

Election Security Advance Planning Checklist

PUBLISHED DECEMBER 19, 2019

Prevent and Recover from Electronic Pollbook Failures and Outages

- Limit or eliminate connectivity to wireless networks whenever possible.**
- Implement proper security protocols when wireless connectivity is required.**
 - Encrypt all communications between e-pollbook units.
 - Adopt new and strong passwords after every election.
- Ensure systems are properly patched as part of Election Day preparations.**
 - Review and adhere to all guidelines or requirements created by state or local government IT agencies.
 - Use the National Institute of Standards and Technology (NIST) cybersecurity framework to develop any additional guidelines.
- Stay up to date on alerts from the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) about recent vulnerabilities and emergency security patches.
- Keep appropriate backup of e-pollbooks in polling places.**
 - Send paper backups of e-pollbooks to polling places with other printed materials.
 - If centralized voting locations are used and backup paper pollbooks are not feasible, arrange for these locations to have nonnetworked alternative devices containing the entire list of registered voters for the jurisdiction.
 - Evaluate recovery procedures to ensure they will be easy for poll workers to follow.
- Provide sufficient provisional ballots and materials for two to three hours of peak voting.**
 - Allow voters to use regular ballots whenever possible.

- Do not deny or delay providing provisional ballots where eligibility or registration is in doubt due to e-pollbook failure.

□ Train poll workers to implement pollbook contingencies.

- Include instructions for managing provisional ballots in case of e-pollbook failure.
- Make sure that each section of provisional ballot forms clearly instructs voters, poll workers, and election staff on what they need to do.

Prevent and Recover from Voting Equipment Failures

□ If using paper ballots, print sufficient ballots for 100 percent of registered voters.

□ If using direct-recording electronic (DRE) machines, ballot-marking devices (BMD), or ballot-on-demand (BOD) printers, print emergency paper ballots for two to three hours of peak voting.

- Make sure emergency paper ballots are in every polling place and poll workers have been trained to use them.
- Count emergency ballots without any additional scrutiny of voter qualifications.
- If using BMDs or BOD printers, program tabulators to accept and read emergency paper ballots.

□ Develop procedures to manage and track equipment failure.

- Take malfunctioning equipment out of service and deploy additional equipment to polling places when needed.
- Recalibrate DRE touchscreens and make any other necessary voting equipment repairs in full view of observers.
- Establish protocols for poll workers to notify the election office of equipment failures and other issues.

- Train poll workers on the process for counting paper ballots, including potential hand-counting.

□ Communicate with voters to build trust in the election process.

- Preprint signage that informs voters of equipment failures and include instructions with other polling place materials for when to post the signage.
- Remind voters to check their ballots or paper printouts for any errors.
- If equipment is not working during voting, provide information to voters about how their ballot will be counted.

□ Take steps to prevent late polling place openings.

- Train poll workers to deal with equipment failures occurring on Election Day morning.

□ Plan to assist voters with disabilities if accessible voting machines fail.

- Distribute backup accessible voting equipment — with all ballot styles available — to geographically dispersed areas.
- In the longer term, provide each polling place with accessible tablets and printers for voters with disabilities to use in the event of voting equipment failure.

□ Conduct a postelection manual audit of paper ballots or an audit trail to verify software totals.

Prevent and Recover from Voter Registration System Failures and Outages

□ Establish a 60-day preelection blackout window for all noncritical software updates and patches.

- Provide a process for emergency updates during the blackout window that specifies who will authorize them and how they will be tested prior to rollout.

Subject the system to independent vulnerability testing on a periodic basis.

- Conduct vulnerability testing well in advance of an election so that there is sufficient time to resolve potential vulnerabilities that are discovered.
- Be transparent about what entity will conduct the testing and what standards it will use.

Maintain backup copies of digital records offline in case online access is limited.

- In the weeks before the election, download an electronic copy of voter information daily and store it securely.

Provide voters with tools to look up their voter registration status online.

- Conduct outreach and urge voters to use the tool in advance of any registration deadline.

Provide voters with tools to look up their polling place information online.

- Be prepared to provide voters with alternative web pages, such as those offered by the Voter Information Project, in case of voter lookup tool failure.
- Provide accurate polling place data to the backup website in advance of the election and confirm that the backup website is working correctly.

Prevent and Recover from Election Night Reporting System Failures and Outages

Establish a redundant election night reporting system to be used in case of an outage.

Do not connect election night reporting systems to voting systems or the statewide registration system.

Develop a Communication Strategy

Draft, review, and approve a communication plan prior to Election Day.

Include key staff and other contacts in the plan.

Prior to Election Day, provide a public website for emergency communications.