POLICY REPORT

BRENNAN CENTER FOR JUSTICE

Preparing for Cyberattacks and Technical Problems During the Pandemic

A Guide for Election Officials

By Edgardo Cortés, Gowri Ramachandran, Liz Howard, Derek Tisler, and Lawrence Norden

PUBLISHED JUNE 5, 2020

Brennan Center for Justice at New York University School of Law

Table of Contents

ABOUT THE BRENNAN CENTER FOR JUSTICE

The Brennan Center for Justice at NYU School of Law is a nonpartisan law and policy institute that works to reform, revitalize — and when necessary defend — our country's systems of democracy and justice. The Brennan Center is dedicated to protecting the rule of law and the values of constitutional democracy. We focus on voting rights, campaign finance reform, ending mass incarceration, and preserving our liberties while also maintaining our national security. Part think tank, part advocacy group, part cutting-edge communications hub, we start with rigorous research. We craft innovative policies. And we fight for them — in Congress and the states, in the courts, and in the court of public opinion.

STAY CONNECTED TO THE BRENNAN CENTER

Visit our website at **www.brennancenter.org**

Introduction

Over the past year, many state and local election jurisdictions have taken crucial steps to improve election security, such as replacing paperless voting equipment with paper ballots and disconnecting ballot scanners from networked election night reporting systems. They have also taken steps to enable a recovery from potential cyberattacks or technical failures, such as requiring polling places to keep emergency paper ballots on hand in case of equipment breakdowns.

Now, election officials face the additional challenge of ensuring secure and safe elections in the midst of a pandemic. Since officials cannot know at this moment whether all of their voters will feel safe voting in person in November, they must prepare for the possibility that a significant portion will opt to vote by mail. At the same time, they must maintain in-person voting options, which are necessary for many, including some voters with disabilities and those with poor mail service.

Deploying or scaling up new voting options can increase the risk of technical malfunctions, but officials have no choice in the current environment but to meet the challenge. Voters are already placing increased demands on online registration systems and mail ballot options. At the same time, the risk of cyberattacks from foreign state and nonstate actors alike remains. Many government personnel must work and access election infrastructure remotely now; so too must vendor personnel. These changes to work environments, if not properly managed, could create new targets for those interested in disrupting American elections through cyberattacks.

Effective digital resiliency plans can ensure that operations continue and eligible citizens are able to exercise their right to vote even in the face of cyberattacks or technical malfunctions. This document seeks to assist officials as they revise their cyber resiliency plans in light of Covid-19. We highlight areas that warrant heightened attention, such as the resiliency of websites and online registration tools. While we recognize that the pandemic raises a variety of new requirements for election administration, we focus here on resiliency against cyberattacks and technical failures. In addition to assisting election officials with their plans, this document and the accompanying checklist can help advocates and policymakers working to ensure that election offices are prepared to handle these uncertainties.

Making the changes necessary to run credible and secure elections this November will cost money, and we urge Congress to provide states with the resources they need to ensure that local election officials can run safe and secure elections this fall.

Election Administration and Infrastructure

Due to concerns about Covid-19, election administration is now more than ever being performed and infrastructure accessed remotely. Election administration and related government functions, such as those carried out by motor vehicles departments, are being undertaken with many employees, including vendors' staff, working from home in order to comply with social distancing guidance and shelter-in-place orders. Voters and third-party organizations, also subject to these orders and guidance, are similarly using online capabilities to register, renew driver's licenses (thereby having the opportunity to register to vote or update registrations), update addresses, request mail ballots, and look up information, whether about elections and election changes generally or about their status as voters.

Even if states and localities slowly relax shelter-in-place orders, many voters will continue to limit their in-person interactions and will prefer to use online tools for election-related transactions. Personnel, too, may continue working from home. In any case, the possibility of a local outbreak or overall surge in Covid-19 cases will remain a risk through November.[1] Any such outbreak may result in renewed shelter-in-place orders and more restrictive social distancing guidance from public health officials.

Secure Remote Elections Office Operations

Many employees who may need access to voter registration databases are working from home or away from their traditional work sites during the pandemic.[2] These include elections personnel, vendor personnel, and personnel who work for other state agencies, such as the Department of Motor Vehicles. This added pressure creates new targets for those interested in disrupting American elections through ransomware or other cyberattacks.[3] Good cybersecurity practices for remote operations are therefore essential.

Ensure that teleworkers comply with cybersecurity best practices.

Election officials should take stock of the technology their teams are using, such as videoconferencing and chat services; evaluate it against national cybersecurity standards and their own policies; and solicit help as needed to ensure compliance.

- **Use national cybersecurity standards to develop technology security policies for all personnel.**[4] Relevant national cybersecurity standards include the National Institute of Standards and Technology's (NIST) *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*.[5] A jurisdiction's own policies may already include continuity-of-operations plans and policies for remote workers that mandate officially approved tools and services, such as virtual private networks (VPNs).[6] The Center for Internet Security (CIS) provides a guide for protecting employees' personal home networks.[7] NIST's guidance on data integrity may also be of use, as remote access to voter information and voter registration databases is a concern.[8]

- **Require personnel to update devices regularly.** State and local offices should regularly install updates on, or "patch," devices that are used to work at home, including laptops, tablets, phones, and home routers.[9] Operating systems, browsers, and other applications used by workers should also be patched. If the IT department approves, auto-updates should be turned on.

- **Train personnel to avoid phishing attacks, rogue Wi-Fi hot spots, and other malicious activity.** If officials have not already partnered with an organization or agency to provide this training to all personnel, they should seek out the assistance of state and federal partners, who often tailor these programs specifically for election officials.

- **Use two-factor authentication.** Requiring two-factor authentication for all log-ons is a simple way to reduce the odds of unauthorized access to sensitive infrastructure.

- **Check whether other teleworking personnel are complying with cybersecurity standards.** Personnel employed by vendors and state agencies such as the Department of Motor Vehicles can have a significant impact on election security. Election officials should make sure that those personnel are also being held to cybersecurity standards.

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

Although shelter-in-place orders may be eased over the months to come, election officials should prepare for the possibility of a local outbreak or one or more employees being infected with the coronavirus.

- **Cross-train staff and consider how staff from other agencies may provide assistance.** This will ensure that critical functions can continue in the event key personnel fall ill, particularly in smaller jurisdictions with a small staff.

- **Determine what tasks can be performed remotely and obtain all necessary equipment for them.** Outbreaks may require critical personnel to work remotely without advance warning, perhaps even in the weeks or days just prior to the election. If a jurisdiction's continuity-of-operations plan does not already include the types of cybersecurity standards for remote working described above, they should be incorporated. Officials should obtain the equipment that personnel who perform critical functions would need for compliance, such as laptops, home high-speed internet access, and VPNs. If other agencies are forced to close nonessential operations, they may be able to loan resources such as computers. Telecommunications providers may be willing to make accommodations for essential government personnel, including elections staff. Planning for staff who must stay home to remotely answer the telephone can reduce stress on those who must work in person to perform functions such as preparing mail ballot packets.

- **Have a backup communications channel for personnel in case email is not working.** Communications channels enabling teams to collaborate and share information, such as Slack, Microsoft Teams, or text messaging, can serve as a useful backup in case email fails at a critical time.

More Resources

Election Assistance Commission
Coronavirus (Covid-19) Resources
https://www.eac.gov/election-officials/coronavirus-covid-19-resources

Cyber and Infrastructure Security Agency
Telework Guidance and Resources
https://www.cisa.gov/telework

Cyber and Infrastructure Security Agency
#Protect2020 (Covid-19 and Elections)
https://www.cisa.gov/covid-19-and-elections

U.S. Department of Homeland Security
Incident Handling Overview for Election Officials
https://www.dhs.gov/sites/default/files/publications/Incident%20Handling%20Elections%20Final%20508.pdf

Cyber and Infrastructure Security Agency
Ransomware
https://www.dhs.gov/sites/default/files/publications/19_1007_cisa_ransomware-cisa.pdf

Election Assistance Commission
Deep Dive: Election Technology
www.eac.gov/documents/2018/05/01/eavs-deep-dive-election-technology

National Cybersecurity Center of Excellence
Data Security Project
https://www.nccoe.nist.gov/projects/building-blocks/data-security

Global Cyber Alliance
Practical Steps to Help You Work from Home Securely
https://workfromhome.globalcyberalliance.org

Global Cyber Alliance
Cybersecurity Toolkit for Elections
https://gcatoolkit.org/elections

Prevent and Recover from Voter Registration System Failures and Outages

A voter registration system maintains a jurisdiction's official list of registered voters, including all voter information and district assignment information. Statewide voter registration systems usually serve additional election-management purposes, such as processing the receipt of mail ballots and verifying signatures. A failure of the system on or near Election Day can cause problems in producing address lists for sending out mail ballot applications, providing accurate information on polling place lookup sites, generating files for paper voter rosters or e-pollbooks, using voter information lookup tools, or validating and canvassing provisional and mail ballots.

A resilient voter registration database, while always important, is especially so now: a compromised database poses particular problems to voters who need to stay home during the pandemic. The accuracy of address lists and other voter registration data impacts whether voters receive their mail ballot request forms, mail ballots, and notices from the elections office, as well as whether they can effectively use tools such as online mail ballot requests. Furthermore, once ballots are mailed in, these lists are used for signature matching and other verification mechanisms. If the data is incorrect, voters could show up at the polling place to be told erroneously that they have already voted by mail and must cast a provisional ballot.

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

With the surging popularity of vote-by-mail methods brought on by the pandemic, Election Day is not the only critical date on which a compromised registration database can profoundly impact voters. Dates on which address lists are created for mail ballots or other large mailings and the beginning of the early-voting period are also critical moments for database security.

- **Establish 60-day blackout windows for noncritical updates.** Creating blackout windows — periods in which noncritical updates are not permitted — prior to critical dates increases the likelihood that any programming errors, viruses, or other problems will be discovered in a timely manner, before mail ballots are sent or in-person voting is held. Coordinating with state and local technology staff is imperative to determine effective and reasonable blackout windows. Sixty days provides sufficient time before each critical date, such as the close of voter registration and the start of mail voting, to identify unintended system issues caused by patches or updates.

- **Require express permission to install any critical patches during the blackout window, as well as testing.** Even updates not associated with the voter registration database, such as server patching, networking equipment upgrades, and locality telecommunication system changes, can impact a local election official's ability to access the state voter registration database. For this reason, blackout dates must be established and communicated to personnel, vendors, and other relevant staff to prevent potential issues in advance of critical periods and on or shortly before Election Day. The plan should indicate who will assess how critical these updates are and authorize that they be made, and how they will be tested prior to rollout. Ideally, updates should be tested in an environment that mirrors the actual database and connections to that database.

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

Remote access to and usage of the voter registration database may surge due to the pandemic or particular outbreaks, with voters making greater use of online registration and election personnel needing to work from home. This increases the risk and impact of malfunctions or attacks, including distributed denial of service (DDoS) attacks. There are several entities that states can partner with for critical assessment and testing. For example, the U.S. Department of Homeland Security offers free vulnerability scanning to state and local officials and their vendors. States can also partner with the National Guard or engage cybersecurity consultants.

- **Conduct vulnerability testing well in advance of an election.** Vulnerability and capacity testing should be conducted well in advance of key dates in the election calendar, such as registration and mail ballot request deadlines, planned dates for producing address lists for mailings, and Election Day. Testing should occur at least quarterly to provide sufficient time to resolve any potential vulnerabilities that are discovered. While the specific results of vulnerability testing should not be released (to maintain system security), officials should be transparent about the entity conducting the testing and the standards it is using. If systems will be off-line for testing, notice should be provided to voter outreach groups well in advance.

- **Use automated monitoring tools and intrusion detection services.** Automated monitoring tools, such as Pingdom, and intrusion detection services, such as Albert sensors, can alert officials when sites are down or have been infiltrated.[10] So can trusted nonpartisan voter outreach groups, to whom officials can give contact information that can be used during evenings and on weekends.

- **Send confirmations of online address changes.** If voters are sent confirmations by email, text, or mail (to their old contact information) when changes to their address are requested online, they can alert officials to alterations that they did not ask for. Any such reports should be investigated.

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

Increased mail voting during the pandemic requires increased attention to the resiliency of voter registration databases in the lead-up to key election calendar dates, such as mail ballot request deadlines.

- **Make daily backups during critical periods.** As key election calendar dates approach, local officials should back up an electronic copy of voter information every day and store distinct copies rather than overwriting previous backups, so they have the most recent information should the voter registration system become unavailable. These backups must be stored separately from the voter registration system to avoid being impacted by a ransomware attack.

- **Make weekly backups during noncritical periods.** During other periods, weekly backups of the full database are standard. Daily backups should still be made of each day's transactions, including those made by phone, on paper, and online. These backups can also be used to research mail and provisional ballots after the election and should be stored off-site, apart from general operations.

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

Use of online registration can be expected to surge due to the pandemic or particular outbreaks, increasing the risk and impact of technical problems that cause a website to fail.

- **Consult IT personnel about how to avoid overloading registration database servers during peak use.** Officials should consult their IT departments and obtain the services of a content delivery network (CDN), which prevents downtime by distributing workload across multiple servers in different regions. They should also batch registration requests for processing to avoid overloading the registration database server during peak times. Properly employed, these services can help protect against DDoS attacks.

- **If registration systems do fail, automatically redirect voters to a different site where they can submit their registration information before applicable deadlines.** In case of a failure of the registration website, the CDN service should automatically redirect voters to a site where they can access a fillable PDF to be uploaded for follow-up by election officials. These voters should be treated as having submitted their registration request at the time they provided their information on the redirect page. The state of Virginia uses a redirect function of this sort to serve as a fail-safe.[11]

Provide voters tools to look up their registration status online.

Voters can supply crucial insights about undesired changes to their registration, such as address changes they did not request, serving as early indicators of a possible breach.

- **Conduct outreach and urge voters to use the lookup tool in advance of the registration deadline.** Encouraging voters to check before a deadline ensures that problems can be resolved in a timely fashion so that they can participate. It can also reduce pressure on poll workers on Election Day.[12]

More Resources

Cyber and Infrastructure Security Agency
#Protect2020 (Covid-19 and Elections)
www.cisa.gov/covid-19-and-elections

Cyber and Infrastructure Security Agency
Election Infrastructure Security Resource Guide
https://www.dhs.gov/sites/default/files/publications/19_0531_cisa_election-security-resources-guide-may-2019.pdf

Election Assistance Commission
Election Security Preparedness
https://www.eac.gov/election-officials/election-security-preparedness

Center for Internet Security
Security Best Practices for Non-Voting Election Technology
https://www.cisecurity.org/wp-content/uploads/2019/11/Security-Best-Practices-Non-Voting-Election-Tech-Singles-19-Nov.pdf

MITRE
Recommended Security Controls for Voter Registration Systems
https://www.mitre.org/sites/default/files/publications/pr-19-3594-recommended-security-controls-for-voter-registration-systems.pdf

Election Assistance Commission
Deep Dive: Election Technology
www.eac.gov/documents/2018/05/01/eavs-deep-dive- election-technology

Pew Charitable Trusts
Upgrading Voter Registration
www.pewtrusts.org/en/projects/election-initiatives/about/upgrading-voter-registration

Election Assistance Commission
Checklist for Securing Voter Registration Data
www.eac.gov/documents/2017/10/23/checklist-for- securing-voter-registration-data

U.S. Department of Homeland Security
Securing Voter Registration Data https://www.dhs.gov/sites/default/files/publications/Securing%20Voter%20Registration%20Data_508.pdf

National Cybersecurity Center of Excellence
Data Security Project
www.nccoe.nist.gov/projects/building-blocks/data-security

National Cybersecurity Center of Excellence
Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events
https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/identify-protect

Mail Voting

Most jurisdictions provide ballots by mail without the voter needing to give a specific reason.[13] This is an option that many voters following social distancing guidance or complying with shelter-in-place orders have sought to take advantage of during the pandemic.[14] Even in jurisdictions that require voters to provide a specific reason when requesting a ballot by mail, many more voters may qualify when social distancing guidelines are in place.[15] And some governors may exercise emergency authority to modify election rules.[16] Even if the pandemic subsides in the next few months, the possibility of a resurgence or localized outbreak in the fall means that all jurisdictions must prepare for rapid and large increases in the use of mail voting in November.

Prepare for Increased Printing and Processing

Preparing for large increases in mail voting requires placing orders to print and process mail ballot kits well in advance of the November election. Although these preparations may seem costly, the pandemic necessitates unexpected changes to the way election officials must prepare, particularly for an election in which historic turnout has been predicted.[17] Fortunately, many of the supplies (such as envelopes) that must be ordered to prepare for this possibility can be used in future elections, and others (such as paper ballots) for in-person voting in November.

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

A last-minute surge in mail ballot requests may require printing many more ballots and envelopes than a jurisdiction has used in the past. Massive print orders of this sort may not be fillable at the last minute, particularly for specialty envelopes.[18] Based on historical data showing last-minute voter registration, anticipated increases in the use of mail balloting this November, and the likelihood that some first-time mail voters will need replacements, officials should order enough mail ballots and envelopes to mail to at least 120 percent of registered voters.[19] Jurisdictions with same-day registration or registration deadlines very close to the election may require an even larger supply.

- **Review envelope design for usability and ease of processing through U.S. Postal Service (USPS) systems before printing.** Many voters will likely be using mail ballots for the first time, and so ballots and envelopes should be designed for ease of use. The Center for Civic Design offers free templates that have been prepared with usability in mind.[20] USPS mail-piece design analysts are available to review envelopes to ensure that they can be processed quickly so that voters receive and can return them in time.[21]

- **Allocate unused mail ballots for in-person voting as Election Day approaches.** In most jurisdictions, costs can be mitigated by saving unused mail ballot envelopes for use in future elections. In many jurisdictions, unmailed ballots can be used for in-person paper ballot voting or as emergency ballots to recover from voting equipment failures or a low supply of regular paper ballots.

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

Some jurisdictions may need to work with new vendors in order to fulfill increased printing and mail processing needs due to surges in demand for voting by mail.

- **Require vendors to keep printed ballots physically secure and to maintain chain-of-custody logs.** Officials should require that vendors keep printed ballots and by-mail packets in locked rooms, with access limited to authorized personnel. They should maintain access and chain-of-custody logs for all finished materials, including ballots and by-mail envelopes.

- **Protect the privacy of voter information.** Officials should make sure that the vendor can accept encrypted data files and that data transfer occurs over an encrypted channel. Officials should also encrypt all locally stored data containing voters' personally identifiable information (PII).

- **Ensure the accuracy of address and ballot style data.** To ensure accuracy, election officials and vendors should both authenticate users before transferring a file and use hash validation to ensure that the transferred files match the originals. Vendors should limit the users who can access the data and permit officials to sample and review printed ballots and envelopes for accuracy *before* full production of the materials begins, in order to catch potential errors.

Prevent and Recover from Mail Ballot Request or Processing Failures

Secure online and email ballot request systems.

Some jurisdictions may be providing or promoting online mail ballot request or address change tools for the first time, in order to accommodate increased demand due to the pandemic. In other jurisdictions, demand for these tools will be much higher than has been typical in the past. Increased use of these systems means that a cyberattack could be far more damaging than it would have been in previous elections.

- **Subject systems to load and vulnerability testing.** States can either partner with the U.S. Department of Homeland Security or the National Guard or engage cybersecurity consultants to test systems periodically for vulnerabilities and for their readiness to deal with increased demand.

- **Check the capacity of email servers and scan attachments for viruses.** Many jurisdictions permit voters to submit an image of their signed mail ballot request form by email. Most email servers have a default setting that caps the amount of email that can be received. If a surge in mail ballot requests exceeds this cap, emails will bounce back and requests that were sent on time will not be processed. Some servers are set to block large attachments, or to filter most emails with attachments into a spam folder. Election officials should consult with their IT department to revise settings so that surges in emails from voters are accommodated and attachments can be opened safely. Officials should consider providing voters an email address dedicated to receiving forms. The inbox and attachment capacity for this address should be increased, spam filters loosened, and virus-scanning software employed. In case the software misses a malicious message, these emails should be opened on machines that have added access control and network restrictions.

- **Use automated monitoring tools and intrusion detection to catch cyberattacks, and alert officials when systems are in danger of overloading.** Tools such as Pingdom or Albert sensors can alert officials when websites are breached or traffic is excessive.

- **Block automated requests using mechanisms such as reCAPTCHA.** Automated requests for address changes should be blocked.[22] Officials should also put in place monitoring for suspicious changes, such as multiple changes from the same IP address occurring at rapid speed, unexplained increases in the rate of requests made, or unauthorized access to application programming interfaces (APIs) that are used by authorized groups to help voters complete their transactions.

- **Ensure that systems do not display PII.** Officials should make certain that systems do not display PII, such as full date of birth or residence, to prevent the capture of this information by malicious actors. Rather than volunteering sensitive information — for instance, by asking "Which of these addresses have you lived at?" — systems should instead validate information provided by the voter without displaying that information on-screen. Sensitive voter information provided by the system can be harvested by malicious actors and used elsewhere, for instance to engage in fraudulent financial transactions.

- **Implement web application firewalls.** These firewalls can provide some protection to web applications, such as online mail ballot request tools, against various attacks, such as a structured query language (SQL) injection. An SQL injection can input malicious code rather than legitimate user data into the ballot request form and use it to query the registration database without authorization, thereby potentially obtaining sensitive information.

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

When officials have an email address or mobile number on file for a voter, confirmation should be sent after a mail ballot is requested, so that if malicious changes or requests are being made, the voter can alert officials to the potential security breach. These confirmations should be sent to all email addresses and mobile numbers previously on record. They should include instructions for voters on where to report changes they did not request, and any such reports should be investigated. Officials should make clear to voters that they should expect such confirmations. This will also allow voters to notify officials when they have submitted an application but have not received a notice (perhaps indicating something is preventing applications from being received or processed).

- **When online ballot request systems fail, automatically redirect voters to a different site where they can submit requests before applicable deadlines.** The use of online ballot request and address-change tools may surge during the pandemic or a future outbreak, which increases the risk and impact of website failures. Officials should consult their IT departments and obtain the services of a content delivery network, as described above for online voter registration sites. In case of a site failure, these services should automatically redirect voters to an alternate site where they can access a fillable PDF to be saved for follow-up by election officials. These voters should be treated as having submitted their requests at the time they provided their information on the redirect page.

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.

If the statewide voter registration database is corrupted, voters might erroneously appear to be unregistered, to reside at a different address, or as having already requested a mail ballot. Providing voters with notice and an opportunity to cure any deficiencies in mail ballot requests, and tracking such problems, can alert officials to errors in the database so that they can be investigated. In addition, providing plenty of secure drop boxes as an alternative to U.S. mail allows for the timely return of mail ballots that were sent late as a result of the need to cure deficiencies. If there is no time left to cure the deficiencies, officials should send a provisional mail ballot rather than rejecting the application. Provisional ballots must be offered as a fail-safe, ensuring that problems with the database do not prevent eligible voters from voting, whether from their homes or at a polling place.

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

Mail-in and provisional ballots often require signature verification under state law. In some jurisdictions, signature-checking protocols involve the use of software that connects to a database, often the voter registration database, containing an electronic image of the voter's signature, or multiple such signatures, on file. The software can automate the process of pulling these images for staff to review or for an automated comparison that some jurisdictions use.

- **Encrypt communications between the signature database and software used during signature matching.** Officials should encrypt communication between the signature database, which is often part of the voter registration database, and computers used in mail ballot processing.

- **Limit access to the database.** Officials should require strong passwords that are changed after every election. NIST's "Cybersecurity Framework," "Guide to Protecting the Confidentiality of Personally Identifiable Information," and resources on data integrity may inform officials in ensuring the security of signature and registration databases, as well as in protecting voters' PII.[23]

- **Back up the database regularly.** Just like the registration database, any separate signature databases should be backed up regularly to ensure that, if network connections fail or the database is compromised, there is still a means by which to process large numbers of mail ballots.

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

By notifying voters of errors and providing an opportunity to cure before rejecting ballots, officials can distinguish possible malicious attacks that require investigation from more common issues, such as a voter's signature changing over time, household members mixing up envelopes, and other innocent errors.

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

Some voters may not be able to vote privately and independently on paper ballots sent to them by mail. Officials can offer these voters a remote accessible vote-by-mail option that allows them to receive an electronic ballot, download it, mark it off-line using their own assistive technologies, print it out, and mail it or drop it off. California has conditionally certified three systems that provide this option.[24] As this is not feasible for all voters with disabilities, accessible in-person voting options must still be made available.

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

Video streams or rooms with more space may be necessary to permit candidates, party representatives, the media, and the public to observe processing and canvassing while keeping their distance from one another and from elections staff. If video observation is the only means provided for observation, place cameras in locations that permit viewers to observe officials' rejection and acceptance of ballots, as well as any duplication of ballots needed in order for them to be placed in scanners.

More Resources

Cyber and Infrastructure Security Agency
#Protect2020 (Covid-19 and Elections)
https://www.cisa.gov/publication/covid-19-election-resources

Center for Civic Design
A Tool Kit of Resources for Scaling Up Vote by Mail
https://civicdesign.org/tool-kit-for-scaling-up-vbm

Election Assistance Commission
Voting by Mail/Absentee Voting
https://www.eac.gov/election-officials/voting-by-mail-absentee-voting

Center for Civic Design
Principles and Guidelines for Remote Ballot Marking Systems
https://civicdesign.org/wp-content/uploads/2015/09/Principles-for-remote-ballot-marking-systems-16-0210.pdf

In-Person Voting

While the popularity of options for voting at home will likely increase due to the pandemic, it is difficult to predict how many voters will take advantage of mail ballots and how many will choose to vote in person, particularly if the pandemic has largely subsided by November.[25]

In California's March 4, 2020, election, voting by mail and early in-person voting was available to many voters, but fewer voters than expected made use of these options. On Election Day, voters across the state faced long lines as vote centers were overwhelmed by in-person turnout, a problem exacerbated by equipment malfunctions and other difficulties.[26] Voters encountered lines of four hours at numerous sites.[27] This November, voters may choose to vote in person in significant numbers; they might even be forced to, if mail service is significantly disrupted or processing difficulties and errors lead to delays in receiving mail ballots. In Wisconsin's April 7, 2020, election, many ballots were mailed out to voters too late. By the Saturday before the election, about 16,000 ballots, or more than 1 percent of those requested, had not been mailed out.[28]

Prevent and Recover from Electronic Pollbook Failures and Outages

Electronic pollbooks, or e-pollbooks, are laptops or tablets that poll workers use instead of paper lists to look up voters. When functioning properly, e-pollbooks expedite the administration process, shorten lines, lower staffing needs, and save money. Most e-pollbooks can communicate with other e-pollbooks in the same polling location to share real-time voter check-in updates. They may also be able to communicate directly with a local election office or with other locations, such as vote centers, via physical connections or wireless networks. This feature can reduce the need for provisional voting by those who were mailed but did not receive a mail ballot or who received but misplaced theirs. It may be particularly helpful in reducing the frequency of lines and crowds at in-person polling locations during and in the wake of the pandemic.

There is no federal certification of e-pollbooks for operations or security. E-pollbooks present unique challenges because they need to maintain updated information across numerous devices and locations. Additionally, many modern devices that can be used as e-pollbooks do not have the ability to connect via physical networks and require some type of wireless connectivity to communicate important information.

Limit or eliminate connectivity to wireless networks whenever possible.

E-pollbooks used in polling places on Election Day for voter check-in purposes generally do not need wireless connections, including Bluetooth, cellular, or Wi-Fi connections.[29] Officials who operate precinct-based voting on Election Day should choose an e-pollbook option that uses hardwired connections to share voter information in real time across units to complete the voter check-in process. This provides the greatest level of security. Bluetooth is not an acceptable alternative to other wireless network connectivity; researchers have found security vulnerabilities that risk the spread of malware and allow unauthorized access to data being transmitted between Bluetooth-connected devices.[30]

When wired connectivity is not available, proper security protocols for network connectivity should be put in place.

Election officials using vote centers and multiple early-voting locations may require network connectivity to share voter check-in information across several locations. Additionally, some e-pollbooks may not fully function if their wireless connections are eliminated or disabled. For example, certain e-pollbooks use Apple iPads, which rely solely on wireless connectivity for communication. Regardless of whether wireless or wired networks are used, officials should implement security requirements, including a VPN, encrypted communication between e-pollbooks, and strong passwords that are changed after every election. Older and insecure Wi-Fi protocols, such as WEP and WPA, should not be used. Any mobile devices, such as tablet computers, that are used as e-pollbooks should be secured with a mobile device management system.[31]

Ensure that systems undergo reliability testing and are properly patched as part of Election Day preparations.

E-pollbook networks, particularly those that serve multiple locations, such as vote centers, should be subject to reliability testing to ensure that they can perform on Election Day and during in-person early voting. If these networks fail or connectivity is too slow, the check-in process for voters can be disrupted, leading to long lines or to heavy provisional voting in some jurisdictions, which is itself a time-consuming process. Network issues of this sort occurred in many counties in California during the March 2020 primary election, leading to long lines in some areas.[32]

- **Update e-pollbook software.** E-pollbooks should receive appropriate operating system updates and software patches in advance of every election to protect against known cyber vulnerabilities. To determine what patches are available or recommended, election officials should review any guidelines or requirements created by state or local government IT agencies. States and localities may develop their cybersecurity requirements on the basis of the National Institute of Standards and Technology's cybersecurity framework.[33] Adhering to these requirements will ensure that election officials are using best practices for securing election systems, protecting voters' PII, and ensuring the integrity of voter data used on Election Day. Alerts from the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) can also provide insights about recent vulnerabilities and emergency security patches.[34]

- **Where possible, ensure that each e-pollbook contains a backup of the full check-in roster.** By keeping a backup of the full roster on the individual e-pollbook, poll workers can check voters in even when connectivity is poor. Data can be synced once connectivity is reestablished.

Keep appropriate backup of e-pollbooks in polling places.

Having a backup in place allows poll workers to confirm voters' eligibility, diminishes the potential for long lines, and may minimize the need to issue provisional ballots.

- **Send paper backups of e-pollbooks to polling places with other printed materials.** Paper backups, when accompanied by easy-to-use transition procedures for poll workers, are the simplest resiliency measure in the event of an e-pollbook failure. While jurisdictions in 41 states and the District of Columbia use e-pollbooks, our research indicates that only 12 states and DC formally require paper backups of e-pollbooks on Election Day, although several other states recommend the practice or have counties that voluntarily keep paper backups.[35]

- **If backup paper pollbooks are not feasible, arrange for polling locations to have nonnetworked alternative devices containing the entire list of registered voters for the jurisdiction.** The use of vote centers and other centralized voting locations, already on the rise, may increase further as a result of the pandemic, as vote centers, including mobile ones, can serve voters across a county during poll worker shortages and last-minute polling place closures. For vote centers in large counties, printing paper pollbooks may create logistical and administrative challenges. These voting locations should employ other backup options, such as a nonnetworked device from a different vendor, containing the entire list of registered voters for the jurisdiction, along with the correct ballot style and current status for each voter (i.e., voted, mailed a ballot, or not voted).

- **Ensure that recovery procedures can be quickly and effectively implemented.** Jurisdictions should evaluate their e-pollbook recovery procedures to ensure that they will be easy for poll workers to follow and will not introduce new obstacles to voters casting ballots quickly. A clear protocol should outline when it is appropriate to switch over to the backup method and how to recover the record of who has already voted.

Provide Sufficient Paper Ballots and Provisional Envelopes

Many election officials using paper materials for in-person voting use formulas based on a certain fraction of registered voters or on prior election turnout when deciding how much to print. This approach can leave jurisdictions unprepared for unexpected surges in voter turnout and result in ballot shortages, as happened across the country during the 2018 midterm elections. Many experts are predicting more record-breaking turnout during the 2020 elections.[36]

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

Even though Covid-19 outbreaks or fears of such outbreaks have increased interest in the use of mail voting in some areas, officials cannot rely on voters being willing and able to use this option in the fall, particularly in jurisdictions where its use has historically been low. For instance, many voters requested a mail ballot in Wisconsin for the April 2020 primary, but not all received one in time to return it by Election Day.[37] These voters had to vote in person, and some stood in long lines to do so.

A cyberattack that results in mail ballots being sent to the wrong address, or to voters who did not request them, could also spur demand for in-person voting. These voters may need to vote in person, or they may choose to do so. Officials should work with ballot printers to ensure that, as the election approaches, a sufficient supply of in-person ballots can be produced, as waiting until absentee ballot request deadlines have passed may leave insufficient time to print ballots for in-person voting.

To prepare for high turnout, election officials should print more than enough in-person ballots for all registered voters who have not requested a mail ballot. Many voters will request a mail ballot for the first time this year, leading to increased uncertainty around levels of in-person voting. We therefore recommend printing ballots for 120 percent of registered voters who have not requested a mail ballot by the time printing must take place.[38] For instance, if 200 registered voters have not requested a mail ballot by that time, then officials should make sure they have enough in-person ballots on hand to cover 120 percent of that number, or 240 ballots. The extra ballots should cover those who may not have returned their mail ballots or made errors in the polling place. Jurisdictions with Election Day registration may require a larger ballot supply, while those with an established history of early voting using ballots printed on demand may require slightly less. However, voters' choice between these methods — mail, early, or Election Day — varies significantly across precincts and across elections, so in general, officials must err on the side of caution to avoid ballot shortages.[39] In some jurisdictions, "double printing" can be avoided, as preprinted ballots can be used for both in-person and mail voting. Any preprinted ballots that are not requested for voting at home should be made available to polling places for in-person voting, at least as an emergency backup ballot.

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

A key backup measure for both Election Day system failures and disruptions to mail ballot systems is a supply of sufficient provisional ballots and provisional balloting materials. These can serve as a fail-safe if, for instance, a cyberattack causes ballots to be mailed to voters who did not request them. It is preferable to issue regular ballots to eligible voters who never received or lost their mailed ballot. Some jurisdictions use securely networked e-pollbooks to facilitate this process; others may lack this capability. In all jurisdictions, it may not be possible to immediately determine voter eligibility in the event of e-pollbook failure, especially if backup paper pollbooks are unavailable or are found to contain errors.

Provisional ballots ensure that individuals can cast a ballot while giving election officials additional time to determine their eligibility. Having sufficient provisional materials, such as envelopes and affidavit forms, to account for more than three hours of peak voting activity, plus a small amount for baseline needs related to eligibility questions and other issues, will allow voting to continue in the event of system failures.[40] Using a comprehensive survey conducted by MIT, we estimate that in the November 2020 election, this will typically amount to 40 percent of the number of registered voters.[41] The expected increase in mail ballot usage may lead to higher-than-normal rates of provisional voting in person because many jurisdictions require voters who requested a mail ballot to vote provisionally if they appear at an in-person voting site. While a supply of 40 percent will not be enough to deal with an all-day problem, it will provide sufficient time for other measures to be implemented or additional ballots and materials to be delivered to polling places.

Election officials may be reluctant to take these steps for fear of unnecessary spending on an unlikely contingency. But we know from recent elections that the failure to have sufficient provisional materials can have profound consequences, causing long lines and, worse, preventing some voters from casting ballots at all. The good news is that in many jurisdictions, unused provisional envelopes and other materials can be used in future elections. Additionally, many jurisdictions do not require that provisional ballots be different from regular ballots or the emergency paper ballots that are used in case of voting machine malfunctions.

Train poll workers to implement contingencies.

Improper or insufficient training of poll workers can lead to voters being turned away, long lines forming, and ineligible individuals being allowed to cast a ballot. Poll worker instructions for managing provisional ballots must include how to handle e-pollbook failures appropriately and how to determine when to allow voters to cast a regular ballot and when to issue a provisional ballot. Whenever voter eligibility can be confirmed in a timely fashion through the use of appropriate backups, regular ballots should be issued. The Election Assistance Commission provides guidance for poll workers on issuing provisional ballots as well as some best practices for poll worker accountability.[42]

Provisional ballot forms must make the sections each person uses clear so that voters, poll workers, and all election staff know what they each need to do. It is also important to provide a clear list of when to use the provisional ballot envelopes, including on the envelope itself. Poll worker manuals and provisional envelopes both should make clear that if there is doubt about a voter's eligibility or whether the voter has already voted, the opportunity to vote provisionally must be offered as a fail-safe. This will ensure that if pollbook data is corrupted in any way, eligible voters are not denied an opportunity to vote. In 2018, Virginia adopted new provisional ballot materials created in coordination with the Center for Civic Design that illustrate these best practices.[43]

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

While it is best to stock enough of all supplies to avoid running out, election officials should ask poll workers to use indicators, such as Post-it notes or stickers, to alert them when paper ballots, provisional ballot materials, emergency backup ballots, or other supplies are running low. For instance, workers can place a “running low” sticky note on top of the hundredth ballot or hundredth envelope from the bottom of the supply. This way, busy poll workers will realize they must call election officials for backup supplies before they run out.

More Resources

Election Assistance Commission
Election Security Preparedness
https://www.eac.gov/election-officials/election-security-preparedness

Center for Internet Security
A Handbook for Elections Infrastructure Security
www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf

Belfer Center
The State and Local Election Cybersecurity Playbook
www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook#voterreg

Pew Charitable Trusts
A Look at How — and How Many — States Adopt Electronic Poll Books
www.pewtrusts.org/en/multimedia/data-visualizations/2017/a-look-at-how-and-how-many-states-adopt-electronic-poll-books

National Conference of State Legislatures
Electronic Pollbooks
www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx

Center for Internet Security
Securing Google Android
https://www.cisecurity.org/benchmark/google_android

Center for Internet Security
Securing Apple iOS
https://www.cisecurity.org/benchmark/apple_ios

Election Assistance Commission
Provisional Voting
www.eac.gov/research-and-data/provisional-voting

Center for Civic Design
You See a Provisional Ballot, Voters See Their Ballot
www.civicdesign.org/you-see-a-provisional-ballot-voters-see-their-ballot

Prevent and Recover from Voting Equipment Failures

Even under the best of circumstances, equipment failures occur. The impact of these failures can be even more difficult to manage during the pandemic or a resurgent outbreak, as they may occur alongside polling place closures, poll worker shortages, and social distancing guidelines. Following public health guidelines to keep one's distance from others can be difficult while standing in a long line, and some voters may understandably be concerned that the risk to their health or that of others is too high.[44]

For digital or optical-scan voting systems, recovery from an equipment failure can be relatively fast; as ballots are already printed, voting can continue while a tabulator issue is resolved. As a Brennan Center report notes, voting systems that rely on direct-recording electronic (DRE) machines can face more problems in the event of a failure, since "voters may have to wait in long lines while election workers scramble to repair them."[45] DRE voting systems electronically record voters' selections in each race or contest on the ballot. These problems can occur as well when jurisdictions use ballot-marking devices (BMDs) and ballot-on-demand (BOD) printers. In the event of a system failure, these machines will not function until repaired or replaced, and jurisdictions using them will need to print ballots in advance of the election to allow voting to continue. Regardless of the voting system used, election officials should conduct logic and accuracy testing on all voting equipment prior to every election in order to minimize the chance of unforeseen equipment failures on Election Day.

If using DRE machines, BMDs, or BOD printers, provide enough emergency paper ballots to cover two to three hours of peak voting activity.

Emergency ballots should be provided to voters who are identified as qualified and meeting all the requirements for voting pursuant to state law but who are unable to use machines due to a malfunction. When voters' eligibility to cast a ballot is clear, they should not be required to fill out an affidavit, and poll workers should not perform additional research.

Election jurisdictions using DREs, BMDs, or BOD-printed ballots as the primary voting option should print emergency paper ballots that can be counted with existing tabulators or stored securely for later counting. Yet, among the states that use DREs as the principal polling place equipment in at least some jurisdictions, at least five do not mandate that paper ballots be made available in the event of DRE failure.[46]

- **Make sure emergency ballots are in every polling place and poll workers have been trained to use them.** Printing enough ballots for two to three hours of peak voting activity allows voting to continue until equipment can be repaired or replaced, or until additional emergency paper ballots can be delivered to a polling place. In the November 2020 election, this will typically amount to 35 percent of registered voters, though this number can be reduced in jurisdictions with a strong history of voting by mail, in rough proportion to those historical levels.[47] Reductions of this sort should not be made in jurisdictions without that history, nor out of proportion to that history, as it is impossible to know well in advance of Election Day whether voting by mail and early voting will surge in popularity this fall. In fact, greater use of these methods can be indicators of increased, not decreased, Election Day turnout.[48] In many jurisdictions, mail ballots that were printed but never requested by voters can be repurposed as emergency ballots for in-person polling places. Appropriate procedures should be in place for chain of custody and accounting for preprinted paper ballots.

- **Count emergency ballots without any additional scrutiny of voter qualifications.** Emergency ballots should be counted as soon as functional voting equipment is available. Unlike some provisional ballots, they do not require research on voter eligibility.

- **If using BMDs or BOD printers, program tabulators to accept and read emergency paper ballots.** Where possible, tabulators should be programmed to accept and read both ballots produced by the BMDs or BOD printers and preprinted ballots used for emergency ballots. Preelection testing should include verification that the tabulators properly identify and record both types of ballot.

- **At vote centers, stock emergency ballots for the most heavily used precincts.** Vote centers that use a large number of ballot styles should stock preprinted emergency ballots for the precincts and languages most likely to be needed at that center. When vote centers have been in use in a jurisdiction for multiple elections, officials can look at usage data from prior elections to determine which ballot styles and languages voters tend to use. North Carolina's Board of Elections required this sort of emergency ballot preparation for early-voting sites operating during the March 2020 election.[49] Some vote centers tend to draw voters from the nearest few precincts, while others, such as those located at commuter college campuses, may draw voters from a wider area. If a vote center is replacing a few traditional polling places, emergency ballots in the styles that would have been needed at the closed polling places should be stocked. Vote centers can also be stocked with master copies of emergency paper ballots in all necessary ballot styles and languages, along with a photocopier to reproduce them in emergency situations. Having on hand a laptop containing all ballot styles and a laser printer is another option.

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.** Any reports of machine errors from voters should be tracked and reported to the central election office throughout the day. Minor problems, such as slow response or a flickering screen, can be an early warning sign of a unit that is going to malfunction more severely. Election offices should review and compare reports across voting locations to identify trends that could indicate widespread problems, including potential cyberattacks. Machines that have experienced problems in past elections can be deployed to polling sites that are well resourced with IT expertise, such as the county elections office, so that if problems arise they can be addressed promptly.

- **Establish a protocol for when in-precinct scanners are not working.** If scanners are not functioning, voting should proceed, and ballots should be stored securely until they can be counted.

- **Recalibrate touch screens and make any other necessary voting equipment repairs in full view of observers.** Making these repairs in front of observers will improve public confidence that any malfunctions have not affected the outcome.

- **Train poll workers on the process for counting paper ballots, including hand counting when necessary.** Providing this training in advance helps ensure consistent approaches to counting votes, boosting public confidence in the outcome.

Communicate with voters to build trust in the election process.

- **Preprint signage that informs voters of equipment failures.** Use information and instructions approved by the election office and consistent across all polling locations. Ensure that voters are not directed to use machines that are suspected of producing erroneous records.

- **Remind voters to check their ballots or paper printouts for any errors.** Take steps to make sure that voters' selections are accurately recorded on their ballots. When using hand-marked paper ballots that are counted without the help of an optical scanner, poll workers should remind voters to check their ballots to prevent overvotes, which occur when voters make more selections than the number allowed. When using DREs with a voter-verifiable paper audit trail (VVPAT) or BMDs, poll workers should clearly explain to voters how their ballots will be cast and remind them to verify that the printout matches the selections they made on the machine. For example, when using BMDs that print a paper ballot that must then be scanned by a separate machine, poll workers should tell voters: "After you make all your choices, your ballot will print out, and you'll go [over there] to cast it." After voters print their ballot but before scanning it, poll workers should remind voters: "Don't forget to check the printed ballot carefully. If you see something wrong, you can get a replacement."

Take steps to prevent delayed polling place openings due to equipment failures.

Inoperable voting equipment should not prevent the timely opening of a polling place. Late polling place openings can lead to long lines and voters leaving without casting a ballot.[50]

Poll workers should be trained to deal with equipment failures occurring on Election Day morning, especially as staffing shortages resulting from the pandemic or other emergencies can delay troubleshooting of equipment problems. Voters should be allowed to vote using emergency paper ballots if operable voting equipment is not available when the polls open. Poll workers should explain to voters how ballots will be counted once working voting equipment is available.

Plan to assist voters with disabilities if voting machines fail.

If accessible voting machines fail, voters with disabilities may not be able to vote privately and independently on paper ballots. Jurisdictions with sufficient resources should have backup accessible voting equipment, with all ballot styles available (similar to what would be used at a central voting site for early voting), geographically dispersed so that it can be rapidly delivered to any polling place where accessible equipment has failed. In the longer term, jurisdictions might consider providing each polling place with accessible tablets and printers to be used by voters with disabilities in the event of voting-equipment failure.[51] Poll workers should be appropriately trained on any backup systems used to provide accessibility.

More Resources

Brennan Center for Justice
America's Voting Machines at Risk: An Update
www.brennancenter.org/analysis/americas-voting- machines-risk-an-update

Brennan Center for Justice
Overview of Voting Equipment
https://www.brennancenter.org/our-work/research-reports/brennan-center-overview-voting-equipment

Verified Voting
The Verifier (Polling Place Equipment)
www.verifiedvoting.org/verifier

Election Assistance Commission
Election Security Preparedness
https://www.eac.gov/election-officials/election-security-preparedness

Election Assistance Commission
Election Management Guidelines
https://www.eac.gov/election_management_resources/election_management_guidelines.aspx

Election Assistance Commission
Contingency Planning
https://www.eac.gov/election-officials/contingency-planning

Center for Internet Security
A Handbook for Elections Infrastructure Security
https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf

Results Reporting, Certification, and Public Communications

All good contingency plans include a communications strategy. As the pandemic has spurred public confusion and worry, election officials are under increased pressure to communicate changes to elections, as well as results, as clearly as possible.[52]

Against this backdrop, a rise in the use of mail voting may increase perceptions of delay due to processing times for large numbers of mail ballots, as well as potential mail disruptions or election staff and equipment shortages related to the pandemic. If canvassing staff must operate under conditions of social distancing, processes such as signature checking may take extra time, and mechanisms for public observation of the process may need adjustment.

Moreover, voters are relying heavily on remote options for communicating with election offices. They are looking up information on official election websites, using online registration and mail ballot request tools, and making inquiries and requests over the telephone and by email. They are also mailing in registration forms rather than registering in person at the Department of Motor Vehicles, and they are requesting mail ballots via mail. This can place stress on elections staff, who must process more remote inquiries and requests than usual.

Prevent and Recover from Election Night Reporting System Failures and Outages

Local and state officials usually post unofficial results on election night. This information does not reflect the certified results, and large differences between unofficial election night results and the final outcome can cause voters to question the accuracy of the process. Perceived delays in reporting can also raise concerns.

Election night reporting sites are prime targets for DDoS attacks because the sites' high-use period is known ahead of time, and preventing access to unofficial results can generate negative media attention about the electoral process. A hotly contested race can increase interest in election results, and a large increase in visitors to the reporting website over a short period can likewise bring down the site.

Establish redundancies.

Several states, including Arizona and Virginia, experienced election night reporting failures in the 2014 midterm elections.[53] Addressing the system failures after the election, some of these states, such as Pennsylvania, established redundant systems that can be made available if the main system fails.[54] Unofficial results can be made public through backup websites, social media posts, uploads of simple PDFs, or announcements to the media.

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

ENRs are attractive targets for cybercriminals and adversarial states. Bad actors have successfully attacked ENRs around the world, including in Ukraine, Bulgaria, and more recently the United States. By publishing unofficial results through an unconnected system, election officials can minimize the potential that a targeted attack on the reporting system will have any lasting impact. Knox County, Tennessee, experienced a website failure linked to foreign IP addresses during the May 1, 2018, primary elections. Although the failure was accompanied by an attack on the county's servers, the reporting website itself did not provide an avenue for future disruption. The deputy director of IT for the county noted that its reporting system is "not connected to any live databases. . . . It's a repository for being able to report to the public, and we have intentionally kept any primary data extremely isolated."[55]

Conduct robust precertification audits that the public can observe.

A robust audit compares the unofficial result of tabulating votes with the paper record that voters can verify before casting their votes. Performing an audit prior to certification ensures that if tabulators were improperly programmed or maliciously attacked, leading to inaccurate declared outcomes, the errors can be fixed before results are certified.

- **Set up live video streams or take other measures to permit public observation of an audit during social distancing.** If video observation is the only means for the public to observe an audit, make sure cameras are placed in locations that permit viewers to check that officials are complying with the rules governing the audit and that interpretations of voter intent match the paper records.

- **Ensure that facilities used for the audit can accommodate social distancing.** Audits typically require multiple officials to agree that the ballots or batches chosen for inspection are correctly being retrieved and that the voter's intent on the ballots being inspected is accurately interpreted. Teams must ensure that mistakes are not made during counting or the entry of counts. Complying with these rules and best practices under conditions of social distancing may require larger facilities for the spacing of seating as well as the provision of personal protective equipment.

More Resources

Election Assistance Commission
Checklist for Securing Election Night Reporting Systems
www.eac.gov/documents/2017/10/23/checklist-for- securing-election-night-reporting-systems-data- election-administration-security

Election Assistance Commission
Post Election: Audits & Recounts
https://www.eac.gov/election-officials/post-election-audits-recounts

Make Needed Public Information Easily Accessible

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

- **Prepare for increased use of county and state election websites, and provide backups.** Officials should ensure that state and county election websites undergo periodic independent load and vulnerability testing, as these websites will get heavier usage while the public practices social distancing. They may see sudden increases in usage in the event of a resurgence or localized outbreak of Covid-19 in the fall. It is crucial that voters be able to obtain services and information through these websites during periods of social distancing.

- **Direct voters to alternative web pages, such as those offered by the Voting Information Project, in case of voter lookup failure.** Make sure that these sites have accurate polling place data in advance of the election and confirm that they are working correctly.

Prepare to hire backup phone attendants.

Emergencies can lead to unexpected staffing needs for telephone lines. For instance, during the Iowa caucuses in 2020, a backup phone system for reporting results was overwhelmed with calls due to widespread problems with the primary reporting system.[56] During the pandemic, voters may have numerous questions about such things as changed polling locations, when their requested mail-in ballot would arrive, and changing election rules.[57] Ahead of the March 2016 election, Virginia, faced with numerous phone calls from voters, automatically redirected calls to a temporary staffing center where basic inquiries, such as requests to look up polling places, could be answered.[58] A contract to provide this kind of supplemental service will ensure that officials can continue to communicate with and serve voters effectively, even if an office experiences a staffing shortage or unexpectedly high demand due to Covid-19 or another emergency.

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

Before Election Day, build trust with voters and the media around election results reporting. Describe the procedures for processing and canvassing mail and provisional ballots and why these procedures may take more time than the public is used to, particularly if there are mail disruptions or an unexpected influx of mail ballots. Explain how the public can observe this process, and have a plan for that observation, such as by video, if social distancing measures are still in place or must be followed once again in November. The Orange County, California, registrar's website provides a documentary video about the vote-by-mail process, called "What It Takes to Count," including interviews with elections staff and a demonstration of how the processing equipment works.[59]

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.

In many jurisdictions, precincts report unofficial results that do not include mail and provisional ballots. In others, all mail ballots are described as belonging to a single precinct. These practices can lead the public to believe that virtually all ballots have been counted well before that is the case. To avoid these misunderstandings, reporting websites can explain that mail and provisional ballots have not yet been counted. For instance, on every contest results page found on the California secretary of state's website, a link is provided to an "Unprocessed Ballots Status" page that explains how long it takes counties to process all ballots, and why.[60] Where feasible, websites can display not only the percentage of precincts providing unofficial results but also the percentage or number of ballots still to be counted. California's secretary of state provides an estimated "unprocessed ballots" report from individual counties on its website. On April 3, 2020, for example, this report let the public know that more than 67,000 ballots remained to be processed from the March 2020 election.[61]

Provide emergency communications on public websites.

Officials should post emergency information to their regular public website as well as to other websites, such as official social media accounts used by state and local election personnel. This will provide an official source for voters, candidates, media, and advocacy organizations to find information regarding extended polling place hours, emergency polling place relocations, and other emergency information. Using a website or social media to provide information to voters in advance of the election will make emergency communications on Election Day easier for election administrators.

Develop a Communications Strategy

At its core, a communications plan should assist election officials in distributing essential information in a timely manner and maintaining public confidence in the election administration system. Communications plans are important in all unexpected situations, from equipment failures to potential cyberattacks to unintentional errors. As the Belfer Center suggests, a good approach to emergency communications is to be transparent but careful: "Transparent communication builds trust, but in a cyber incident you will have few facts at hand, especially at the outset."[62]

Draft, review, and approve a communications plan prior to negative developments.

Keeping voters, poll workers, and others informed minimizes the negative impact of issues that arise on or before Election Day. The most basic communications plan identifies key staff and other contacts. A more detailed communications strategy may include various options to respond to potential problems and longer-term considerations, such as notification requirements in the event personal voter information is leaked.

More Resources

Belfer Center
The State and Local Election Cybersecurity Playbook
www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook#voterreg

Belfer Center
The Elections Battle Staff Playbook
https://www.belfercenter.org/sites/default/files/2019-12/Battle%20Staff.pdf

Endnotes

1 Glen Howatt, "COVID-19 Cases Could Surge in Fall, Last 2 Years, University of Minnesota Report Says," *Minnesota Star-Tribune*, May 3, 2020, https://www.startribune.com/covid-19-cases-could-surge-in-fall-last-2-years-u-report-predicts/570130602.

2 See, e.g., Keith Ingram, *Election Advisory No. 2020-14*, Texas Secretary of State, Elections Division, April 2, 2020, https://www.documentcloud.org/documents/6824368-ADV2020-14-COVID-19-Coronavirus-Voting-and.html.

3 Hon. Bennie Thompson, Hon. Cedric Richmond, Hon. Derek Kilmer, and Hon. C.A. Dutch Ruppersberger, letter to Hon. Nancy Pelosi, speaker, and Hon. Kevin McCarthy, minority leader, April 13, 2020, https://homeland.house.gov/imo/media/doc/2020-04-13%20T%20Pelosi%20McCarthy%20-%20COVID%20SLTT%20Cyber.pdf (noting that "State and local government employees . . . may be less accustomed to teleworking and less prepared to do it securely, making State and local networks more vulnerable to ransomware and other cyber attacks").

4 Global Cyberalliance, "Practical Steps to Help You Work from Home Securely," accessed April 2020, https://workfromhome.globalcyberalliance.org.

5 Karen Scarfone, Jeffrey Greene, and Murugiah Souppaya, *ITL Bulletin March 2020: Security for Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Solutions*, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce, March 2020, https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2020-03.pdf; and Murugiah Souppaya and Karen Scarfone, *Guidance on Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*, National Institute of Standards and Technology, U.S. Department of Commerce, July 2016, https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final.

6 Cybersecurity and Infrastructure Security Agency, "Enterprise VPN Security" (Alert AA20-073A), last revised April 15, 2020, https://www.us-cert.gov/ncas/alerts/aa20-073a.

7 Center for Internet Security, "CIS Controls Telework and Small Office Network Security Guide," accessed April 9, 2020, https://www.cisecurity.org/white-papers/cis-controls-telework-and-small-office-network-security-guide.

8 National Cybersecurity Center of Excellence, "Data Security," accessed April 9, 2020, https://www.nccoe.nist.gov/projects/building-blocks/data-security.

9 Cybersecurity and Infrastructure Security Agency, "Top 10 Routinely Exploited Vulnerabilities" (Alert Number AA20-133A), May 12, 2020, https://www.us-cert.gov/sites/default/files/publications/AA20-133A_Top_10_Routinely_Exploited_Vulnerabilities_S508C.pdf.

10 Pingdom is a service that monitors websites for whether they are functioning or "down": https://www.pingdom.com/website-monitoring. Albert is a service that detects potentially malicious intrusions and attempted intrusions: https://www.cisecurity.org/services/albert-network-monitoring.

11 Matt Davis (former chief information officer, Virginia Department of Elections), interview by Brennan Center for Justice, April 29, 2020.

12 Third-party organizations encourage voters to use these tools via a #checkyourreg campaign. See Twitter, "#CheckYourReg," https://twitter.com/hashtag/checkyourreg.

13 Thirty-four states and Washington, DC, offer "no-excuse" absentee/mailed ballot voting. See National Conference of State Legislatures, "Voting Outside the Polling Place: Absentee, All-Mail and Other Voting at Home Options," last updated April 24, 2020, https://www.ncsl.org/research/elections-and-campaigns/absentee-and-early-voting.aspx#do%20not.

14 See, e.g., Kevin Wilson and Randall Dullum, "Absentee Ballots on a Roll as Election Nears," *Daily Jefferson County Union*, April 1, 2020, https://www.dailyunion.com/news/covid-19/absentee-ballots-on-a-roll-as-election-nears/article_a48d2c89-aa77-53e4-8a53-f6ae-87b24aea.html; and Megan Alley, "Ohio's Primary Election Moves to April 28 All-Mail Vote amid COVID-19 Pandemic," *Clermont Sun*, April 4, 2020, https://www.clermontsun.com/2020/04/04/ohios-primary-election-moves-to-april-28-all-mail-vote-amid-covid-19-pandemic.

15 See, e.g., Emily Allen, "Facing Coronavirus, W.Va. Secretary of State Expands Access to Absentee Ballots for May 12 Primary," West Virginia Public Broadcasting, March 18, 2020, https://www.wvpublic.org/post/facing-coronavirus-wva-secretary-state-expands-access-absentee-ballots-may-12-primary#stream/0.

16 See, e.g., Tessa Weinberg, "Gov. Greg Abbott Allows Local Officials to Postpone May 2 Elections Due to COVID-19," *Fort Worth Star-Telegram*, March 18, 2020, https://www.star-telegram.com/news/politics-government/article241246056.html. As of April 2019, 35 states explicitly permitted governors to suspend or amend both statutes and regulations, 7 states permit governors to amend regulations during a declared emergency, and 8 states and the District of Columbia provide no explicit authority to governors to change statutes or regulations during a declared emergency. See Gregory Sunshine et al., "An Assessment of State Laws Providing Gubernatorial Authority to Remove Legal Barriers to Emergency Response," *Health Security* 17, no. 2 (2019), https://www.nga.org/wp-content/uploads/2019/06/An-Assessment-of-State-Laws-Providing-Gubernatorial-Authority-to-Remove-Legal-Barriers-to-Emergency-Response.pdf.

17 See, e.g., Susan Milligan, "Preparing for a Voter Surge: Experts Predict Record Voter Turnout in 2020, but Will It Materialize?" *U.S. News & World Report*, September 20, 2019, https://www.usnews.com/news/elections/articles/2019-09-20/experts-predict-huge-turnout-in-2020; William A. Galston, "What Does High Voter Turnout Tell Us About the 2020 Elections?" Brookings, November 20, 2019, https://www.brookings.edu/blog/fixgov/2019/11/20/what-does-high-voter-turnout-tell-us-about-the-2020-elections ("While the 2020 outcome may be unclear, what is clear is that turnout in 2020 could break all records and test our election machinery as it has never been tested before."); and Richard H. Pildes and Charles Stewart III, "The Wisconsin Primary Had Extraordinarily High Voter Turnout," *Washington Post*, April 15, 2020, https://www.washingtonpost.com/politics/2020/04/15/wisconsin-primary-had-extraordinarily-high-voter-turnout.

18 See, e.g., Wisconsin Elections Commission, "Absentee Envelope Issues and Options," March 18, 2020, https://elections.wi.gov/sites/elections.wi.gov/files/2020-03/Absentee%20Envelope%20Issues%20and%20Options%20FAQ%203.18.2020_0.pdf ("The Wisconsin Elections Commission (WEC) has received numerous questions regarding absentee ballot envelopes, potential shortages and what procedures can be used if clerks are running low on envelopes. We also understand that printing vendors around the state have exhausted their stock of envelopes and have cited delays in the paper supply chain.").

19 The baseline number of registered voters used for these calculations should include inactive voters, as these voters may typically request and be provided with a mail ballot. We recommend 120 percent of this base amount for three primary reasons. First, there is typically a surge in the number of registered voters as registration deadlines approach. For instance, in the 2016 presidential election, California saw registrations increase from 73 percent to 78 percent of eligible voters, an increase of 1.2 million voters, between 60 and 15 days prior to the election. See California Secretary of State, Elections Division, "Voter Registration Statistics," accessed April 2020, https://www.sos.ca.gov/elections/voter-registration/voter-registration-statistics. Printing orders may need to be placed much earlier than registration deadlines, however. Edgardo Cortés et al., *Preparing for*

Election Day: Deadlines for Running a Safe Election, Brennan Center for Justice, May 11, 2020, https://www.brennancenter.org/our-work/research-reports/preparing-election-day-deadlines-running-safe-election (recommending that orders for November 2020 be placed by mid-June). Second, a sizable increase in the level of mail voting is quite likely this year, as are high levels of overall turnout. Jonathan Lai, "Philly Voters Have Requested More Mail Ballots than All of Pennsylvania Did in 2016," *Philadelphia Inquirer*, May 20, 2020, https://www.inquirer.com/politics/election/coronavirus-philadelphia-mail-ballot-requests-20200520.html. Third, since many mail ballot voters will be using this method for the first time, the rate at which voters ask for a replacement mail ballot may be higher than normal. Supplies must be ready for those who do not receive their ballot, lose it, or spoil it or the return envelope. Enrijeto Shino et al., "Here's the Problem with Mail-In Ballots: They Might Not Be Counted," *Washington Post*, May 21, 2020, https://www.washingtonpost.com/politics/2020/05/21/heres-problem-with-mail-in-ballots-they-might-not-be-counted.

[20] Center for Civic Design, "Vol. 104 Designing Vote at Home Envelopes and Materials," accessed April 2020, https://civicdesign.org/fieldguides/104-designing-vote-at-home-envelopes.

[21] United States Postal Service, *Your 2020 Official Election Mail Kit*, https://about.usps.com/kits/kit600.pdf.

[22] reCAPTCHA is a newer iteration of CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart).

[23] National Institute of Standards and Technology, "Cybersecurity Framework," accessed April 2020, https://www.nist.gov/cyberframework; National Cybersecurity Center of Excellence, "Data Security"; and Erika McCallister, Tim Grance, and Karen Scarfone, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, National Institute of Standards and Technology, April 2010, https://csrc.nist.gov/publications/detail/sp/800-122/final.

[24] These systems are Democracy Live Secure Select 1.2.2., Five Cedars Group Alternate Format Ballot (AFB) v 5.2.1, and Dominion ImageCast Remote 5.2. See California Secretary of State, "Two New Remote Accessible Vote by Mail Systems Approved by California Secretary of State," October 13, 2017, https://www.sos.ca.gov/administration/news-releases-and-advisories/2017-news-releases-and-advisories/two-new-remote-access-vote-mail-systems-approved-california-secretary-state.

[25] "Dr. Fauci Says 'Rolling Reentry' of U.S. Economy Possible in May," *Boston Herald*, April 12, 2020, https://www.bostonherald.com/2020/04/12/fauci-says-rolling-re-entry-of-u-s-economy-possible-in-may.

[26] Janie Har and Stefanie Dazio, "Voting Problems, Long Lines Mar California Primary Voting," *U.S. News & World Report*, March 4, 2020, https://www.usnews.com/news/politics/articles/2020-03-04/voting-problems-long-lines-mar-california-primary-voting; and John Myers, Dakota Smith, and James Rainey, "California Officials Demand Changes to L.A. Voting After Election Day Chaos," *Los Angeles Times*, March 5, 2020, https://www.latimes.com/california/story/2020-03-05/california-officials-demand-changes-los-angeles-voting-election-day-chaos.

[27] Tim Reid and Sharon Bernstein, "Sanders Asks Court to Keep Los Angeles County Polls Open After Voting Delays," Reuters, March 3, 2020, https://www.reuters.com/article/us-usa-election-delays/sanders-campaign-requests-emergency-injunction-to-keep-los-angeles-county-polls-open-idUSKBN20R0GP.

[28] This percentage was calculated using data made available by the Wisconsin Election Commission. See Wisconsin Election Commission, "Absentee Voting Statistics," https://elections.wi.gov/publications/statistics/absentee.

[29] Devices described as "Wi-Fi devices" use IEEE 802.11 network protocols.

[30] See, e.g., Armis, *Protecting the Enterprise from BlueBorne*, 2019, https://info.armis.com/rs/645-PDC-047/images/Armis-Protecting-the-Enterprise-from-BlueBorne-WP.pdf; and Daniele Antonioli, Nils Ole Tippenhauer, and Kasper B. Rasmussen, "The KNOB Is Broken: Exploiting Low Entropy in the Encryption Key Negotiation of Bluetooth BR/EDR, paper presented at the 28th Usenix Security Symposium, Santa Clara, California, August 2019, https://www.usenix.org/conference/usenixsecurity19/presentation/antonioli.

[31] National Institute of Standards and Technology, "Guidelines for Managing the Security of Mobile Devices in the Enterprise," https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r2-draft.pdf; and Center for Internet Security, "Benchmarks: Securing Google Android" and "Benchmarks: Securing Apple iOS," https://www.cisecurity.org/benchmark/google_android and https://www.cisecurity.org/benchmark/apple_ios.

[32] Michael McGough, "Data Issue Causes Voting Delays in These 15 California Counties. State Says Problem Fixed," *Sacramento Bee*, March 3, 2020, https://www.sacbee.com/news/politics-government/election/article240843751.html; and Stefanie Dazio and Janie Har, "Long Lines in Los Angeles Prompt Sanders Complaint," Associated Press, March 4, 2020, https://apnews.com/cb2ce758796eb6d714c2596a8d369b4c.

[33] National Institute of Standards and Technology, "Cybersecurity Framework."

[34] Cybersecurity and Infrastructure Security Agency, "Top 10 Routinely Exploited Vulnerabilities."

[35] In our research, we found written paper backup requirements for e-pollbooks in 12 states and DC. These 12 states are Connecticut, Georgia, Michigan, Minnesota, New Jersey, North Carolina, Ohio, Pennsylvania, Rhode Island, South Carolina, South Dakota, and Wisconsin. Mississippi and West Virginia have laws recommending paper backups. In Nevada and Wyoming, backup paper pollbooks are available in practice everywhere that e-pollbooks are used, while in other states, such as Colorado, Kansas, and Texas, paper backups are available in many jurisdictions. Arizona and Maryland formally require that either paper or electronic backups be available, while Idaho has indicated that it makes this recommendation. A few other states require or recommend that electronic backups be available. New Hampshire mandates that a sufficient number of high-speed printers be available to produce a backup paper checklist in the event of a system failure but has not yet deployed its electronic pollbook solution.

[36] See, e.g., Milligan, "Preparing for a Voter Surge"; Galston, "What Does High Voter Turnout Tell Us?" ("While the 2020 outcome may be unclear, what is clear is that turnout in 2020 could break all records and test our election machinery as it has never been tested before."); and Pildes and Stewart, "The Wisconsin Primary Had Extraordinarily High Voter Turnout."

[37] Nick Corasaniti and Stephanie Saul, "Inside Wisconsin's Election Mess: Thousands of Missing or Nullified Ballots," *New York Times*, April 9, 2020, https://www.nytimes.com/2020/04/09/us/politics/wisconsin-election-absentee-coronavirus.html; and Daphne Chen et al., "'Voter Suppression at Its Finest': Wisconsin Citizens Say Missing Ballots, Lines and Coronavirus Kept Them from Being Counted in Election," PBS, April 13, 2020, https://www.pbs.org/wgbh/frontline/article/voter-suppression-wisconsin-election-missing-ballots-lines-coronavirus-covid-19.

[38] We recommend multiplying those voters who have not requested a mail ballot by 120 percent for three primary reasons. First, some voters who were sent a mail ballot will nevertheless vote in person. Some may have moved after making the request, some may prefer to vote in person, and some may lose or spoil a ballot or envelope. See Mark Niesse et al., "Social Distancing Leads to Some Lines as Georgia Early Voting Begins," *Atlanta Journal-Constitution*, May 18, 2020, https://www.ajc.com/news/state--regional-govt--politics/social-distancing-leads-some-lines-georgia-early-voting-begins/LsXxsSUxD8XTMfMAnNKVZN ("Lines were also slowed by voters who requested absentee ballots but then had to cancel them when they showed up at early voting locations."). Second, overall turnout is expected to be extremely high in November 2020. See Galston, "What

Does High Voter Turnout Tell Us?" ("While the 2020 outcome may be unclear, what is clear is that turnout in 2020 could break all records and test our election machinery as it has never been tested before."). Third, high turnout in mail and early voting methods is not a predictor of lower Election Day in-person turnout. In fact, the reverse can be true, as high mail and early turnout can indicate overall high voter enthusiasm for that election. See Brennan Center for Justice, "Comment on Proposed Amendments to Georgia SEB Rules 183-1-12 and 183-1-13," February 17, 2020, 5 and n. 7, https://www.brennancenter.org/our-work/research-reports/brennan-center-submits-follow-comment-georgia-state-board-elections; and Lawrence Norden and Gowri Ramachandran, "How to Shorten Voting Lines for the November Election," *Los Angeles Times*, March 5, 2020 (describing increased vote-by-mail and in-person turnout in Orange County, California).

39 Jurisdictions should use historical data on mail, early, and Election Day turnout to determine what supply is needed for in-person voting. For instance, a jurisdiction that typically sees 60 percent mail turnout should prepare for at least 40 percent of registered voters to vote in person, even if a mail ballot is sent to 100 percent of registered voters. Likewise, a jurisdiction that typically sees only 10 percent mail turnout should prepare for much higher in-person voting turnout.

40 Nicholas Weaver, "Election Vulnerability: Voter Registration Systems," *Lawfare*, February 23, 2018, https://www.lawfareblog.com/2018-election-vulnerability-voter-registration-systems.

41 In the typical state, 35 to 45 percent of voters surveyed arrived at their polling place during the peak three hours of voting. Because historically high turnout is expected in the 2020 elections, we multiplied this range by 90 percent, to estimate that emergency supplies to serve 30 to 40 percent of voters would be prudent, or 35 percent in the typical case. We then supplemented the number slightly to account for an expected increase in the baseline need for provisional ballots stemming from increased requests for a vote-by-mail ballot: in many jurisdictions a voter who requested such a ballot but then appears at the polling place may vote only provisionally. See Charles Stewart III, *2016 Survey of the Performance of American Elections: Final Report*, Massachusetts Institute of Technology, 2017, 343, http://www.legendsvote.org/wp-content/uploads/MITCharles-Stewart-Voter-Turnout-Study-2016.pdf. This number can be reduced in jurisdictions with a strong history of voting by mail, in rough proportion to those historical levels, but officials should note that high vote-by-mail turnout can be an indicator of overall interest and high Election Day turnout, rather than the reverse.

42 Election Assistance Commission, "Provisional Voting," 2019, https://www.eac.gov/research-and-data/provisional-voting.

43 Center for Civic Design, "Making Provisional Voting Easier in Virginia," accessed April 9, 2020, https://civicdesign.org/showcase/making-provisional-voting-easier-in-virginia.

44 Astead Herndon, "They Turned Out to Vote in Wisconsin During a Health Crisis. Here's Why," *New York Times*, April 7, 2020, https://www.nytimes.com/2020/04/07/us/politics/wisconsin-democratic-voters.html (quoting a 70-year-old voter who did not vote in the Wisconsin April 2020 election: "I was told by my doctor to stay in and stay away from crowds. . . . That's why I didn't go.").

45 Lawrence Norden and Christopher Famighetti, *America's Voting Machines at Risk*, Brennan Center for Justice, 2015, 30, https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf.

46 We have identified five states with no provisions mandating that paper ballots be made available in the event of DRE failure: Kansas, Nevada, Texas, Utah, and West Virginia. While not required by statute, polling places in these states should provide emergency paper ballots when systems fail. For instance, Kansas requires counties to keep an additional supply of ballots to meet any emergency need for such ballots, although machine failure is not specifically listed; Nevada requires each local election official to submit a plan for the disposition of absentee ballots in case of an emergency; Texas advises its counties to adopt procedures to provide emergency paper ballots in the event of DRE machine failure; Utah allows for the provision of emergency paper ballots; and West Virginia counties have contingency plans in the event of machine failure.

47 In the typical state, 35 to 45 percent of voters surveyed arrived at their polling place during the peak three hours of voting. Because historically high turnout is expected in the 2020 elections, we multiplied this range by 90 percent, to estimate that emergency supplies to serve 30 to 40 percent of voters would be prudent, or 35 percent in the typical case. See Stewart, *2016 Survey of the Performance of American Elections*.

48 Brennan Center for Justice, "Comment on Proposed Amendments to Georgia SEB Rules"; and Norden and Ramachandran, "How to Shorten Voting Lines for the November Election" (describing increased vote-by-mail and in-person turnout in Orange County, California).

49 Karen Brinson Bell, "Ballot Preparation Instructions," memorandum, North Carolina State Board of Elections, January 9, 2020, https://s3.amazonaws.com/dl.ncsbe.gov/sboe/numbermemo/2020/Numbered%20Memo%202020-02_Ballot%20Preparation%20Instructions.pdf ("Distribution of ballots to one-stop sites should be based on the percentage of votes cast during the one-stop period in the 2016 presidential primary election.").

50 For example, during New York's June 2018 federal primary election, a voter was reportedly unable to vote because an election worker had not yet activated voting equipment. The voter was not offered an emergency ballot before having to leave the polling place. See Jake Offenhartz, "Voters Reporting Closed Poll Sites and Other Primary Day Confusion," *Gothamist*, June 26, 2018, http://gothamist.com/2018/06/26/voters_primary_confusion_nyc.php.

51 States like Oregon have adopted remote accessible voting by mail without requiring access to the internet to mark the ballot. Jurisdictions may want to consider having such systems available in the polling place in the event of machine failures. See Oregon Secretary of State, Voting & Elections, "Voting Instructions for Voters with a Disability," accessed April 9, 2020, https://sos.oregon.gov/voting/Pages/instructions-disabilities.aspx.

52 Joanne Kenen and Rachel Roubein, "Why America Is Scared and Confused: Even the Experts Are Getting It Wrong," *Politico*, March 31, 2020, https://www.politico.com/news/2020/03/31/experts-coronavirus-cdc-158313.

53 Eyragon Eidam, "Is Your Election Night Reporting System Ready for 2016?" *Government Technology*, December 21, 2015, https://www.govtech.com/state/Is-Your-Election-Night-Reporting-System-Ready-for-2016.html.

54 Marian Schneider (former deputy secretary for elections and administration, Pennsylvania Department of State), interview by Brennan Center for Justice, May 8, 2020; and Eidam, "Is Your Election Night Reporting System Ready?"

55 Sam Levine, "Hackers Tried to Breach a Tennessee County Server on Election Night: Report," *Huffington Post*, May 11, 2018, https://www.huffpost.com/entry/knox-county-election-cyberattack_n_5af5ca21e4b032b10bfa56ee; and Tyler Whetstone, "Knox County Election Night Cyberattack Was Smokescreen for Another Attack," *Knox News*, May 17, 2018, https://www.knoxnews.com/story/news/local/2018/05/17/knox-county-election-cyberattack-smokescreen-another-attack/620921002.

56 Trip Gabriel and Reid J. Epstein, "Snail Mail and Nuisance Calls: New Details on the Iowa Caucus Problems," *New York Times*, February 5, 2020, https://www.nytimes.com/2020/02/05/us/politics/iowa-caucus-problems.html.

57 The Madison, Wisconsin, clerk's official Twitter feed reported a backlog of 1,493 emails on April 2, 2020, five days before an election was held after numerous court rulings altered, in rapid succession, various deadlines and requirements for voters seeking to vote by mail, as well as widespread polling place closures. See Madison WI Clerk (@MadisonWIClerk), "The @CityofMadison has issued 82,938 absentees, but only 34,448 (41.5%) are returned to be counted. That includes 4,344 cast in-person/curbside (351 today). Our e-mail backlog is 1,493. We have 1,426 requests we can't process until the voter sends us voter ID, per state law," Twitter, April 2, 2020, 7:12 p.m., https://twitter.com/MadisonWIClerk/status/1245851531431366656; and Wisconsin Elections Commission, "Election Day Update Blog," https://elections.wi.gov/blog.

[58] Edgardo Cortés (former commissioner of elections, Virginia), interview with Brennan Center for Justice, April 1, 2020.

[59] Orange County Registrar of Voters, "About," accessed April 8, 2020, https://www.ocvote.com/vc/web/about.

[60] California Secretary of State, "Election Results: Unprocessed Ballots Status," accessed April 9, 2020, https://electionresults.sos.ca.gov/unprocessed-ballots-status.

[61] California Secretary of State, "Estimated Unprocessed Ballots for the March 3, 2020, Presidential Primary Election," April 3, 2020, https://web.archive.org/web/20200404171017/https://elections.cdn.sos.ca.gov/statewide-elections/2020-primary/unprocessed-ballots-report.pdf.

[62] Siobhan Gorman et al., *Election Cyber Incident Communications Coordination Guide*, Belfer Center for Science and International Affairs, 2018, 12, https://www.belfercenter.org/sites/default/files/files/publication/CommunicationsGuide.pdf.

ABOUT THE AUTHORS

▶ **Edgardo Cortés** is the election security adviser for the Brennan Center's Democracy Program. An expert on election administration and policy, Cortés served as Virginia's first commissioner of elections. During his tenure, he served as chairman of the board for the Election Registration Information Center and chairman of the U.S. Election Assistance Commission Standards Board. He previously served as the general registrar in Fairfax County, Virginia, and deputy director for policy and grants director at the U.S. Election Assistance Commission. Cortés received his undergraduate degree from Cornell University and his master's degree in political management from the George Washington University.

▶ **Gowri Ramachandran** serves as counsel for the Brennan Center's Democracy Program. She came to the Brennan Center from Southwestern Law School in Los Angeles, where she is on leave from her position as professor of law. At Southwestern, she has taught courses in constitutional law, employment discrimination, and critical race theory, as well as the Ninth Circuit Appellate Litigation Clinic, which received the Ninth Circuit's 2018 Distinguished Pro Bono Service Award. She received her JD from Yale Law School.

▶ **L iz Howard** serves as counsel for the Brennan Center's Democracy Program, where she works on cybersecurity and elections. Prior to joining the Brennan Center, Howard served as deputy commissioner of the Virginia Department of Elections. During her tenure, she coordinated many election administration modernization projects, including the decertification of all paperless voting systems, implementation of the e-Motor Voter program, and adoption of online, paperless absentee ballot applications. Before her appointment, she worked as general counsel at Rock the Vote and as a senior associate at Sandler Reiff. She received her JD from William and Mary School of Law.

▶ **Derek Tisler** is a fellow with the Brennan Center's Democracy Program. A recent graduate of the University of Chicago Law School, he served as editor in chief of the *University of Chicago Legal Forum* and participated in the Jenner & Block Supreme Court and Appellate Clinic. He previously interned with the Brennan Center, the Voting Rights Project at the Chicago Lawyers' Committee for Civil Rights, and the U.S. Department of Housing and Urban Development. Prior to law school, he worked in state legislative advocacy with a focus on urban policy. He holds a BA in economics from Michigan State University.

▶ **Lawrence Norden** is director of the Brennan Center's Election Reform Program. He has authored several nationally recognized reports and articles related to voting rights and voting technology, including *Securing Elections from Foreign Interference* (2017), *America's Voting Machines at Risk* (2015), *How to Fix Long Lines* (2013), *Better Design, Better Elections* (2012), and *Voting Law Changes in 2012* (2011). His work has been featured in media outlets across the country, including the *New York Times*, the *Wall Street Journal*, CNN, Fox News, MSNBC, and NPR. He has testified before Congress and several state legislatures on numerous occasions. He received his JD from New York University School of Law.

ABOUT THE BRENNAN CENTER'S DEMOCRACY PROGRAM

The Brennan Center's Democracy Program encourages broad citizen participation by promoting voting and campaign finance reform. We work to secure fair courts and to advance a First Amendment jurisprudence that puts the rights of citizens — not special interests — at the center of our democracy. We collaborate with grassroots groups, advocacy organizations, and government officials to eliminate the obstacles to an effective democracy.

ACKNOWLEDGMENTS

The authors would like to thank the many colleagues who collaborated in preparing this tool kit or earlier iterations of it. Lisa Danetz, Frank Reyes, Amy Larsen, Christopher Deluzio, and Wilfred Codrington contributed crucial research and editorial support. Research and Program Associates Brianna Cea, Shyamala Ramakrishna, and Andrea Córdova McCadney merit special thanks for their sustained assistance in researching, fact checking, and editing. We are also indebted to the many experts and officials whose knowledge and feedback helped shape this tool kit or its earlier iterations. We gratefully acknowledge the following individuals for sharing their insights:

Joshua Franklin, deputy chief information security officer, and Maurice Turner, senior advisor to the executive director, Election Assistance Commission; Noah Praetz, former director of elections, Cook County, Illinois, and partner, Elections Group; Maribeth Witzel-Behl, city clerk, Madison, Wisconsin; Joseph Kirk, elections supervisor, Bartow County, Georgia; Neal Kelley, registrar of voters, Orange County, California; Susannah Goodman, director of election security, Common Cause; Liza McLenaghan, state chair, Common Cause Florida; Matthew Davis, former chief information officer, Virginia Department of Elections; Marian K. Schneider, president, and Cris Landa, program director, Verified Voting; Matthew Bernhard, PhD candidate, University of Michigan; Jared Marcotte, president, The Turnout; Meredith Berger, senior manager, Defending Democracy, Microsoft; Ginny Badanes, director of strategic projects, Cybersecurity & Democracy, Microsoft; Jocelyn Woolbright, policy analyst, and Alissa Starzak, head of public policy, Cloudflare; Megan Stifel, executive director of the Americas, Mary Kavaney, chief legal and administrative officer, and Shehzad Mirza, director of operations, Global Cyber Alliance; Dan S. Wallach, professor, Department of Computer Science, and Rice Scholar, Baker Institute of Public Policy, Rice University; Joseph Lorenzo Hall, senior vice president, Strong Internet, Internet Society; Whitney May, director of government services, Center for Tech and Civic Life; James Suver, vice president of business development, Runbeck Election Services; Pam Smith, senior adviser, Verified Voting; Whitney Quesenbery, codirector, Center for Civic Design; Dana Chisnell, codirector, Center for Civic Design; Marcia Johnson-Blanco, codirector, Lawyers' Committee for Civil Rights Under Law; Laura Grace, election protection manager, Lawyers' Committee for Civil Rights Under Law; Michelle Bishop, disability advocacy specialist for voting rights, National Disability Rights Network; Aquene Freechild, campaign codirector, Public Citizen; Emily Berger, senior fellow, Public Citizen; Dana DeBeauvoir, county clerk, Travis County, Texas; Genya Coulter, precinct clerk at Polk County, Florida, Supervisor of Elections; Tonia A. Tunnell, director of government relations, Maricopa County, Arizona, Recorder's Office and Elections Department; Richard Rydecki, assistant administrator, Wisconsin Elections Commission; and Susan Greenhalgh, senior advisor on election security, Free Speech for People.

BRENNAN CENTER FOR JUSTICE

Brennan Center for Justice at New York University School of Law
120 Broadway // 17th Floor // New York, NY 10271
www.brennancenter.org