This document is one in a series created as part of the Cybersecurity and Infrastructure Security Agency (CISA) Elections Infrastructure Government Coordinating Council and Sector Coordinating Council's Joint COVID Working Group. These documents provide guidance for state, local, tribal, and territorial election officials on how to administer and secure election infrastructure in light of the COVID-19 epidemic.

The Importance of Accurate Voter Data When Expanding Absentee or Mail Ballot Voting

Overview

Election officials expanding the use of absentee or mail voting must continually work to ensure that voter data is accurate. An incorrect name, address, or signature on file for a voter may result in that voter not receiving a ballot on time or at all, or their voted ballot not being counted. Up-to-date voter information helps promote election integrity, strengthen voter trust, increase candidate confidence in the outcome/process, and increase effective stewardship of scarce tax dollars.

All jurisdictions already engage in some form of voter registration or absentee list maintenance but mailing more ballots will exacerbate the problems caused by incorrect addresses on a voter registration list. Inaccuracies in address records can result from voter actions or omissions, such as moving to a new address without providing notice to election officials, or they can be caused by other factors, such as data entry errors. An initial mailing to voters, sent well before mailing any ballots, can give election officials an early indication of existing issues with their records and offer an early opportunity to clean up potential errors. This initial mailing could serve the dual purposes of explaining any coming changes to voters—including any COVID-19-related changes—and exposing potentially problematic addresses for election officials. It can also inform voters displaced because of COVID-19 (e.g., people living with family/friends, in care facilities) that they need to update their voter registration information, such as temporary mailing address. Election officials may also work with vendors that provide data on the change of address information of voters.

As jurisdictions increase the number of ballots they send by mail, election officials must prepare for some percentage of those ballots to be returned as undeliverable, which is a normal part of the process. Even Oregon—which has been sent every voter a ballot since 1998 and has a robust list maintenance program through its participation in the Electronic Registration Information Center (ERIC)—has 2–3 percent of its ballots returned as undeliverable in a federal

election. Washington, which has mailed every voter a ballot since 2005 and is a founding member of ERIC, recently estimated that approximately 10 percent of its ballots are returned as undeliverable. Jurisdictions considering expansion of their absentee or mail ballot programs should consider whether and how mailings or ballots returned as undeliverable can be used for list maintenance purposes.

Risks Associated with Incorrect Voter Records

Incorrect Address

- An incorrect address can result in the voter not receiving a ballot or in delayed receipt of the ballot.
- If the voter's address is incorrect, it may result in another person receiving a ballot that does not belong to him or her.
- If a ballot is returned to the election official as undeliverable by the United States Post Office, it may impact the voter's ability to receive an absentee or mail ballot in future elections unless the voter takes specific action to cure the issue.

Name on Voter Registration Record is Incorrect

- If a voter's name on their registration record is incorrect (e.g., their voter registration record is misspelled or has not been updated to reflect a name change), it could result in the voter not receiving a ballot package.
- In a state where absentee or mail ballot voters are required to submit voter identification while casting a mail ballot (e.g., providing a copy of a photo ID), the voter's identification would not match the name on the ballot package.

Outdated Signature(s) on File

- Outdated or lack of quality signature(s) in the voter's record could result in rejection of the voter's ballot package (in jurisdictions where signature match is required).

Operational Considerations

Methods for Correcting Voter Registration Records

- Does your state have online voter registration (OVR), or other electronic tools, that allow voters to verify and update their voter registration record easily?
- Can an application for an absentee ballot serve as a means for a voter to update his or her record?

- If a mail ballot (or piece of election office direct mail) is returned to the election office, can that trigger the process to update a voter record?
- If necessary, can voters request a mail ballot through the OVR system or separate online platform?
    - If not, can that feature be added?
- Does your state use United States Postal Service National Change of Address (NCOA) data for list maintenance?
    - How frequently do you run and process the NCOA list?

Because these processes for correcting inaccuracies sometimes require voters to take action, it is prudent to educate voters that these processes are available. Such outreach campaigns may be conducted via direct mail, email, the press, and social media, and should aim to educate all stakeholders on the importance of voters verifying and updating their voter registration record and are discussed in Election Education and Outreach for Increased Absentee or Mail Voting. These campaigns should begin 60 to 90 days before Election Day, educating voters on the importance of registering to vote or verifying/updating their voter registration to ensure their information is current. List maintenance mailings serve to provide voters an opportunity to confirm their residence or change of address with election officials. In states where voters must submit an application to receive an absentee ballot, these campaigns are most effective if they include mailing all non-absentee voters an absentee ballot application, allowing those voters to provide their current address information.

Voter Registration and Absentee Ballot Application

- Does your jurisdiction have deadlines for a voter to update his or her voter record and if applicable, apply for an absentee ballot?
    - Outreach efforts through direct mail, social media, and other methods should begin at least 60 days prior to Election Day to ensure adequate time to for election officials to receive and enter voter information and/or absentee ballot requests into the Voter Registration Database.
- How will you deal with a large influx of last-minute new voter registrations and updates?
    - National Voter Registration Day, Facebook voter registration drive, and other celebrity pushes to register generally create a large influx of changes to voter records.

Undeliverable Ballots

- How do you handle undeliverable ballots?
    - Do you proactively contact a voter if a ballot is returned as undeliverable?
    - Have you planned for staffing needs to deal with the undeliverable ballots?
- Do you have a process for updating a voter's record after a ballot has been sent?
- What is the last day that election officials can mail ballots in your state?
    - Many voters update their registration later than requested by the designated election official.

    - If a ballot is returned as undeliverable after the last day to mail ballots, how will you process the undeliverable ballot?
    - How can a voter whose ballot has been returned as undeliverable update their voter registration record and obtain a replacement ballot?
- Have you developed a process for supplemental or late mailings?
    - Your ballot printer and/or fulfillment center should be able to help you with supplemental ballot mailings.

Inbound Process

- Will the voter have an opportunity to update his or her voter record if the ballot package was rejected because the voter could not be authenticated?

Signature Cure

- It is helpful for voters to be notified when their ballot has been rejected because of a discrepant or missing signature and be given an opportunity to resolve the issue. In states with a formal process for this, election officials are typically required to notify the voter, often by mail, that they must complete another step for their ballot to be counted as cast. In states with a ballot tracking system, a voter could proactively check that system, which would notify them of the need to take an additional step to "cure" the ballot.
- Please be aware that this process may add time and an additional administrative layer to counting that ballot.

Securing Voter Registration Data

Using technology always comes with cybersecurity concerns. Those are exacerbated when individualized data is captured. As the 2016 General Election demonstrated, voter registration databases are targets for those looking to undermine public confidence in our elections. Unauthorized changes to a voter's record have the same impact as outdated information in the voter's record in that under both circumstances, the voter may not receive their ballot and/or have their ballot rejected upon receipt. To mitigate risks associated with the threat of an outsider making unauthorized changes to a voter record, consider the following recommendations:

Basic Prevention Measures

- Patch applications and operating systems—Vulnerable applications and operating systems are the target of most attacks. Ensuring these are patched with the latest updates greatly reduces the number of exploitable entry points available to an attacker.
- Use application whitelisting—Whitelisting is one of the best security strategies because it allows only specified programs to run while blocking all others, including malicious software.

- Restrict administrative privileges—This practice may prevent malicious software from running or limit its capability to spread through the network.
- Validate input—Input validation is a method of sanitizing untrusted user input provided by users of a web application and may prevent many types of web application security breaches, such as SQLi, XSS, and Command Injection.
- Understand the advantages of firewalls—When anyone or anything can access your network at any time, your network is more susceptible to attack. Firewalls can be configured to block data from certain locations (i.e., by using IP whitelisting) or applications while allowing relevant and necessary data through.

Questions to Consider:

- Do you back up all critical information?
    - Are the backup files stored offline?
    - Have you tested your ability to revert to backups during an incident?
- Have you conducted a cybersecurity risk analysis of your organization?
- Have you trained staff on cybersecurity best practices?
- Have you implemented regular scans of your network and systems, as well as appropriate patching of known system vulnerabilities?
- Do you allow only approved programs to run on your networks?
- Do you have an incident response plan, and have you practiced it?
- Can you sustain business operations without access to certain systems?
    - If yes, for how long?
    - Have you tested this sustainment capability and its duration?
- Have you or an outside entity conducted penetration tests on your systems (i.e., red team) to test the security of those systems and your ability to defend against attacks?
- Is your jurisdiction a member of the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)?
- Do you have Multifactor authentication (MFA) enabled for all users?
- Are you using a dot-gov (.gov) top-level domain (TLD)?

CISA provides some of these services at no cost to its state, local, tribal, and territorial (SLTT) partners, including vulnerability (a.k.a. Cyber Hygiene) scans, remote penetration testing (RPT), phishing campaign assessment. For a list of all CISA services, see the CISA Election Infrastructure Security Resource Guide. To request CISA services, contact CISAServiceDesk@cisa.dhs.gov. You can also sign up to become an EI-ISAC member by visiting https://www.cisecurity.org/ei-isac/

Resources

- Cybersecurity & Infrastructure Security Agency (CISA): Securing Voter Registration Data
- Election Assistance Commission (EAC): Checklist for Securing Voter Registration Data

- Center for Election Innovation and Research (CEIR): 2018 Voter Registration Database Security Report
- Department of Justice (DOJ): The National Voter Registration Act of 1993 (NVRA)