provide voters with audio instruction to perform all actions, such as selecting language, adjusting volume and speed of ballot, and reviewing, editing, or changing a write-in selection. A handheld device can be used by a voter during an Accessible Voting Session to navigate through and make selections on their ballot.
- Voters may also take advantage of curbside voting or drive-thru options at select voting locations. These options allow voters to request, mark, and return a ballot from the convenience of their car.
- Polling places and vote centers are subject to the same language requirements, with printed ballots in federally-required languages and translations in other languages to assist with voting.
- At both polling places and vote centers, first time voters whose registrations were not verified by the DMV or Social Security Administration will be required to show a current valid photo I.D. when checking in to vote.
- Polling places and vote center election workers utilize the same chain of custody procedures, two person teams, and security measures to maintain the integrity of the election.
- Whether you vote at a polling place or vote center, your votes are safe with us!

Be Sure Your Voter Registration is Up-to-Date

- Check your voter status at https://voterstatus.sos.ca.gov/
- To update your voter status, re-register at https://registertovote.ca.gov/
- To track your VBM ballot, sign up at https://wheresmyballot.sos.ca.gov

Develop your Personal Voting Plan

- Voting the ballot you are sent is an easy and safe way to vote. It allows you to vote on your own schedule.
- If you are voting by mail, be sure to sign your VBM return envelope and drop it in the mail, a VBM ballot drop box, or deliver it in person at a voting location on or before Election Day.
- If you need specific assistance or wish to vote in person, you can go to your assigned polling location. Locations, dates, and times will be in the County Voter Information Guide or posted on the San Joaquin County website. Election day hours will always be 7:00 a.m. to 8:00 p.m.

FACTSHEET

Topic: Voting by Mail

VBM (Vote by Mail) Has Been Around for Over 20 Years

- The permanent VBM program has been in place since 2002. Over the past 20 years, the percentage of voters that vote by mail has evolved from 27.08% (2002) to 86.72% (2020). Voters have demonstrated that by-and-large, they prefer voting by mail.
- Today, AB37 requires counties to mail a ballot to every active, registered voter in California, while still retaining the option to vote in person.
- Over the past 20 years, the procedures to safeguard VBM voting and make voting easier have matured into a robust, secure process.

VBM Essentials: Sign, Seal, Deliver

- Sign: Remember to sign your VBM return envelope before sending it. It must be signed in order to be counted. Your signature must compare to your signature on file with us, which is often the signature on your driver's license.
- Deliver: You can return your VBM ballot by mail, by VBM Drop Box, or personally at any in-person voting location on Election Day.
- Voters who have received a Vote-By-Mail (VBM) ballot but opt to vote in-person have the liberty to do so. You can either surrender your VBM ballot at your local polling location or choose to retain it. Please note that once you cast your vote in-person, your VBM ballot will be deemed invalid.
- Voters may designate an individual to return their VBM ballot. Be sure it is someone you know and trust. They should sign the appropriate space on the return envelope.

VBM is Safe and Secure

- VBM is a highly regulated process. Systematic fraud is nearly impossible due to the number of multiple factors, checkpoints, people, and systems that coordinate to keep your vote safe.
- Safeguards are in place to eliminate or prevent fraud. Ballots cannot be forwarded by the USPS. If you move and you don't update your address, your ballot will be returned to the election office, and you will have to take action. You will need to vote in person or contact your local elections office for a replacement ballot.
- VBM ballot return envelopes are assigned unique ID numbers, including re-issued ballots, to ensure that voters only vote once.
- Ballot Tracking: Voters can track their VBM ballot to know when it is mailed, received, and processed by the county elections office. This provides a voter

greater transparency on where their ballot is during the election process. Sign up at the Secretary of State's office (https://wheresmyballot.sos.ca.gov).

- VBM ballots are retrieved with strict chain-of-custody procedures and two- person teams pick up ballots from the post office or VBM ballot drop boxes daily.
- Signature Comparison: VBM ballot envelopes are required to be signature verified to the voters' signatures on file.
- Cure Process: Letters are sent to voters who failed to sign the return envelope or whose signatures do not compare, to give the voter the opportunity to "cure" their VBM challenge status. Voters have up until certification to cure their challenged VBM status.
- Safeguards are in place to prevent voting twice, such as voting by mail and then trying to vote in person on Election Day. Only the first ballot received is counted and KNOWiNK Poll Pad technologies are in place to notify the polling place if a voter has already returned a VBM ballot.
- Safeguards also detect if a voter voted twice: first in one county and then in another county.
- Elections operations use advanced auditing measures during the canvass to assure systems tallied the votes correctly.

VBM is Convenient

- VBM ballots are required to be mailed at least 29 days before the election, allowing ample time for the voter to study the issues and vote.
- Voters don't have to take time off from work to vote on Election Day.
- VBM return envelopes come with pre-paid postage. No stamps are needed.
- RAVBM (Remote Accessible Vote by Mail): If you need accessibility features to vote your VBM ballot, you are out of state, or it is too late to receive a ballot in the mail, you can request a Remote Accessible VBM ballot which will give you access to an online secure ballot marking system. The voter must mark their ballot, print their ballot, and then mail their ballot to the elections office.

VBM Increases Voter Turnout

- There has been an increase in voter turnout throughout the state since VBM has been implemented.

VBM Does Not Benefit One Party Over Another

- Studies show that VBM benefits all parties and does not discriminate.

Top Reasons Why VBM Ballots are Not Counted

- The VBM return envelope is not signed and the voter failed to cure the issue.
- The signature on the envelope does not compare to the signature on file and the voter failed to cure the issue.
- The ballot is not returned in the VBM return envelope.
- There is no ballot inside the VBM return envelope.

Qualifications to Register to Vote

To register to vote in California, you must be:

- A United States citizen and a resident of California
- 18 years old or older on Election Day,
- Not currently serving a state or federal prison term for the conviction of a felony, and
- Not currently found mentally incompetent to vote by a court

Qualifications to Pre-register to Vote

To pre-register to vote in California, you must be:

- 16 or 17 year old, and
- Meet all of the other eligibility requirements to vote
- You will automatically be registered to vote on your 18th birthday

FACTSHEET
Topic: Redistricting

What is Redistricting?

- Every ten years following the US Census count, district boundaries for federal, state and local elected offices are redrawn to reflect new population data.
- The constitution requires this process in order to accommodate for growth and demographic changes that have taken place over the past 10 years.
- California uses that census data in order to distribute the population equally amongst the Congressional, State Senate, State Assembly, and State Board of Equalization districts.

What are key points to consider when drawing lines?

- Districts must be of equal population.
- Districts must comply with the "one-person, one-vote" principle of the Voting Rights Act which ensures minority voters have an equal opportunity to elect representatives of their choice.
- Districts must be contiguous meaning all areas of the district need to physically touch each other.
- District lines should minimize the division of cities, counties, neighborhoods, and communities of interest.
- Districts should be geographically compact, meaning that everyone in the district should live as near to each other as possible not spread out across the district.
- Where possible each Senate district should be adjacent to Assembly Districts and Board of Equalization districts shall be composed of 1O complete adjacent State Senate Districts.

Who draws the lines?

- On the state level, the California Citizens Redistricting Commission (CCRC) redraws the Congressional, State Senate, State Assembly, and State Board of Equalization district boundaries following each decennial census.

  You can learn more about the CCRC at www.WeDrawTheLinesCA.org

- Locally, the boundaries for districts such as county supervisorial, city council, schools, and special districts like fire, water and recreation districts are drawn by their governing bodies and not by the CCRC.

  Local jurisdictions need to follow the same criteria as the CCRC when redrawing their district boundaries.

What changes did voters see in the 2022 election cycle relating to Redistricting?

At the June 7th Statewide Direct Primary Election, each voter in the state was mailed a ballot including their new districts and those candidates for all Federal, State, County, and Local offices including:

- Congress
- State Assembly
- State Senate
- State Board of Equalization
- County Board of Supervisors

- And some Cities (where applicable)

At the November 8th General Election, voters saw the updated new local office boundary changes including:

- County Boards of Education
- School Districts
- Cities
- And Special Districts such as Community Services, Fire Protection, Sanitary, and Water districts.

What does redistricting mean to voters?

- There are possibilities that the districts for Congressional, State Assembly, State Senate, and State Board of Equalization and County Board of Supervisors did change for some voters; that means the representatives in those elected offices may have been different.
- Voters voted for candidates who ran for office using the new district lines for these contests on the ballot.

Language Assistance

The results of the Census also affect which language assistance counties are required to provide for voters at their voting locations.

- Section 203 of the Federal Voting Rights Act uses the census data to review how language assistance is provided in state and local jurisdictions:
- The law includes provisions where there are either more than 10,000, or more than 5% of citizens of voting age who are members of a single language minority group who cannot speak or read English very well.
- Historically, the languages covered under Section 203 are of Spanish, Asian, Native American, and Alaskan Native groups.

  For more information on Section 203 of the Voting Rights Act, you can visit the Justice Department's website.
- Section 14201 of the California Elections Code requires the county elections official to provide facsimile (exact duplicate) copies of the official ballot to voters in precincts where the Secretary of State has determined a need.

  These determinations take place every four years by January 1st of each year that the Governor is elected, and is based on the following:
- There is a group of single language minority residents who have limited-English capabilities and cannot vote without assistance.
- That number equals 3 percent or more of the voting-age residents of a county or precinct; OR
- Interested citizens or organizations provide information giving the Secretary of State reason to believe there is a need for providing facsimile ballots.

How does Redistricting look to a voter?

- Any voter can be assigned to one precinct today and in 10 years, be assigned to another precinct while still living at the same address.

- You and your neighbor may be in the same school district today, but it can change based on redistricting.

- Your ballot may not have the same familiar candidate because of the new district lines.

- Voters are encouraged to look up their districts in advance of approaching elections so that they are prepared to vote. Please call San Joaquin County Registrar of Voters office at (209) 468-VOTE(8683)

FACT SHEET

Topic: The Official Canvass

Counties have up to 30 days to complete the official election canvass in gubernatorial elections, and 28 days in presidential elections, before certifying the results of an election.

There are Four Critical Tasks that are Performed During the Canvass of the Vote

1. To ensure that every eligible ballot is counted.
2. To ensure that voters only voted once.
3. To ensure proper procedures were followed on Election Day.
4. To ensure the vote tabulation system is properly counting ballots by utilizing a manual audit.

Ensuring Every Eligible Ballot is Counted

- Vote by Mail (VBM) Ballots: VBM ballots that are postmarked on or before Election Day and received up to 7 days after Election Day are eligible to be processed and counted by law.
- **Conditional Voter Registration (CVR):** This allows voters who missed the registration deadline to register and vote a provisional ballot as late as Election Day. These ballots are processed for eligibility prior to being counted during the Canvass.
- **Inactive Voters:** Voters that have not voted in the last two federal elections are placed on inactive status. Upon verification of their information, these voters can vote at any polling location and are automatically updated to active status.
- **Ballot Duplication:** Ballots that are torn, stained, or otherwise unreadable by the tabulation equipment must be duplicated by teams of at least two staff. The original ballots are retained as historical records.

Ensuring that Voters Only Vote Once

- Multiple procedures detect fraudulent activity related to voting more than once:
  - When a voter submits his or her VBM ballot, "voting history" is applied in the voter record within the Election Management System. When a voter votes in person, voting history is applied to the voter record.
  - When processing provisional and Conditional Voter Registration ballots, the voting history of the voter is reviewed to ensure the voter has not previously voted.
  - VoteCal, the statewide voter registration database, allows counties to ensure a voter has not also voted elsewhere in the state.
  - Voter records that indicate a voter may have voted more than once (within the county and across the state) are investigated.
  - Cases that truly indicate a voter may have tried to vote twice are reported to the San Joaquin County Sheriff's office and the Secretary of State Fraud Division for investigation and possible prosecution.

Ensuring Proper Procedures were followed on Election Day

- After Election Day, staff will inspect all precinct supplies that are returned from voting locations to ensure all eligible ballots are retrieved for processing.
- Ballot statements, logs, and notes from each voting location are collected and reviewed to ensure proper procedures were followed.
- Notes from call logs between staff and election workers are reviewed to ensure issues were resolved.
- To maintain ballot integrity, the number of voters is reconciled to the number of ballots cast for each voting location. This is a critical step in ensuring that all ballots are accounted for at each voting location.

Ensuring the Hart Voting System is Properly Counting Ballots

- During pre-election activities, the Hart Voting System is subjected to rigorous Logic and Accuracy Testing with pre-marked test decks and expected outcomes to ensure the system is properly counting ballots. This is completed before any official ballots are counted. Members of the public are encouraged to take part in this process.
- During the canvass, counties are required to perform audits of the ballot counting system by performing a One Percent Manual Tally.
- One percent of the precincts and VBM ballots are randomly selected for a manual hand tally and compared to the machine count results produced by the Hart Voting System.
- To ensure every contest is audited, additional precincts and sets of VBM ballots are manually tallied to include every contest not initially tallied.
- The combination of the Logic and Accuracy Test and the One Percent Manual Tally during the canvass subjects the tabulation system to two audits before and after Election Day.

Transparency: Observers Welcomed

- All election processes and procedures are open to the public for observation.

FACTSHEET

Topic: Voting Systems & Security

Election Security

- Election security is a major concern at all levels of government. Elections have been designated as critical infrastructure by the Federal Department of 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.

Voting Systems Certification

- Voting systems used in San Joaquin County to count ballots must be certified for use by the California Secretary of State prior to being sold and/or used in any California election.
- The state has developed one of the most strenuous voting system testing and certification programs in the country.
- Vendors applying for voting system certification ***MUST*** have their equipment and software 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 and is used to conduct an election, is delivered directly from the Secretary of State into the hands of the Elections Official; only this "trusted build" (the certified version of the software and firmware) shall be installed by counties and must be reinstalled prior to any election.

Voting Systems Rules & Regulations

- The voting system used by the County is a paper-based, optical 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 and only authorized personnel are allowed in the area.
- 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.
- Election staff ensure that specific procedures for programming, deployment, and use of voting equipment during elections are met.
- Strict chain of custody procedures and ballot inventory controls are required.

- If any part or component of a voting system has the chain of custody compromised, the security or information breached, or attempted to be breached, the Secretary of State requires immediate notification, and an investigation, verification, and a sanitation protocol to be followed.

Voting System Security

- Voting system security is a multi-layered process with multiple factors, multiple checkpoints, multiple people, and multiple systems that makes systematic fraud nearly impossible:

Four Pillars of Election Security

- Facilities
  - Physical facility assessments
  - Designated high security areas
  - Alarms and/or 24/7 video surveillance
  - ID badges, key card access & logs
  - Emergency & disaster planning
- Networks
  - Stand-alone voting system
  - Cybersecurity measures (multi-factor authentication, password policy, staff training)
  - Limited access to the voting system by designated staff
  - Network hardening with vulnerability scanning for cyber hygiene and penetration testing
  - Firewalls, network segmentation, active monitoring with intercept software
  - Robust back-up and patching protocol
  - Trusted build of system is reinstalled prior to each election
- People
  - Oath of allegiance
  - Background checks
  - Training & supervision
  - Two-person rule
  - Chain of custody rule
  - Photo ID badges
  - Limited access
  - Proactive security culture
- Procedures
  - Adherence to California Elections Code, administrative regulations, and local ordinances.
  - Cornerstones of election security & integrity: chain of custody procedures, two-person teams, accountability forms
  - Ballot inventory controls
  - Robust training (staff, temporary staff, poll workers)
  - Testing & compliance auditing of voting systems
  - Preservation of logs, ballots, and election materials

Remaining Ever Vigilant and Adapting

- 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.
- Support from security agencies at the State, Federal, and local levels aid in the initiative to provide safe, secure, and transparent elections for our residents and jurisdictions.

Election Security Safeguards

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

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

Rumor vs. Reality

Pre-Election

Reality: Election officials regularly update voter registration lists in accordance with legal protections against the removal of eligible registrants.

Rumor: Election officials don't clean the voter rolls.

Get the Facts: Election officials regularly update their voter registration lists based on voter requests and data from varying sources that may indicate that a voter has died, moved, registered elsewhere, changed their name, or become otherwise ineligible. These data sources include motor vehicle licensing agencies, entities that maintain death records, confirmation notices mailed to voters, and interstate data exchanges. This helps election officials identify and merge duplicate records and remove records for individuals who are no longer eligible.

Federal and state laws protect against the removal of eligible registrants from the voter rolls. These include federal prohibitions, applicable in most states, against removing some registrants in the 90 days prior to a federal election and removing registrants solely due to their failure to vote. Unless an election official has first-hand information that a registrant has moved, processes used for removing records for those who may have moved can take longer than two years due to protections to prevent registrants from being removed incorrectly. Such legal protections and the timing of data sharing can result in a lag time between a person becoming ineligible and the removal of their record. This can lead to some official election mail, including mail-in ballots in some states, being delivered to addresses of those who have moved or may be otherwise ineligible. Election officials often encourage people to notify the election office if they receive election mail for individuals who no longer reside at the address.

State and federal laws prohibit voter impersonation, including voting on behalf of an individual who has died, moved, or otherwise become ineligible yet whose record remains temporarily on the voter rolls. Additional election integrity safeguards, including signature matching and verification of other personal data, protect against people casting ballots on behalf of others.

The voter registration practices described in this entry do not apply to North Dakota, where voter registration does not occur.

Useful Sources

- 18 U.S.C. § 1708
- 52 U.S.C. §§ 10307(c), 20507, 20511(2), 21083(a)(2)(A)

- Election Infographic Products
- The National Voter Registration Act of 1993: Questions and Answers, DOJ
- Election Crimes, FBI
- Election Mail Information Center,
- USPS Your local or state election officials. EAC state-by-state directory
- Maintenance of State Voter Registration Lists, NASS
- Voter List Accuracy, NCSL
- Election FAQs, NASED

Reality: Safeguards protect the integrity of the mail-in/absentee ballot process, including relating to the use of mail-in/absentee ballot request forms.

Rumor: People can easily violate the integrity of the mail-in/absentee ballot request process to receive and cast unauthorized mail-in/absentee ballots or prevent authorized voters from voting successfully in person.

Get the Facts: Election officials utilize various security measures to protect the integrity of the mail-in/absentee voting process, including those that protect against the unauthorized use of ballot request forms, in states where such forms are used, the submission of mail-in/absentee ballots by ineligible individuals, and eligible in-person voters being erroneously precluded from being able to vote due to being listed in the poll book as having received a mail-in/absentee ballot.

Mail-in/absentee ballot request forms typically require applicants to sign the form and affirm their eligibility to cast a mail-in/absentee ballot under penalty of law. Upon receipt of a mail-in/absentee ballot request form, election officials implement varying procedures to verify the identity and eligibility of the applicant prior to sending the applicant a mail-in/absentee ballot. Such procedures include checking the signature and information submitted on the form against the corresponding voter registration record, as well as ensuring that multiple mail-in/absentee ballots are not sent in response to applications using the same voter's information.

Election officials further implement varying procedures to verify the identity and eligibility of those who submit mail-in/absentee ballots. Those who submit mail-in/absentee ballots are required to sign the mail-in/absentee ballot envelope. In some states, a notarized signature, the signature of a witness or witnesses, and/or a copy of valid identification is also required. Upon receipt of a mail-in/absentee ballot, election officials verify the signature on the mail-in/absentee ballot envelope and/or that the mail-in/absentee ballot has been otherwise properly submitted prior to retrieving the ballot from its envelope and submitting it for counting. Some states notify the voter if there is a discrepancy or missing signature, affording the voter an opportunity to correct the issue.

State policies vary on how to handle an in-person voter who is listed in the poll book as having been sent a mail-in/absentee ballot. In most states, the voter would be required to cast a provisional ballot that could be later reviewed by election officials. In others, the voter may cast a regular ballot and any corresponding mail-in/absentee ballot returned in the name of that voter would be rejected. In all such cases, instances of potential double voting or voter impersonation could be directed to appropriate authorities for investigation.

Useful Sources

- Mail-in Voting in 2020 Infrastructure Risk Assessment, CISA
- Mail-in Voting in 2020 Infrastructure Risk Infographic, CISA
- Mail-in Voting Integrity Safeguards Infographic, CISA

- USPS Election Mail Information Center, USPS
- How States Verify Absentee Ballot Applications, NCSL
- How States Verify Voted Absentee Ballots, NCSL
- States That Permit Voters to Correct Signature Discrepancies, NCSL
- 52 U.S.C. § 21082
- Provisional Ballots, NCSL
- State Policies on Voting In-Person or Changing Vote After Requesting a Mail/Absentee Ballot, NASS
- Election FAQs, NASED
- Your local or state election officials. EAC state-by-state directory

Reality: Robust safeguards protect against tampering with ballots returned via drop box.

Rumor: Drop boxes used by election officials to collect returned mail-in/absentee ballots can be easily tampered with, stolen, or destroyed.

Get the Facts: Election officials utilize various safeguards to protect ballots returned by voters via drop boxes from being tampered with, stolen, or destroyed. Drop boxes located outdoors are typically made of heavy and high-grade metal, bolted to the ground, and include security features such as locks, tamper-evident seals, minimally sized ballot insertion slots, and fire and water-damage prevention features. Drop boxes located indoors are typically staffed and protected by existing building security measures. Many election offices monitor their drop boxes via 24-hour video surveillance. Ballots returned via drop box are retrieved by election officials or designated individuals, often in bi-partisan teams, at frequent intervals.

Useful Sources

- Ballot Drop Box, Election Infrastructure Subsector's Government Coordinating Council and Sector Coordinating Council Joint COVID-19 Working Group
- Ballot Drop Box Definitions, Design Features, Location, and Number, NCSL
- Voting Outside the Polling Place: Absentee, All-Mail and other Voting at Home Options, NCSL
- Election FAQs, NASED
- Your local or state election officials. EAC state-by-state directory

Reality: Voting system hardware and software undergo testing from federal, state, and/or local election authorities.

Rumor: Voting system software is not reviewed or tested and can be easily manipulated.

Get the Facts: State and local election officials implement varying testing practices to help ensure voting system hardware and software function as intended. These practices include federal and state testing and certification, testing prior to procurement, acceptance testing, and/or pre- and post-election logic and accuracy testing. Such testing helps detect and protect against malicious or anomalous software issues. Under federal and state certification programs, voting system manufacturers submit systems to undergo testing and review by an accredited laboratory or state testers. This testing is designed to check that systems function as designed and meet applicable state and/or federal requirements or standards for accuracy, privacy, and accessibility, such as the Voluntary Voting System Guidelines set by the U.S. Election Assistance Commission. Certification testing usually includes a review of a system's source code as well as environmental, security and functional testing. Varying by state, this testing may be conducted by a state-certified laboratory, a partner university, and/or a federally certified testing laboratory.

Useful Sources

- 52 U.S.C. §§ 20971, 21081
- Voting System Certification Process, EAC
- Voting System Security Measures, EAC
- Election Infrastructure Security, CISA
- Election Infrastructure Cyber Risk Assessment and Infographic, CISA
- Voting System Standards, Testing and Certification, NCSL
- Post-Election Audits, NCSL
- Election FAQs, NASED
- Your local or state election officials. EAC state-by-state directory

Reality: Voter registration list maintenance and other election integrity measures protect against voting illegally on behalf of deceased individuals.

Rumor: Votes are being cast on behalf of dead people and these votes are being counted.

Get the Facts: State and federal laws prohibit voter impersonation, including casting a ballot on behalf of a deceased individual. Election officials regularly update their voter registration lists, removing voter records for those who have died, moved, registered elsewhere, or became otherwise ineligible. Removal of deceased individuals is based on death records shared by state vital statistics agencies and the Social Security Administration. While there can be lag time between a person's death and their removal from the voter registration list, which can lead to some official election mail, including mail-in ballots being delivered to addresses of deceased individuals, death records provide a strong audit trail to identify any attempts to cast ballots on behalf of deceased individuals. Additional election integrity safeguards, including signature matching and information checks, further protect against voter impersonation and voting by ineligible persons.

In some instances, living persons may return mail-in ballots or vote early in-person, and then die before Election Day. Some states permit such voters' ballots to be counted, while others disallow such ballots and follow procedures to identify and reject them during processing.

Taken out of context, some voter registration information may appear to suggest suspicious activity but is actually the result of an innocuous clerical error or intended data practices. For example, in rare instances when a registrant's birth date is not known (e.g., a voter who legally registered prior to modern voter registration practices), election officials may use temporary placeholder data (e.g., 1/1/1900) until the registrant's birth date can be updated. In other instances, a voting-age child with the same name and address as their deceased parent could be misinterpreted as a deceased voter or contribute to clerical errors.

Useful Sources

- 18 U.S.C. § 1708
- 52 U.S.C. §§ 10307(c), 20507, 20511(2), 21083(a)(2)(A)
- Mail-in Voting Integrity Safeguards Infographic, CISA
- Election Infrastructure Cyber Risk Assessment and Infographic, CISA
- Election Infrastructure Security, CISA
- Election Security, DHS
- The National Voter Registration Act of 1993: Questions and Answers, DOJ
- Election Crimes, FBI
- Election Mail Information Center, USPS
- Your local or state election officials. EAC state-by-state directory
- Maintenance of State Voter Registration Lists, NASS

- What If an Absentee Voter Dies Before Election Day?, NCSL
- Voter List Accuracy, NCSL
- Election FAQs, NASED

Reality: Some voter registration data is publicly available.

Rumor: Someone possessing or posting voter registration data means voter registration databases have been hacked.

Get the Facts: Some voter registration information is public information and is available to political campaigns, researchers, and often members of the public, frequently for purchase. According to a joint FBI and CISA public service announcement, cyber actors may make false claims of "hacked" voter information to undermine confidence in U.S. democratic institutions.

Useful Sources

- Availability of State Voter File and Confidential Information, EAC
- FBI-CISA Public Service Announcement: False Claims of Hacked Voter Information Likely Intended to Cast Doubt on Legitimacy of U.S. Elections
- Access To and Use Of Voter Registration Lists, NCSL
- Election FAQs, NASED

Reality: Online voter registration websites can experience outages for non- malicious reasons.

Rumor: An online voter registration website experiences an outage and claims are made the election has been compromised.

Get the Facts: Outages in online voter registration systems occur for a variety of reasons, including configuration errors, hardware issues, natural disasters, communications infrastructure issues, and distributed denial of service (DDoS) attacks. As CISA and FBI warned in a public service announcement, a system outage does not necessarily mean the integrity of voter registration information or any other election system has been impacted. When an outage occurs, election officials work to verify the integrity of voter registration information.

Useful Sources

- FBI-CISA Public Service Announcement: False Claims of Hacked Voter Information Likely Intended to Cast Doubt on Legitimacy of U.S. Elections
- Securing Voter Registration Data, CISA
- Your local or state election officials EAC state-by-state directory

Reality: A compromise of a state or local government system does not necessarily mean election infrastructure or the integrity of your vote has been compromised.

Rumor: If state or local jurisdiction information technology (IT) has been compromised, the election results cannot be trusted.

Get the Facts: Hacks of state and local IT systems should not be minimized; however, a compromise of state or local IT systems does not mean those systems are election related. Even if an election-related system is compromised, a compromise of a system does not necessarily mean the integrity of the vote has been affected. Election officials have multiple safeguards and contingencies in place, including provisional ballots or backup paper poll books that limit the impact from a cyber incident with minimal disruption to voting. Additionally, having an auditable paper record ensures that the vote count can be verified and validated.

Useful Sources

- FBI-CISA Public Service Announcement: Cyber Threats to Voting Processes Could Slow But Not Prevent Voting
- Election Infrastructure Cyber Risk Assessment and Infographic, CISA

Reality: Malicious actors can fake manipulation of voter registration data to spread disinformation.

Rumor: Videos, images or emails suggesting voter registration information is being manipulated means voters will not be able to vote.

Get the Facts: Claims are easy to fake and can be used for disinformation purposes. If voter registration data were to be manipulated, states have several safeguards in place to enable voters to vote, including offline backups of registration data, provisional ballots, and in several states, same-day registration.

Useful Sources

- FBI-CISA Public Service Announcement: False Claims of Hacked Voter Information Likely Intended to Cast Doubt on Legitimacy of U.S. Elections
- Securing Voter Registration Data, CISA
- Securing Voter Registration Systems, NCSL
- Election FAQs, NASED

Reality: Safeguards are in place to prevent home-printed or photocopied mail-in ballots from being counted.

Rumor: A malicious actor can easily defraud an election by printing and sending in extra mail-in ballots.

Get the Facts: This is false. Committing fraud through photocopied or home-printed ballots would be highly difficult to do successfully. This is because each local election office has security measures in place to detect such malicious activity. While the specific measures vary, in accordance with state and local election laws and practices, such security measures include signature matching, information checks, barcodes, watermarks, and precise paper weights.

Useful Sources

- Mail-in Voting Election Integrity Safeguards Infographic, CISA
- Election FAQs, NASED

Reality: Safeguards are in place to protect against fraudulent voting using the Federal Write-In Absentee Ballot (FWAB).

Rumor: A malicious actor can easily defraud an election using the Federal Write-In Absentee Ballot (FWAB).

Get the Facts: Changing an election using fraudulently submitted FWABs would be highly difficult to do. This is because election offices have security measures in place to detect such activity.

The FWAB is primarily used as a backup ballot for military and overseas voters who requested but did not yet receive their absentee ballot. FWAB users must provide their signature and meet varying state voter registration and absentee ballot request requirements, which can include provision of full or partial social security number, state identification number, proof of identification, and/or witness signature.

Since only military and overseas voters are eligible to use the FWAB, relatively few of them are submitted in each election. In 2016, states reported that only 23,291 total FWABs were submitted nationwide, with all but six states receiving less than 1,000 FWABs statewide. Since use is relatively rare, spikes in FWAB usage would be detected as anomalous.

Useful Sources

- 52 U.S.C. § 20303
- Voting Assistance Guide, FVAP
- Election Forms and Tools for Sending, FVAP
- 2020 Election Administration and Voting Survey Comprehensive Report, EAC
- 2018 Election Administration and Voting Survey Comprehensive Report, EAC

Rumor vs. Reality

Election Day

Reality: The use of paper ballots and other redundancy measures ensure that votes can be counted when a ballot scanner malfunctions or cannot scan ballots for other reasons.

Rumor: Problems with ballot scanners at my voting site mean that my ballot won't be counted.

Get the Facts: Like all digital systems, ballot scanners can malfunction. Similarly, properly functioning ballot scanners may be unable to scan ballots that are damaged, misprinted, or have ambiguous markings. When a ballot cannot be read by a scanner at a voting site, election officials apply procedures to securely store the ballots until they can be counted at a later time. Because the paper ballot itself is the official record of the votes, there is no impact on the accuracy or integrity of election results.

Useful Sources

- Voluntary Voting System Guidelines, EAC
- Voting Equipment, NCSL
- Your local or state election officials EAC state-by-state directory.

Reality: Election officials provide writing instruments that are approved for marking ballots to all in-person voters using hand-marked paper ballots.

Rumor: Poll workers gave specific writing instruments, such as Sharpies, only to specific voters to cause their ballots to be rejected.

Get the Facts: Election jurisdictions allow voters to mark ballots with varying types of writing instruments, based on state law and other considerations such as tabulation system requirements. Poll workers are required to provide approved writing devices to voters.

Although felt-tip pens, like Sharpies, may bleed through ballots, some election officials have stated that ballot tabulation equipment in their jurisdictions can still read these ballots. Many jurisdictions even design their ballots with offset columns to prevent any potential bleeding through from impacting the ability to easily scan both sides of ballots.

If a ballot has issues that impact its ability to be scanned, it can be hand counted or duplicated, or adjudicated by election officials, who use defined procedures such as chain of custody to ensure protect ballot secrecy and integrity. Many states additionally have "voter intent" laws that allow for ballots to be counted even when issues such as bleed-throughs or stray marks are present, as long as the voter's intent can still be determined.

Useful Sources

- After the Voting Ends: The Steps to Complete an Election, NCSL
- Ballot Duplication blog series, Council of State Governments Overseas Voting Initiative
- Your local or state election officials. EAC state-by-state directory

Reality: Voters are protected by state and federal law from threats or intimidation at the polls, including from election observers.

Rumor: Observers in the polling place are permitted to intimidate voters, campaign, and interfere with voting.

Get the Facts: While most states have a process to permit a limited number of credentialed or registered observers at in-person voting locations to observe the voting process, state and federal laws offer voters general protection from threats and intimidation, including from observers. States use varying terms for observers, including "poll watchers," "challengers," and "poll agents." In general, observers are prohibited from violating ballot secrecy, campaigning, collecting private voter information, and obstructing or interfering with the voting process. Observers in some states may report potential issues to election officials, such as questioned eligibility of a voter, suspicious behavior, or suspected rule violation. Intimidation or threatening behavior is never permissible.

Under certain circumstances, the U.S. Department of Justice (DOJ) Civil Rights Division may monitor polling place procedures for the protection of voters under federal voting rights laws. International observers, including delegations from the Organization for Security and Cooperation in Europe or the Organization for American States, who have been invited by the U.S. Department of State, may also observe in-person voting processes in some states.

If you feel that you've been a victim of, or witnessed, voter intimidation or threats, please report the experience to the DOJ Civil Rights Division's Voting Section by phone 800-253-3931 or through its complaint portal at https://civilrights.justice.gov/. If you experience an emergency, please call 911.

Useful Sources

- 18 U.S.C. § 245(b)(1)(A), 18 U.S.C. § 594, 52 U.S.C. § 20511, 18 U.S.C. §§ 241 and 242
- Election Crimes and Security, FBI
- Federal Prosecution of Election Offenses, DOJ
- About Federal Observers and Election Monitoring, DOJ
- State Laws on Poll Watchers and Challengers, NASS
- Poll Watchers and Challengers, NCSL
- Policies for Election Observers, NCSL
- OSCE/ODIHR Election Observation USA 2020 Factsheet, OSCE
- Election FAQs, NASED

Reality: Safeguards are in place to protect ballot secrecy.

Rumor: Someone is claiming to know who I voted for.

Get the Facts: Ballot secrecy is guaranteed by law in all states. Election officials implement various safeguards to protect voters' choices from being viewable or knowable by others, including the election officials themselves. With few exceptions, these security measures ensure that individual ballots, once cast, cannot be traced back to the voters who cast them. For in-person voting, privacy measures include dividers between voting stations and requirements that poll workers maintain distance from voters while they are casting their ballots. For mail-in and provisional voting, election officials follow strict procedures to ensure ballot secrecy when ballots are retrieved from mail-in and provisional ballot envelopes.

Ballot secrecy rights may be voluntarily waived by voters in certain circumstances, and waiver may be required in some of these, such as military and overseas voters that vote by fax or e-mail.

While ballot choices are secret in almost all circumstances, a voter's party affiliation and history of voting generally are not. Information contained in voter registration records, such as name, address, phone number, and political party affiliation (in states with party-based voter registration), is generally available to political parties and others. This data also regularly contains information on whether a voter voted in a particular election, but not their ballot choices.

Useful Sources

- Voting Outside the Polling Place: Absentee, All-Mail and other Voting at Home Options, NCSL
- Secrecy of the Ballot and Ballot Selfies, NCSL
- States that are Required to Provide Secrecy Sleeves for Absentee/Mail Ballots, NCSL
- Access To and Use of Voter Registration Lists, NCSL
- Election FAQs, NASED

Reality: Polling place lookup sites can experience outages for non-malicious reasons.

Rumor: If polling place lookup sites experience an outage, election infrastructure must have been compromised.

Get the Facts: Polling place lookup sites, like all websites, may experience outages for a variety of reasons, impacting their availability to voters. Polling place lookup sites are not connected to infrastructure that counts votes and are typically segmented from infrastructure that enables voting, such as the voter registration database. Election officials will point potential voters to alternate tools and resources for this information in the event of an issue.

Useful Sources

- Election Infrastructure Cyber Risk Assessment and Infographic, CISA
- Your local or state election officials EAC state-by-state directory

Rumor vs. Reality

Post-Election

Reality: The existence of a vulnerability in election technology is not evidence that the vulnerability has been exploited or that the results of an election have been impacted. Identifying and mitigating vulnerabilities is an important security practice.

Rumor: Vulnerabilities in election technology mean that elections have been hacked and hackers are able to change election results.

Get the Facts: Like all digital systems, the technologies used to administer elections have vulnerabilities. Election officials use varying technological, physical, and procedural controls to help safeguard these systems and the integrity of the election processes they support. Identified vulnerabilities should be taken seriously and mitigations implemented in a timely manner. Identifying and mitigating vulnerabilities is a key part of ordinary cybersecurity practices. Mitigations include installing software patches, implementing physical and procedural safeguards, and applying compensating technical controls. These safeguards and compensating controls include measures that seek to identify and mitigate vulnerabilities prior to potential exploitation as well as those that help detect and recover from a malfunction or an actual or attempted exploitation of known or zero-day vulnerabilities. It's important to note that there is no indication that cyber vulnerabilities have contributed to any voting system deleting, losing, or changing votes.

Useful Sources

- Intelligence Community Assessment on Foreign Threats to the 2020 U.S. Federal Elections, ODNI
- Key Findings and Recommendations: Foreign Interference Related to the 2020 US Federal Elections, DHS and DOJ
- CISA Insights: Chain of Custody and Critical Infrastructure Systems, CISA
- Chain of Custody Best Practices, EAC
- Voting Testing and Certification Program, EAC
- Voting System Standards, Testing and Certification, NCSL
- Post-Election Audits, NCSL
- Your local or state election officials. EAC state-by-state directory

Reality: Ballot handling procedures protect against intentional or unintentional ballot destruction and related tampering.

Rumor: Ballots can easily be removed, added, replaced, or destroyed without detection, altering official vote counts.

Get the Facts: Election officials implement varying ballot processing and tabulation safeguards designed to ensure each ballot cast in the election can be correctly counted. These safeguards include chain of custody procedures, auditable logging requirements, and canvass processes. Election officials use these security measure to check that votes are accurately accounted for during processing and counting.
Federal law and varying state laws and regulations govern election officials' retention practices for ballots and other election records. Per federal law, ballots, applications, registrations, and other records related to elections for federal offices, such as those for President and Vice President, Members of the U.S. Senate or House of Representatives, must be retained and preserved for 22 months from the date of the election Beyond retention, many state, local, and territorial jurisdictions require specific security protocols for stored ballots and other election records, such as storage in a secure vault featuring double lock systems that can only be opened when authorized representatives from both political parties are present. This type of common requirement is intended to ensure all ballots and relevant records are preserved in their post-election state in case they are needed for recounts, audits, or other post-election processes.

Election officials may destroy or discard ballots and other election records required to be retained following applicable retention periods set in federal, state, and/or local requirements. Election officials may discard other election materials that are not subject to retention requirements at any time.

Images or video of election officials discarding papers may appear suspicious when taken out of context, but they are likely depicting legal disposal of election materials.

Useful Sources

- 52 U.S.C. § 20701
- Federal Law Constraints on Post-Election "Audits", DOJ
- CISA Insights: Chain of Custody, CISA
- Chain of Custody Best Practices, EAC
- Task force of Vote Verification: Post-election Audit Recommendations, NASS
- Retention Chart for Boards of Elections, State of Ohio
- Election Infrastructure Security, CISA
- Election Infrastructure Cyber Risk Assessment and Infographic, CISA
- Election FAQs, NASED
- Your local or state election officials. EAC state-by-state directory

Reality: Variations in vote totals for different contests on the same ballot occur in every election and do not by themselves indicate fraud or issues with voting technology.

Rumor: More votes in one contest than other contests on the ballot means that results cannot be trusted.

Get the Facts: Variations in vote totals for different contests on the same ballot occur in every election. For example, this can occur because of "undervotes." These variations by themselves are not indications of issues with voting technology or the integrity of election processes or results.

An undervote occurs when a voter intentionally or unintentionally does not make a selection in a given contest on their ballot (e.g., a voter votes for a presidential candidate, but not for any candidates in other contests on their ballot) or, where a voter selects fewer than the maximum number allowed for a particular contest. Undervotes commonly occur in so-called "down-ballot" races. For example, a voter may choose to vote for president, senator, and governor, but not for other offices or ballot measures that are lower down on their ballot. Even if a ballot includes an undervote in a particular contest, properly marked votes on their ballot are counted.

Useful Sources

- Your local or state election officials. EAC state-by-state directory
- Voter Intent Laws, NCSL
- Post-Election Audits, NCSL
- Election FAQs, NASED

Reality: Robust safeguards including canvassing and auditing procedures help ensure the accuracy of official election results.

Rumor: A bad actor could change election results without detection.

Get the Facts: The systems and processes used by election officials to tabulate votes and certify official results are protected by various safeguards that help ensure the accuracy of election results. These safeguards include measures that help ensure tabulation systems function as intended, protect against malicious software, and enable the identification and correction of any irregularities.

Every state has voting system safeguards to ensure each ballot cast in the election can be correctly counted. State procedures often include testing and certification of voting systems, required auditable logs, and software checks, such as logic and accuracy tests, to ensure ballots are properly counted before election results are made official. With these security measures, election officials can check to determine that devices are running the certified software and functioning properly.

Every state also has laws and processes to verify vote tallies before results are officially certified. State processes include robust chain-of-custody procedures, auditable logs, and canvass processes. The vast majority of votes cast in this election will be cast on paper ballots or using machines that produce a paper audit trail, which allow for tabulation audits to be conducted from the paper record in the event any issues emerge with the voting system software, audit logs, or tabulation. These canvass and certification procedures are also generally conducted in the public eye, as political party representatives and other observers are typically allowed to be present, to add an additional layer of verification. This means voting system software is not a single point of failure and such systems are subject to multiple audits to ensure accuracy and reliability. For example, some counties conduct multiple audits, including a post-election logic and accuracy test of the voting system, and a bipartisan hand count of paper ballots.

Useful Sources

- Election Results Reporting Risks and Mitigations Infographic, CISA
- Election Infrastructure Cyber Risk Assessment and Infographic, CISA
- Mail-in Voting Integrity Safeguards Infographic, CISA
- Mail-in Voting Processing Factors Map (Updated October 29, 2020), CISA
- Post-Election Process Mapping Infographic, CISA
- Your local or state election officials. EAC state-by-state directory
- Post-election audits, NCSL
- Policies for Election Observers, NSCL
- Election FAQs, NASED

Reality: The Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA) do not design or audit ballots, which are processes managed by state and local election officials.

Rumor: DHS or CISA printed paper ballots with security measures and is auditing results as a countermeasure against ballot counterfeiting.

Get the Facts: While DHS and CISA assist states and localities with securing election infrastructure, DHS and CISA do not design, print, or audit ballots. State and local election officials manage ballot design and printing, as well as the auditing of results.

Local election offices have security and detection measures in place that make it highly difficult to commit fraud through counterfeit ballots. While the specific measures vary, in accordance with state and local election laws and practices, ballot security measures can include signature matching, information checks, barcodes, watermarks, and precise paper weights.

DHS and CISA operate in support of state and local election officials, and do not administer elections or handle ballots. CISA's role in election security includes sharing information, such as cyber threat indicators, with state and local election officials, as well as providing technical cybersecurity services (e.g., vulnerability scanning) upon the request of those officials. CISA funded an independent third-party to develop an open-source election auditing tool for voluntary use by state and local election officials. (Note: The previous sentence was updated 9 November 2020.) CISA does not audit elections and does not have access to the tool as states use it.

Useful Sources

- Election Infrastructure Security, CISA
- Election Security, DHS
- Federal Role in U.S. Campaigns and Elections: An Overview, CRS
- Mail-in Voting Integrity Safeguards Infographic, CISA
- Mail-in Voting 2020 Risk Assessment, CISA
- Risk-Limiting Audits with Arlo, Voting Works
- Your local or state election officials EAC state-by-state directory

Reality: Election results are not final until certification. Election night reporting is unofficial and those results may change as ballot counting is completed.

Rumor: If results as reported on election night change over the ensuing days or weeks, the process is hacked or compromised, so I can't trust the results.

Get the Facts: The timeline for reporting election results may be impacted by a number of factors, including changes to state or local level policies that affect how the election is administered, changes to when ballots can be processed, or additional protocols implemented to make voting and vote processing safer during the pandemic. Election results reported on election night are always unofficial and are provided solely for voters' convenience. In fact, no state requires that official results be certified on election night itself. Fluctuations in unofficial results reporting will occur during and after election night as more ballots are processed and counted, often including military and overseas ballots, and validated provisional ballots. Variations in state processes may also mean ballots cast through different methods (e.g., early in-person voting, mail-in voting, and election day voting) are counted and unofficially reported in different orders. Official results are released after rigorous canvassing (verification) and certification by local and state election officials.

Useful Sources

- FBI-CISA Public Service Announcement: Foreign Actors and Cybercriminals Likely to Spread Disinformation Regarding 2020 Election Results
- Election Results Reporting Risks and Mitigations, CISA
- Mail-in Voting 2020 Risk Assessment, CISA
- Mail-in Voting Integrity Safeguards Infographic, CISA
- Mail-in Voting Processing Factors Map (Updated October 29, 2020), CISA
- Post-Election Process Mapping Infographic, CISA
- Checklist for Securing Election Night Results Reporting, EAC
- USPS Election Mail Information Center, USPS
- Federal Election Results FAQs, CRS
- State Election Canvassing Timeframes and Recount Thresholds, NASS
- After the Voting Ends: The Steps to Complete an Election, NCSL
- Election Security State Policies, NCSL
- Changes to Mail in Voting in 2020, NCSL
- Election FAQs, NASED

Reality: Provisional ballots are counted in every election regardless of result margins.

Rumor: Provisional ballots are only counted if there's a close race.

Get the Facts: All provisional ballots are reviewed by election officials in every election regardless of result margins. Provisional ballots cast by individuals whose eligibility can be verified are counted. Additionally, election officials are required to provide individuals who cast provisional ballots written information regarding how they can determine whether their vote was counted and, if it was not counted, the reason for its rejection.

Useful Sources

- 52 U.S.C. § 21082
- Post-Election Process Mapping Infographic, CISA
- Provisional Ballots, NCSL
- State Policies on Voting In-Person or Changing Vote After Requesting a Mail/Absentee Ballot, NASS
- Election FAQs, NASED
- Your local or state election officials. EAC state-by-state directory

Reality: In some circumstances, elections officials are permitted to "duplicate" ballots to ensure they can be properly counted.

Rumor: Witnessing election officials marking ballots means that fraudulent voting is taking place.

Get the Facts: Voters do not always submit ballots that can be accurately interpreted by a ballot scanner due to issues, such as damage, misprinting and/or ambiguous markings on the ballot. Election officials apply the jurisdiction's rules for determining voter intent regarding the marks on such ballots and capture the ballots' valid votes in election results via varying electronic and/or manual processes.
Ballot duplication is a process by which election officials carefully transfer a voter's choices from an unscannable ballot to a duplicate ballot so it can be read by a ballot scanner. Both the original and duplicate ballot are labeled and logged so that the two ballots can be tracked and audited. Many jurisdictions require bipartisan teams of two or four personnel to complete this process and verify that votes are accurately transferred to duplicated ballots. The process is often open to public observation.
In some jurisdictions, ballot duplication is referred to as ballot remaking, ballot replication, or ballot transcription.

Useful Sources

- After the Voting Ends: The Steps to Complete an Election, NCSL
- Ballot Duplication blog series, Council of State Governments Overseas Voting Initiative
- Your local or state election officials EAC state-by-state directory.

Reality: Results displayed via election results reporting websites are unofficial and subject to change until results are certified. An outage, defacement, or other issue affecting the integrity or availability of the information displayed on such sites would not impact the counting of ballots or the accuracy of the official certified results.

Rumor: If an election night reporting site experiences an outage, is defaced, or displays incorrect results, vote counts will be lost or manipulated.

Get the Facts: Election officials use websites to share unofficial results with the public as votes are being counted and other results management processes are taking place. The results displayed on these sites are unofficial and may be updated, as necessary, until official results are certified. These sites may experience outages due to a variety of issues including a high volume of Internet traffic or cyber incidents. Cyber incidents, as well as human or technological error, may also lead to inaccurate information being displayed on these sites. As these websites are not connected to any portion of the voting system, such disruptions would not impact the ability of election officials to count ballots or the accuracy of official certified results.

Useful Sources

- FBI-CISA Public Service Announcement: Foreign Actors and Cybercriminals Likely to Spread Disinformation Regarding 2020 Election Results
- Election Results, Canvass, and Certification, EAC
- Post-Election Process Mapping Infographic, CISA
- Federal Election Results FAQs, CRS
- Election FAQs, NASED

Reality: Malicious actors can use fake personas and impersonate real accounts.

Rumor: If a social media account claims an identity, the account must be run by that person or organization.

Get the Facts: Malicious actors often use fake personas and impersonate real accounts to trick the public into believing disinformation, including election-related disinformation.

Popular social media platforms such as Facebook, Instagram, Twitter, Snapchat, and others provide an indication, such as a checkmark that is either blue or grey, to indicate that an account is verified by the platform. If an account claims to be a well-known person or official organization but is not verified, they may be an imposter.

There are multiple things to look for if you think an account is fake or spoofed. Is the account brand new? Do they create content or merely re-share? Do they have a coherent profile description and does it match what they are sharing? Do they have a real profile photo? A best practice when looking for election-related information is to go to trusted sources, like your local election official.

If you find a suspicious social media post or account, consider reporting the activity to the platform so others don't get duped. Most platforms have a "report" function built into posts, so it's easy to report suspicious items, such as misinformation about election infrastructure. If an account is posting election disinformation, consider reporting to your state or local election official.

Useful Sources

- Election Mis-, Dis-, and Malinformation Toolkit, CISA
- #TrustedInfo2022, NASS
- Voter Resources: State Voter Information, NASED
- Voting and Elections Information, usa.gov
- Your local or state election officials EAC state-by-state directory

Reality: Cyber actors can "spoof" or forge email sender addresses to look like they come from someone else.

Rumor: I received an election-related email that looks like it came from a certain organization, so the organization must have sent it.

Get the Facts: Cyber actors can forge emails to look like they came from someone else. This common tactic is called email spoofing, where attackers send an email pretending to be from a specific domain or organization in an attempt to harvest personal data or spread malware. Such spoofed emails can also be used to disseminate false or inflammatory information. To send realistic-looking emails, cyber actors may forge the sender address to hide the origin of an email or set up spoofed domains that have a slightly different name from the real domain. Always be wary of out of the ordinary emails and look to trusted sources, such as the organization's official website, in order to verify. Never provide personal information or download files from suspicious emails. If you receive a suspicious election-related email, consider reporting it to your local election official or local FBI field office.

Useful Sources

- FBI-CISA Public Service Announcement: Spoofed Internet Domains and Email Accounts Pose Cyber and Disinformation Risks to Voters
- Actions to Counter Email-based Attacks on Election-Related Entities, CISA
- Enhanced Email and Web Security, CISA


Registrar of
Voters
SAN JOAQUIN COUNTY