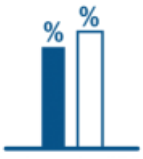
ELECTION SECURITY RUMOR VS. REALITY

Last Updated: November 2, 2021

Mis- and disinformation can undermine public confidence in the electoral process, as well as in our democracy. Elections are administered by state and local officials who implement numerous safeguards to protect the security of your vote pursuant to various state and federal laws and processes. This resource is designed to debunk common misinformation and disinformation narratives and themes that relate broadly to the security of election infrastructure and related processes. It is not intended to address jurisdiction-specific claims. Instead, this resource addresses election security rumors by describing common and generally applicable protective processes, security measures, and legal requirements designed to protect against or detect large-scale security issues related to election infrastructure and processes.

You can learn more about mis- and disinformation from CISA's Mis-, Dis-, Malinformation (MDM) team. Click an icon below to go directly to that section.



Post-Election

Pre-Election

Election Day

NEW RUMOR VS. REALITY

✔ 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
- Your local or state election officials. EAC state-by-state directory
- Link directly to this rumor by using: https://www.cisa.gov/rumorcontrol#rumor25

✔ 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
- Your local or state election officials. EAC state-by-state directory
- Link directly to this rumor by using: https://www.cisa.gov/rumorcontrol#rumor24

POST-ELECTION

TLP:WHITE

✔ Reality: Ballot handling procedures protect against intentional or unintentional destruction.

✘ Rumor: Ballots can easily be destroyed without detection, preventing them from being counted.

Get the Facts: States have ballot processing and tabulation safeguards designed to ensure each ballot cast in the election can be correctly counted. State procedures often include robust 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.

Per federal law, all ballots, applications, and registrations 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. In addition, many states also require specific state and local security protocols for stored ballots, 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 requirement is intended to ensure all ballots and relevant records, such as voter registrations, cannot be discarded, but are available in case they are needed for recounts or audits to resolve any potential issues.

Election officials, based on state and local law, may discard non-relevant materials, such as addressed envelopes or duplicate applications. Taken out of context, images or video of election officials discarding papers may appear suspicious , but are likely depicting legal discarding of these non-relevant election materials.

Useful Sources:

- 52 U.S.C. § 20701
- Retention Chart for Boards of Elections, State of Ohio
- Election Infrastructure Security, CISA
- Election Infrastructure Cyber Risk Assessment and Infographic, CISA
- Your local or state election officials. EAC state-by-state directory
- Link directly to this rumor by using: https://www.cisa.gov/rumorcontrol#rumor22

✔ 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 as a result 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 on 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
- Link directly to this rumor by using: https://www.cisa.gov/rumorcontrol#rumor20

TLP:WHITE

✔ Reality: Robust safeguards including canvassing and auditing procedures help e 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
- Tabulation Security, Maricopa County AZ
- Link directly to this rumor by using: https://www.cisa.gov/rumorcontrol#rumor17

✔ 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 b
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
- Link directly to this rumor by using: https://www.cisa.gov/rumorcontrol#rumor19

✔ Reality: Election results reporting may occur more slowly than some voters expect. This alone does not indicate a problem with the counting process or results, or that there are issues affecting the integrity of the election. Official results are not certified until all validly cast ballots have been counted, including ballots that are legally counted after election night.

✘ 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
- 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
- Link directly to this rumor by using: https://www.cisa.gov/rumorcontrol#rumor14

TLP:WHITE

✔ 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
- Your local or state election officials. EAC state-by-state directory
- Link directly to this rumor by using: https://www.cisa.gov/rumorcontrol#rumor15

✔ Reality: In some circumstances, elections officials are permitted to "duplicate" or otherwise further mark cast ballots to ensure they can be properly counted.

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

Get the Facts: Some ballots cannot be read by a ballot scanner due to issues such as damage or misprinting. Some jurisdictions hand count such ballots, while others create duplicate ballots so they can be read by a ballot scanner. Some jurisdictions permit election officials to enhance markings on ballots that are too faint to scan following a process to adjudicate the voter's intent based on state law. In jurisdictions where duplication of unscannable ballots is permitted, election officials duplicate the ballot precisely to ensure all the voter's choices are transferred correctly to the new ballot. 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.
- Link directly to this rumor by using: https://www.cisa.gov/rumorcontrol#rumor16

✔ Reality: Election night results are not official results.

✘ Rumor: If election night reporting sites experience an outage, vote counts will be lost or manipulated.

Get the Facts: Election night results are not official results. These sites may experience outages due to a variety of issues including too many people trying to view the site or cyberattacks. Such disruptions do not impact the integrity of votes or the official certified results. Election results made available on election night are always unofficial. Official results are rigorously

TLP:WHITE

canvassed (reviewed), and certified by local and state election officials. Most states have requirements for post-e

as well.

Useful Sources

- FBI-CISA Public Service Announcement: Foreign Actors and Cybercriminals Likely to Spread Disinformation Regarding 2020 Election Results
- FBI-CISA Public Service Announcement: Cyber Threats to Voting Processes Could Slow But Not Prevent Voting
- Post-Election Process Mapping Infographic, CISA
- Federal Election Results FAQs, CRS
- Link directly to this rumor by using: https://www.cisa.gov/rumorcontrol#rumor11

✔ Reality: A defaced or manipulated election night reporting webpage would not impact counting and certification of official results.

❌ Rumor: If the election night reporting webpage is defaced or displays incorrect results, the integrity of the election is compromised.

Get the Facts: If a webpage has been defaced or is displaying incorrect results, it would not impact the integrity of votes or the official certified results. Election results made available on election night are always unofficial.

Useful Sources

- FBI-CISA Public Service Announcement: Foreign Actors and Cybercriminals Likely to Spread Disinformation Regarding 2020 Election Results
- FBI-CISA Public Service Announcement: Cyber Threats to Voting Processes Could Slow But Not Prevent Voting
- Post-Election Process Mapping Infographic, CISA
- Link directly to this rumor by using: https://www.cisa.gov/rumorcontrol#rumor12

✔ 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
- #TrustedInfo2020, NASS

- Voter Resources: State Voter Information, NASED
- Voting and Elections Information, usa.gov
- Your local or state election officials EAC state-by-state directory
- Link directly to this rumor by using: https://www.cisa.gov/rumorcontrol#rumor1

✔ 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
- Link directly to this rumor by using: https://www.cisa.gov/rumorcontrol#rumor2

PRE-ELECTION

✔ Reality: Voting systems undergo testing from state and/or federal voting system testing programs, which certify voting system hardware and software.

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

Get the Facts: Before use in elections, voting systems undergo hardware and software testing to ensure they are consistent with state and/or federal requirements. Under these 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. Certification testing usually includes a review of a system's source code as well as environmental, security and functional testing. Depending on the state, this testing may be conducted by a state-certified laboratory, a partner university, and/or a federally certified testing laboratory.

Before local jurisdictions acquire voting systems, voting systems must go through a testing process to ensure compliance with the state's standards and, in many states, federal standards as well. While each state sets specific standards for voting systems, many states leverage the Voluntary Voting System Guidelines developed by the U.S. Election Assistance Commission.

Once systems are deemed compliant with applicable state and federal standards, jurisdictions also conduct logic and accuracy testing before deployment of a voting machine to ensure proper functioning and to detect any malicious or anomalous software issues. Post-election audits also help ensure the proper functioning of voting equipment.

Useful Sources:

TLP:WHITE

- 52 U.S.C. §§ 20971, 21081
- Voting System Certification Process, EAC
- Election Infrastructure Security, CISA
- Election Infrastructure Cyber Risk Assessment and Infographic, CISA
- Voting System Standards, Testing and Certification, NCSL
- Post-Election Audits, NCSL
- Your local or state election officials. EAC state-by-state directory
- Link directly to this rumor by using: https://www.cisa.gov/rumorcontrol#rumor23

✔ 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 remove deceased individuals from voter registration rolls based on death records shared by state vital statistics agencies and the Social Security Administration. While there can be some lag time between a person's death and their removal from the voter registration list, which can lead to some mail-in ballots being delivered to addresses of deceased individuals, death records provide a strong audit trail to identify any illegal 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 are actually innocuous clerical errors or the result of intended data practices. For example, election officials in some states use temporary placeholder data for registrants whose birth date or year is not known (e.g., 1/1/1900, which makes such registrants appear to be 120 years old). 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 lead 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 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
- Link directly to this rumor by using: https://www.cisa.gov/rumorcontrol#rumor21

✔ Reality: Some voter registration data is publicly available.

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

TLP:WHITE

Get the Facts: Some voter registration information is public information and is available to political campaigns, r and often members of the public, frequently for purchase. According to a recent FBI and CISA public alert, 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
- 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
- Link directly to this rumor by using: https://www.cisa.gov/rumorcontrol#rumor3

✔ 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 recent public alert, 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
- Link directly to this rumor by using: https://www.cisa.gov/rumorcontrol#rumor4

✔ 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
- Link directly to this rumor by using: https://www.cisa.gov/rumorcontrol#rumor5

✔ Reality: Malicious actors can fake manipulation of voter registration data to spre 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
- Link directly to this rumor by using: https://www.cisa.gov/rumorcontrol#rumor6

✔ 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 Source

- Mail-in Voting Election Integrity Safeguards Infographic, CISA
- Link directly to this rumor by using: https://www.cisa.gov/rumorcontrol#rumor7

✔ 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 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

TLP:WHITE

- 52 U.S.C. § 20303
- Voting Assistance Guide, FVAP
- Election Forms and Tools for Sending, FVAP
- 2016 Election Administration and Voting Survey Comprehensive Report, EAC
- Link directly to this rumor by using: https://www.cisa.gov/rumorcontrol#rumor8

ELECTION DAY

✔ 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 bleed 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
- Link directly to this rumor by using: https://www.cisa.gov/rumorcontrol#rumor18

✔ 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 violations. Intimidation or threatening behavior is never permissible.

TLP:WHITE

Under certain circumstances, the U.S. Department of Justice (DOJ) Civil Rights Division may monitor polling plac 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
- Link directly to this rumor by using: https://www.cisa.gov/rumorcontrol#rumor13

✔ 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
- Link directly to this rumor by using: https://www.cisa.gov/rumorcontrol#rumor9

✔ 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, impac 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
- Link directly to this rumor by using: https://www.cisa.gov/rumorcontrol#rumor10

Back to top

TLP:WHITE