BRENNAN
CENTER
FOR JUSTICE

Preparing for Cyberattacks and Technical Problems During the Pandemic

A Checklist for Election Officials

Election Administration and Infrastructure

Secure Remote Elections Office Operations

□ **Ensure that teleworkers comply with cybersecurity best practices.**

» Use National Institute of Standards and Technology (NIST) guidance to develop technology security policies for all personnel.

» Require personnel to update devices regularly and use two-factor authentication.

» Train personnel to avoid phishing attacks, rogue Wi-Fi hot spots, and other malicious activity.

□ **Prepare for remote work and social distancing in the weeks leading up to the November election.**

» To ensure that critical functions can continue, cross-train staff to perform multiple roles.

» Determine what tasks can be performed remotely and obtain all necessary equipment for them.

Prevent and Recover from Voter Registration System Failures and Outages

□ **Establish blackout windows for noncritical software updates and patches, as well as a testing and authorization protocol for any critical updates.**

» Establish 60-day blackout windows for noncritical updates.

» Require personnel, vendors, and other agency staff to obtain express permission to install any critical patches during the blackout window, and test updates prior to rollout.

□ Subject the system to periodic independent vulnerability testing and automated monitoring.

» Conduct vulnerability testing well in advance of an election so that there is sufficient time to resolve any potential vulnerabilities that are discovered.

» Use automated monitoring tools and intrusion detection services to alert election officials when sites are down.

» Send confirmations of online address changes to voters by email, text, or mail.

□ Maintain backup copies of digital records off-line in case online access is limited.

» Make backups daily during critical periods and weekly during noncritical periods.

□ Build in resiliency measures to prevent and recover from online voter registration failure.

» Consult IT personnel about how to avoid overloading registration database servers during peak use. Consider batching registration requests and using content delivery network services.

» If registration systems do fail, automatically redirect voters to a different site where they can submit their registration information before applicable deadlines.

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

» Conduct outreach and urge voters to use the lookup tool in advance of the registration deadline.

Mail Voting

Prepare for Increased Printing and Processing

□ Print enough mail-in ballots and envelopes to mail them to all voters if needed.

» Review envelope design for usability and ease of processing through U.S. Postal Service systems before printing.

» If possible, allocate unused mail ballots for in-person voting as Election Day approaches.

□ Ensure that printing vendors meet best practices for data integrity and physical security.

» Require vendors to keep printed ballots physically secure and to maintain chain-of-custody logs.

» Protect voter information by encrypting all locally stored data containing personally identifiable information (PII) and making sure that vendors can accept encrypted data files.

» Ensure the accuracy of address and ballot style data by authenticating users before transferring files and using hash validation to guarantee that the transferred files match the originals.

Prevent and Recover from Mail Ballot Request or Processing Failures

□ Secure online and email mail ballot request systems.

» Subject systems to load and vulnerability testing.

» Check the capacity of email servers, and scan attachments for viruses.

» Use automated monitoring tools and intrusion detection to catch cyberattacks and alert officials when systems are in danger of overloading.

» Block automated requests using mechanisms such as reCAPTCHA.

» Ensure that systems do not display voter PII.

» Implement web application firewalls that protect against injections of malicious code.

» Use email and text confirmations after a voter makes a request.

» If online ballot request systems fail, automatically redirect voters to a different site where they can submit requests before applicable deadlines.

□ **Provide voters with notice and an opportunity to cure mail ballot request deficiencies, and track problems. Distribute secure drop boxes and offer provisional mail ballots as a fail-safe.**

□ **Secure signature databases by encrypting network connections and using strong passwords that are changed after every election.**

» Back up signature databases regularly to ensure that a system failure does not prevent mail ballot processing.

□ **Provide voters with notice and an opportunity to correct mail ballot errors, such as unverifiable or missing signatures.**

□ **Choose remote accessible vote-by-mail technology that provides access to more voters with disabilities without risking election integrity or voters' ballots.**

» Provide an electronic ballot that voters can download, mark off-line using their own assistive technologies, print out, and mail or drop off.

□ **Provide for public observation of the processing and canvassing of mailed ballots under conditions of social distancing.**

In-Person Voting

Prevent and Recover from Electronic Pollbook Failures and Outages

□ **Limit or eliminate connectivity to wireless networks whenever possible.**

□ **When wireless connectivity is required, implement proper security protocols.**

» Encrypt all communications between e-pollbook units.

» Adopt new and strong passwords after every election.

□ **Ensure that systems undergo reliability testing and 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 and use the NIST cybersecurity framework to develop additional guidelines.

» Stay up to date on alerts from the Election Infrastructure Information Sharing and Analysis Center about recent vulnerabilities and emergency security patches.

» Where possible, ensure that each e-pollbook contains a backup of the full check-in roster.

□ **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.

- » Ensure that recovery procedures can be quickly and effectively implemented.

Provide Sufficient Paper Ballots and Provisional Envelopes

□ If using preprinted paper ballots as the primary in-person voting method, print enough ballots for 120 percent of all registered voters who have not requested a mail ballot.

- » If possible, avoid double printing by re-allocating unused mail ballots for use during in-person voting.

□ Provide sufficient provisional ballot materials to cover more than three hours of peak voting — usually enough for 40 percent of registered voters.

- » Allow voters to use regular ballots whenever possible.
- » If a voter's eligibility or registration is in doubt due to an e-pollbook failure, do not deny or delay providing a provisional ballot.

□ Train poll workers to implement contingencies.

□ Create easy-to-use systems for alerting election officials when supplies are running low.

Prevent and Recover from Voting Equipment Failures

□ If using direct-recording electronic (DRE) machines, ballot-marking devices (BMDs), or ballot-on-demand (BOD) printers, provide enough emergency paper ballots to cover two to three hours of peak voting activity — usually enough for 35 percent of registered voters.

- » Make sure that emergency 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.
- » When possible, program tabulators to accept and read emergency paper ballots.
- » At vote centers, stock emergency ballots for the most heavily used precincts.

□ Develop procedures to manage and track malfunctioning equipment or equipment failure.

- » Establish protocols to track malfunctioning equipment, take it out of service, and deploy additional equipment to polling places where needed.
- » If in-precinct scanners are not working, store ballots securely until they can be counted.
- » Recalibrate touch screens and make any other necessary voting equipment repairs in full view of observers.
- » Train poll workers on the process for counting paper ballots, including hand counting when necessary.

□ 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 it.
- » Remind voters to check their ballots or paper printouts for any errors.

□ Train poll workers to deal with equipment failures occurring on Election Day morning to prevent late poll openings.

□ **Plan to assist voters with disabilities if 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 as backup for voters with disabilities.

Results Reporting, Certification, and Public Communications

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.**

□ **Conduct robust precertification audits that the public can observe under social distancing guidelines.**

Make Needed Public Information Easily Accessible

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

- » Prepare for increased use of election websites and provide backup sources in case of failure.

□ **Prepare to hire backup phone attendants to guide voters through election changes.**

□ **Educate voters and the media in advance about the canvassing process and when results can be expected.**

□ **Design reporting websites and educate the media to avoid misunderstandings about how many votes have been counted and how many have yet to be processed.**

□ **Provide emergency communications on public websites.**

Develop a Communications Strategy

□ **Draft, review, and approve a communications plan prior to a negative development on or before Election Day.**

- » Include key staff and other contacts in the plan.