POLICY REPORT

BRENNAN CENTER FOR JUSTICE

Preparing for Cyberattacks and Technical Failures

A Guide for Election Officials

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

PUBLISHED DECEMBER 19, 2019

Brennan Center for Justice at New York University School of Law

Table of Contents

STAY CONNECTED TO THE BRENNAN CENTER

Visit our website at
www.brennancenter.org

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.

ABOUT THE BRENNAN CENTER'S DEMOCRACY PROGRAM

The Brennan Center's Democracy Program works to repair the broken systems of American democracy. We encourage 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.

Introduction

America's intelligence agencies have unanimously concluded that the risk of cyberattacks on election infrastructure is clear and present — and likely to grow.[1] While officials have long strengthened election security by creating resiliency plans,[2] the evolving nature of cyber threats makes it critical that they constantly work to improve their preparedness. It is not possible to build an election system that is 100 percent secure against technology failures and cyberattacks, but effective resiliency plans nonetheless ensure that eligible voters are able to exercise their right to vote and have their votes accurately counted. This document seeks to assist officials as they revise and expand their plans to counter cybersecurity risks.

Many state and local election jurisdictions are implementing paper-based voting equipment, risk-limiting audits, and other crucial preventive measures to improve overall election security. In the months remaining before the election, it is at least as important to ensure that adequate preparations are made to enable quick and effective recovery from an attack if prevention efforts are unsuccessful.

While existing plans often focus on how to respond to physical or structural failures, these recommendations spotlight how to prevent and recover from technological errors, failures, and attacks. Advocates and policymakers working to ensure that election offices are prepared to manage technology issues should review these steps and discuss them with local and state election officials.

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. E-pollbooks expedite the administration process, shorten lines, lower staffing needs, and save money. Most e-pollbooks can communicate with other units in the same 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.

There are no national standards for e-pollbook operations or security. E-pollbooks present unique challenges because they need to maintain updated information across numerous devices and locations. Additionally, many devices that may be used as e-pollbooks do not have the ability to connect via physical networks and require some type of wireless communication to convey important information. Election officials should consider the following security recommendations when using e-pollbooks:

Limit or eliminate connectivity to wireless networks whenever possible. E-pollbooks used for voter check-in generally do not need wireless connections. Officials who operate precinct-based voting on Election Day should choose e-pollbook options that use 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 types of 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.[3]

Implement proper security protocols when wireless connectivity is required. Election officials using vote centers and multiple early-voting locations may require some 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. If wireless networks must be used, officials should implement security protocols, including encrypting communication between e-pollbooks and requiring strong passwords that are changed after every election.

Ensure that systems are properly patched as part of Election Day preparations. E-pollbooks must 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 start by reviewing 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.[4] Adhering to these requirements will ensure that election officials are using best practices for securing election systems, protecting the personally identifiable information (PII) of voters, and preserving 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.

Keep appropriate backup of e-pollbooks in polling places. Paper backups of e-pollbooks are the best resiliency measure in the event of an e-pollbook failure. They allow poll workers to continue confirming voters' eligibility, diminish the potential for long lines, and may minimize the need to issue provisional ballots. While jurisdictions in 41 states and the District of Columbia (DC) use e-pollbooks, our research indicates that only 11 states and DC formally require paper backups on Election Day, although several other states recommend the practice or have counties that voluntarily keep paper backups.[5] Durham County, North Carolina, experienced a significant failure of e-pollbooks in November 2016, when many voters arrived at the polls to find that they had been marked on the e-pollbooks as already having voted or were improperly marked as needing to provide additional identification.[6] Voting was delayed for more than an hour and a half as the county printed paper pollbooks and delivered them.[7] This delay could have been avoided if printed pollbooks had been sent ahead of time with other polling place materials. Preemptively sending paper backup of e-pollbooks to polling places obviates the need for detailed logistics in case of e-pollbook failure.

Jurisdictions should evaluate their e-pollbook recovery procedures to ensure they will be easy for poll workers

to follow and will not introduce new obstacles to voters casting their ballots quickly. As the use of vote centers and other centralized voting locations increases, printing pollbooks may create logistical and administrative challenges. These types of voting locations may need other backup options, such as nonnetworked devices from a different vendor that contain the entire list of registered voters for a jurisdiction, along with the correct ballot style and current status (i.e., voted, absentee, or not voted) for each voter. Another option is to produce a backup list on demand using high-speed printers. This backup procedure, which New Hampshire law calls for, could allow polling places to quickly transition from malfunctioning e-pollbooks to paper backups.

Provide sufficient provisional ballots and materials for two to three hours of peak voting. A key backup measure for Election Day is to supply sufficient provisional ballots and provisional balloting materials. It is preferable to issue regular ballots to eligible voters if the e-pollbook system fails. However, it may not be possible to determine voter eligibility in the event of such a failure, especially if backup paper pollbooks are unavailable or are found to contain errors. Provisional ballots ensure that individuals can cast a ballot while providing election officials time to determine their eligibility. These ballots should be counted once officials determine eligibility, with no further action required of the voter. Having sufficient provisional ballots to account for two to three hours of peak voting activity will allow voting to continue in the event of system failures.[8] For the November 2020 election, this will require enough provisional ballots for at least 35 percent of registered voters.[9] While not 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. Contingency plans must provide for additional materials to be delivered if the problem cannot be resolved.

Train poll workers to implement pollbook contingencies. Improper or insufficient training of poll workers can lead to voters being turned away, long lines, and ineligible individuals casting ballots. Poll worker instructions for managing provisional ballots must specify how to handle e-pollbook failures appropriately, including when to allow voters to cast a regular ballot and when to issue provisional ballots instead. Whenever voter eligibility can be confirmed in a timely fashion through the use of appropriate backups, regular ballots should be issued. The U.S. Election Assistance Commission (EAC) provides a list of guidelines for poll workers regarding provisional ballots as well as some best practices for poll worker accountability. Provisional ballot forms must clearly indicate the sections that should be filled out by voters, poll workers, and election staff, so each person knows what he or she needs to do. It is also important to provide a clear list of circumstances in which to use provisional ballot envelopes, including on the envelopes themselves. In 2018, Virginia adopted new provisional ballot materials created in coordination with the Center for Civic Design that illustrate these best practices.[10]

More Resources

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

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

Pew E-pollbook Database
www.pewtrusts.org/en/research-and-analysis/data-visualizations/2017/a-look-at-how-and-how-many-states-adopt-electronic-poll-books

National Conference of State Legislatures Page on E-pollbooks
www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx

EAC Standards for Poll Workers
www.eac.gov/research-and-data/provisional-voting

Center for Civic Design on Provisional Ballots
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. For digital or optical-scan voting systems, recovery in case of an equipment failure can be relatively fast; as ballots are already printed, voting can continue while the tabulator issue is resolved. As a Brennan Center report on voting machines notes, jurisdictions 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."[11]

These problems can occur when jurisdictions use ballot-marking devices (BMDs) and ballot-on-demand (BOD) printers as well. 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 failures on Election Day.

If using paper ballots, print enough ballots for all registered voters. Many election officials using paper ballots decide how many ballots to print on the basis of prior election turnout or the percentage of registered voters expected to vote. This approach can result in ballot shortages and leave jurisdictions unprepared for unexpected voter surges. This happened across the country during the 2018 midterm elections, when turnout reached historic levels, and many experts predict record-breaking turnout in 2020.[12] To prepare, election officials should print enough ballots for all registered voters. Jurisdictions that allow Election Day registration may require an even higher ballot supply.

If using voting systems that do not require preprinted ballots, print enough emergency paper ballots for 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 vote due to a voting machine malfunction. Emergency ballots are different from provisional ballots, which are given to voters whose eligibility is unclear. Emergency ballots should be counted as soon as functional voting equipment becomes available, without any additional scrutiny of voter qualifications, unlike provisional ballots, which may require research on voter eligibility. Printing enough emergency ballots for two to three hours of peak voting activity will allow voting to continue until equipment can be repaired or replaced, or until additional paper ballots can be delivered to a polling place. For the November 2020 election, this will require enough provisional ballots for at least 35 percent of registered voters. Appropriate procedures should be put in place for chain of custody and accounting for preprinted paper ballots.

DRE voting systems directly record, in electronic form, voters' selections in each race or contest on the ballot. An increasing number of states and local jurisdictions have begun replacing antiquated DREs with BMDs as the primary voting option. Others are increasingly using vote centers, which often rely on BOD printers to produce on-site any ballot style and language that might be needed for a particular voter. Because these systems do not need preprinted ballots, election jurisdictions using DREs, BMDs, or BOD-printed ballots as their primary voting option should preprint and distribute emergency paper ballots that can be counted by existing tabulators. There are 16 states that will use DREs as the principal polling place equipment in at least some jurisdictions in 2020.[13] However, at least seven do not mandate that paper ballots be made available in the event of DRE failure.[14]

In vote centers that have a large number of ballot styles, preprinted emergency ballots for at least the precincts closest to that vote center should be stocked. Vote centers can also be stocked with master copies of emergency paper ballots in all necessary styles and languages, along with a photocopier to reproduce them in emergency situations.

Tabulators should be programmed to accept and read both ballots produced by the BMD/BOD printers and preprinted emergency ballots. Preelection testing should verify that the tabulators properly identify and record both types of ballots.

Develop procedures to manage and track malfunctioning equipment or equipment failure. Machines that appear to be malfunctioning or improperly calibrated should be taken out of service and additional voting equipment deployed to the polling place or vote center. Recalibrating DRE touch screens or conducting any other necessary voting equipment repairs should be done in full view of observers. Any reports from voters of machine errors should be tracked and immediately reported to the

central election office. Election offices should review and compare these reports across voting locations to identify trends that could indicate widespread problems, including potential cyberattacks. Training should ensure that poll workers understand the process for counting ballots, including potentially hand-counting ballots, if equipment failure cannot be resolved before voting ends.

Communicate with voters to build trust in the election process. Election officials should preprint signage that will allow poll workers to inform voters of equipment failures in a manner that is consistent across locations and approved by the election office. On Election Day, poll workers should ensure that voters are not directed to use machines that are suspected of producing erroneous records.

Poll workers should also take steps to make sure that voters accurately recorded their selections 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 paper printout matches the selections they made on the machine. For example, when using BMDs that print a ballot that must then be scanned by a separate machine, poll workers should say to voters, after their ballot has been printed and before it is cast: "Don't forget to check the printed ballot carefully. If you see something wrong, you can get a replacement. Then you'll go [over there] to cast it."

Take steps to prevent late 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 an opportunity to cast a ballot.[15] Poll workers should be trained to deal with equipment failures occurring on the morning of Election Day. Voters should be allowed to vote using emergency paper ballots if voting equipment is not operable when the polls open. Poll workers should explain to voters how their ballots will be counted once working voting equipment becomes available.

Plan to assist voters with disabilities if voting machines fail. If accessible voting machines fail and paper ballots are used instead, disabled voters may not be able to vote privately and independently. 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 equipment failure.[16] Poll workers should be appropriately trained on any backup systems used to provide accessibility.

More Resources

Brennan Center Report on Voting Machines at Risk
www.brennancenter.org/analysis/americas-voting-machines-risk-an-update

Brennan Center Voting Equipment Overview
www.brennancenter.org/analysis/overview-voting- equipment

Verified Voting Verifier – Lookup Tool for Polling Place Equipment
www.verifiedvoting.org/verifier

Prevent and Recover from Voter Registration System Failures and Outages

Voter registration systems maintain official lists of registered voters, including all voter information and district assignment information. The statewide systems usually serve additional election-management purposes as well, such as processing absentee ballots. A failure of the registration system on or near Election Day can cause problems producing files for paper pollbooks or e-pollbooks, using voter information lookup tools, or validating provisional ballots immediately after the election.

Establish a 60-day preelection blackout window for all noncritical software updates and patches. These windows increase the likelihood that programming errors, viruses, or other problems will be discovered in a timely manner prior to Election Day. Sixty days provides sufficient time before the close of voter registration or the start of absentee voting to identify whether installed patches or updates have created unintended system issues. Even updates that do not directly impact voter registration databases, such as server patching, networking equipment upgrades, and locality telecommunications system changes, may impact a local election official's ability to access the state voter registration database. Therefore it is critical that these blackout dates be established and communicated with relevant staff to prevent potential issues on or shortly before Election Day. The plan should include a process for emergency updates during the blackout window, indicating who will authorize the emergency update and how it will be tested prior to rollout.

Subject the system periodically to independent vulnerability testing. States can either partner with the Department of Homeland Security or engage outside cybersecurity consultants to test the system for vulnerabilities on a periodic basis. Vulnerability testing should be conducted well in advance of an election, and at least quarterly, to provide sufficient time to resolve any potential vulnerabilities that are discovered. While the specific results of vulnerability testing need not be released so as to maintain system security, officials should be transparent about what entity conducted the testing and what standards it used.

Maintain backup copies of digital records off-line in case online access is limited. In the lead-up to the election, local officials should download an electronic copy of voter information on a daily basis and store it securely, so that they have the most recent information in case the voter registration system becomes unavailable. This can be used to conduct research on provisional ballots after the election.

Provide voters with tools to look up their voter registration status online and conduct outreach to urge voters to use the tool in advance of any registration deadline. Voters can provide crucial information about undesired changes to their registration, including address changes they did not request, which could be an early indicator of a possible breach. Encouraging voters to check before a deadline ensures that problems can be resolved in a timely fashion. It may also reduce pressure on poll workers on Election Day.

Provide voters with tools to look up their polling place information online, and make alternative websites available. In case a voter lookup tool fails, election officials should be prepared to provide links to other polling place lookup tools, such as the Voting Information Project (VIP), an independent entity that provides information to voters using official data. New Jersey successfully used VIP to provide information to voters after Hurricane Sandy made state systems unavailable and necessitated a large number of polling place changes in advance of the 2012 election.[17] Using tools such as VIP for polling place lookups, instead of sites that depend on statewide registration systems, also reduces the load on state servers at busy times in the election season. This requires providing accurate polling place data to the backup site in advance of elections and confirming that the backup site is working correctly.

More Resources

EAC Deep Dive on Election Technology
www.eac.gov/documents/2018/05/01/eavs-deep-dive-election-technology

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

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

Voting Information Project
www.votinginfoproject.org

Prevent and Recover from Election Night Reporting System Failures and Outages

Local and state officials usually post unofficial results on election night. While this information does not reflect the certified results, large differences between unofficial election night results and the final outcome can create questions for voters about the accuracy of the process. Election night reporting sites are prime targets for denial of service (DoS) attacks because the sites' high-use period is known ahead of time, and preventing access to unofficial results can create negative media attention about the electoral process. A hotly contested race can intensify interest in the election results, and a large increase in visitors to a reporting site in a short period can likewise bring down the site.

Establish redundancies. Some states, including Arizona and Virginia, experienced election night reporting failures in the 2014 midterm elections.[18] Addressing the system failures after the election, several of these states established a redundant system that can be made available if the main system fails.[19]

Do not connect election night reporting systems to voting systems or the statewide registration system. Election night reporting systems (ENRs) are attractive targets for cybercriminals and other nations. 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 DoS attack linked to foreign IP addresses during its May 1, 2018, primary elections. Although this attack likely served as a distraction from a separate attack on the county's servers, the reporting website itself did not provide an avenue for future disruption. The county's deputy director of IT 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."[20]

More Resources

EAC 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

Communication Strategy

All good contingency plans include a communication plan. At its core, a communication plan is intended to assist election officials in distributing essential information in a timely manner and maintaining public confidence in the election's administration. Communication plans are important in all unexpected situations, from equipment failures to potential cyberattacks to unintentional errors.

Draft, review, and approve a communication plan prior to Election Day. Keeping voters, poll workers, and others informed minimizes the harm that could arise on Election Day in the event of negative developments. The most basic communication plan includes key staff and contacts. A more detailed strategy may include various response options for potential problems as well as longer-term considerations, such as notification requirements in the event personal voter information has been leaked.

Provide a public website for emergency communications. Officials should publicize links where emergency information will be posted on Election Day, possibly including official social media accounts used by state and local election officials. These can serve as official sources where voters, candidates, media, and advocacy organizations can find information regarding extended polling place hours, polling place relocations, and other emergency information. Doing this in advance of an election will make emergency communications easier for election officials.

Be transparent but careful. As the Belfer Center for Science and International Affairs suggests, "Transparent communication builds trust, but in a cyber incident, you will have few facts at hand, especially at the outset. Public comments should demonstrate that you are taking the issue seriously but avoid providing any details that may change as the investigation progresses, so you don't have to correct yourself down the line. Avoid speculation on the perpetrator of the incident."[21]

More Resources

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

Endnotes

1 See generally Senate Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 1*, 2019, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf; Robert S. Mueller III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, U.S. Department of Justice, 2019, https://www.justice.gov/storage/report.pdf; and Olivia Gazis, "Intel Chiefs Warn of Russia-China Alliance as Threats Grow More Complex," CBS News, Jan. 29, 2019, https://www.cbsnews.com/news/intelligence-chiefs-provide-updates-on-worldwide-threats-2019-01-28-live-updates.

2 See, e.g., Wisconsin State Board of Elections, *Report on Election Related Contingency Planning*, 2007, https://elections.wi.gov/sites/default/files/publication/65/election_related_contingency_planning_2007_pdf_19060.pdf; Senate Select Committee on Intelligence, *Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Draft SSCI Recommendations*, 2018, https://www.burr.senate.gov/imo/media/doc/RussRptInstlmt1-%20ElecSec%20Findings%2CRecs2.pdf.

3 See, e.g., Armis, *Protecting the Enterprise from BlueBorne*, 2017, https://go.armis.com/hubfs/BlueBorne%20Technical%20White%20Paper.pdf; 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, CA, Aug. 2019), https://www.usenix.org/conference/usenixsecurity19/presentation/antonioli.

4 National Institute of Standards and Technology, "Cybersecurity Framework," accessed Nov. 20, 2019, https://www.nist.gov/cyberframework.

5 In our research, we found written paper backup requirements for e-pollbooks in 11 states and Washington, DC. These 11 states are Connecticut, Georgia, Michigan, Minnesota, New Jersey, North Carolina, Ohio, Pennsylvania, Rhode Island, South Carolina, and South Dakota. Mississippi and West Virginia have laws recommending paper backups. In Nevada and Wyoming, backup paper pollbooks are available in practice everywhere e-pollbooks are used, while in other states, like 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 e-pollbook solution.

6 Pam Fessler, "Russian Cyberattack Targeted Elections Vendor Tied to Voting Day Disruptions," NPR, Aug. 10, 2018, https://www.npr.org/2017/08/10/542634370/russian-cyberattack-targeted-elections-vendor-tied-to-voting-day-disruptions.

7 Fessler, "Russian Cyberattack Targeted Elections Vendor."

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

9 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 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/MIT-Charles-Stewart-Voter-Turnout-Study-2016.pdf.

10 Center for Civic Design, "Making Provisional Voting Easier in Virginia," accessed Nov. 20, 2019, https://civicdesign.org/showcase/making-provisional-voting-easier-in-virginia.

11 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.

12 Henry Olsen, "We Could Have Record Turnout in the 2020 Election. We're Not Ready for It," *Washington Post*, Oct. 10, 2019, https://www.washingtonpost.com/opinions/2019/10/10/we-could-have-record-turnout-election-were-not-ready-it.

13 These 16 states are Arkansas, Indiana, Illinois, Kansas, Kentucky, Louisiana, Mississippi, Nevada, New Jersey, North Carolina, Ohio, Texas, Tennessee, Utah, Wyoming, and West Virginia. Three states that have recently used DREs — Georgia, South Carolina, and Pennsylvania — have committed to replacing them by 2020.

14 We have identified the following states where there are no provisions mandating that paper ballots be made available in the event of DRE failure: Kansas, Nevada, North Carolina, Texas, Utah, West Virginia, and Wyoming. While not required by statute, polling places in some of these states may provide some form of emergency paper ballots when systems go down. 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 use 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 the provision of emergency paper ballots; and West Virginia counties have contingency plans in the event of machine failure.

15 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.

16 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 State of Oregon, "Voting Instructions for Voters with a Disability," accessed Nov. 20, 2019, https://sos.oregon.gov/voting/Pages/instructions-disabilities.aspx.

17 Susan K. Urahn, "Collaboration, Technology and the Lessons of Election Day," *Governing: States and Localities*, Jan. 16, 2013, https://www.governing.com/columns/mgmt-insights/col-collaboration-technology-voting-information-accessibility.html.

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

19 Eidam, "Is Your Election Night Reporting System Ready?"

20 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/.

21 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 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.

▶ **Liz 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.

▶ **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.

ACKNOWLEDGMENTS

The Brennan Center gratefully acknowledges Carnegie Corporation of New York, Change Happens Foundation, Craig Newmark Philanthropies, Lee Halprin and Abby Rockefeller, the JPB Foundation, Leon Levy Foundation, Open Society Foundations, Rockefeller Brothers Fund, and Wallace Global Fund for their generous support of our election security work.

The authors would like to thank the many colleagues who collaborated in preparing this tool kit. Derek Tisler, Christopher Deluzio, and Wilfred Codrington contributed crucial research and editorial support to this project. 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. We gratefully acknowledge the following individuals for sharing their insights: 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; Susannah Goodman, director of election security, Common Cause; Neal Kelley, registrar of voters, Orange County, California; Noah Praetz, director of elections, Cook County, Illinois; Matthew Davis, former chief information officer, Virginia Department of Elections; 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; Maribeth Witzel-Behl, city clerk, Madison, Wisconsin; Richard Rydecki, assistant administrator, Wisconsin Elections Commission; Susan Greenhalgh, national policy director, National Election Defense Coalition; and Maurice Turner, senior technologist, Center for Democracy & Technology.

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