BRENNAN
CENTER
FOR JUSTICE

Better Safe Than Sorry

HOW ELECTION OFFICIALS CAN PLAN AHEAD TO PROTECT THE VOTE IN THE FACE OF A CYBERATTACK

By Edgardo Cortés, Liz Howard,
and Lawrence Norden

Brennan Center for Justice at *New York University School of Law*

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. At this critical moment, 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.

About the Brennan Center's Publications

Red cover | Research reports offer in-depth empirical findings.

Blue cover | Policy proposals offer innovative, concrete reform solutions.

White cover | White papers offer a compelling analysis of a pressing legal or policy issue.

Acknowledgments

The Brennan Center gratefully acknowledges the Carnegie Corporation of New York, Change Happens Foundation, Democracy Alliance Partners, Ford Foundation, The JPB Foundation, The Kohlberg Foundation, Leon Levy Foundation, Open Society Foundations, Rockefeller Brothers Fund, Abby Rockefeller and Lee Halprin, 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 toolkit. Christopher Deluzio and Wilfred Codrington contributed crucial research and editorial support to this project. Zachary Roth, Director of the Brennan Center's Editorial and Social Strategy section, lent valuable review and editing assistance. Research and Program Associates Brianna Cea and Shyamala Ramakrishna merit special thanks for their sustained assistance in researching, fact-checking, and editing.

We are also immensely grateful to the many experts and officials whose knowledge and feedback helped shape this toolkit. We gratefully acknowledge the following individuals for their insight in the research and writing process: Pam Smith, Senior Advisor, Verified Voting; Whitney Quesenbery, Co-Director, Center for Civic Design; Dana Chisnell, Co-Director, Center for Civic Design; Marcia Johnson-Blanco, Co-Director, 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 Co-Director, Public Citizen; Emily Berger, Senior Fellow, Public Citizen; 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; Susan Greenhalgh, National Policy Director, National Election Defense Coalition; and Maurice Turner, Senior Technologist, Center for Democracy & Technology.

About the Authors

Edgardo Cortés is the Election Security Advisor for the Brennan Center's Democracy Program. An expert on election administration and policy, Mr. Cortés served as the first Virginia 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 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. Mr. Cortés received his undergraduate degree from Cornell University and earned his master's degree in political management from George Washington University.

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, Ms. Howard served as Deputy Commissioner for 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. Prior to her appointment, she worked as General Counsel at Rock the Vote and as a Senior Associate at Sandler Reiff. She earned her J.D. from William and Mary School of Law.

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

Table of Contents

Introduction

America's intelligence agencies have unanimously concluded that possible cyberattacks on election infrastructure pose a clear and present danger — one that is likely to grow.[1] The intelligence community is also unanimous in their conclusion that Moscow was behind a coordinated infiltration of America's election infrastructure in 2016. "These actions are persistent, they're pervasive, and they are meant to undermine America's democracy on a daily basis, regardless of whether it is election time or not,"[2] said Dan Coats, Director of National Intelligence. Republican Senator James Lankford of Oklahoma summed up this new reality for election officials by noting that "we must proactively work to ensure the security of our election infrastructure for the possibility of interference from not just Russia, but possibly another adversary like Iran or North Korea or a hacktivist group."[3]

While there are many options to improve overall election security through the use of paper-based voting equipment, risk-limiting audits, and other crucial steps, they might not happen before November. Efforts to prevent attacks in the first place are, of course, critical. But in the months remaining before the election, it is at least equally important to ensure adequate preparations are in place to quickly and effectively recover if prevention efforts are unsuccessful.

Election officials have long been focused on creating contingency plans ahead of Election Day, creating battle plans that are a source of strength as our elections face new security threats.[4] The Senate Intelligence Committee recently reviewed security planning by state and local election officials as part of its investigation into foreign interference in the 2016 election and concluded "that U.S. election infrastructure is fundamentally resilient."[5] Nevertheless, in light of the evolving nature of cyber threats, it is critical that officials constantly examine and work to improve our systems' preparedness, particularly related to election technology.

This document seeks to assist election officials as they revise and expand existing plans to counter cybersecurity risks. Many existing plans focus on physical or structural failures; the Brennan Center's recommendations spotlight preventing and recovering from technological errors, failures, or attacks. Advocates and policy makers working to ensure election offices are prepared for technology issues should review these steps and discuss them with local and state election officials. Effective contingency plans will ensure that eligible voters are able to exercise their right to vote and have those votes accurately counted.

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 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.

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 modern devices that may be used as electronic pollbooks do not have the ability to connect via physical networks and require some type of wireless communication to connect and communicate important information.

Election officials should consider the following security recommendations when using electronic pollbooks:

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. Officials who operate precinct-based voting on Election Day should opt for e-pollbook options that utilize 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 like BlueBorne between Bluetooth-connected devices.[6]

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 the wireless connections within the systems are eliminated or disabled. For example, certain e-pollbooks use Apple iPads that rely solely on wireless connectivity for communication. If wireless networks must be used, officials should implement security protocols, including utilizing encrypted communication between e-pollbooks and strong passwords that are changed after every election.

Ensure 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. A good place to start is reviewing any guidelines or requirements created by state or local government IT agencies. States and localities may develop their state cybersecurity requirements based on the National Institute of Standards and Technology's cybersecurity framework.[7] 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 ensuring the integrity of voter data used on Election Day.

Keep paper backup of electronic pollbooks in the polling place. Paper backups of e-pollbooks are the best form of reinforcement in the event of an e-pollbook failure. They allow poll workers to continue confirming eligibility of voters, minimize the potential for long lines, and may minimize the need to issue provisional ballots. While jurisdictions in 34 states use e-pollbooks, at least 11 of those states do not require paper backup of e-pollbooks on Election Day.[8] Durham County, North Carolina, experienced a significant failure of e-pollbooks in November 2016, when voters appeared at the polls on Election Day but were marked on the e-pollbooks as already having voted or were improperly marked as needing to provide additional identification.[9] Voting was delayed for more than an hour and a half while the county printed paper pollbooks and managed delivery logistics.[10] This delay could have been avoided by preemptively sending printed paper pollbooks with other polling place materials ahead of time. Sending paper backup of e-pollbooks to polling places obviates the need for detailed logistics to deliver paper pollbooks in case of e-pollbook failure. Jurisdictions should evaluate their recovery procedures to ensure they will be easy for poll workers to follow and will not introduce new obstacles to allowing voters to cast ballots quickly. Vote centers and early voting locations may need to consider other backup options, such as a nonnetworked device containing the entire list of registered voters for a jurisdiction.

Provide sufficient provisional ballots and materials for two to three hours of peak voting. A key backup measure for Election Day system failures is a supply of 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 e-pollbook failure, especially if backup paper pollbooks are unavailable or are found to contain errors. Provisional ballots ensure individuals can cast a ballot, while providing election officials additional time to determine their eligibility. 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.[11] This will not be enough to deal with an all-day problem, but it will provide sufficient time for other measures to be implemented or additional ballots and materials to be delivered. The contingency plan must include plans to deliver additional materials if the problem cannot be resolved.

Provide training for poll workers on implementing pollbook contingencies. Improper or insufficient training of poll workers can lead to voters being turned away, long lines, and ineligible individuals being allowed to cast a ballot. Poll worker instructions for managing provisional ballots must include e-pollbook failure as a reason for issuing provisional ballots.[12] The EAC's list of ideal standards provides a list of items that poll workers should know about issuing provisional ballots as well as some best practices for poll worker accountability. Provisional ballot forms must make the sections each person uses clear, so voters, poll workers, and all election staff know what they 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. Virginia recently adopted new provisional ballot materials created in coordination with the Center for Civic Design that illustrate these best practices.[13]

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/multimedia/data-visualizations/2017/a-look-at-how-and-how-many-states-adopt-electronic-poll-books

NCSL 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 much faster as ballots are already printed and voting can continue while the tabulator issue is resolved. As a Brennan Center report on voting machines notes, direct-recording electronic ("DRE") machines can cause more problems at the polls in the event of a failure as "voters may have to wait in long lines while election workers scramble to repair them."[14] These machines — used by 21 states as primary polling place equipment in at least some jurisdictions [15]— 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. Election officials should conduct logic and accuracy testing on 100 percent of voting equipment prior to every election to minimize the chance of unforeseen equipment failures on Election Day. In a recent report, the Center for American Progress gave four states — Hawaii, Indiana, Tennessee, and Virginia — a score of "unsatisfactory" for not requiring election officials to perform preelection logic and accuracy testing of all voting machines to be used in an election, though the Virginia Department of Elections *Handbook* states that all machines must be tested before being used in any election.[16]

If still using DREs, print backup emergency paper ballots for two to three hours of peak voting activity. DRE voting systems directly record, in electronic form, the voters' selections in each race or contest on the ballot. Typical DRE machines have flat panel display screens with touch-screen input, although other input technologies have been used, such as push-button. Election jurisdictions that rely solely on DREs for voting should print emergency paper ballots that can be hand-counted or tabulated by the jurisdiction's vote-by-mail voting equipment to use in case of equipment failure. Yet among the states that use DREs as the principal polling place equipment in at least some jurisdictions, at least eight states do not mandate that paper ballots be made available in the event of DRE failure.[17] Emergency ballots are 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 than provisional ballots that are provided to voters when their eligibility is unclear. Emergency ballots should be counted after the election without any additional scrutiny of voter qualifications, unlike provisional ballots that require research of voter eligibility. As with provisional ballots, printing enough ballots for two to three hours of peak voting activity allows voting to continue until paperless DRE equipment can be repaired or replaced, or until additional emergency paper ballots can be delivered to a polling place.

Print sufficient ballots for 100 percent of registered voters if using paper-based voting systems. Many election officials using paper-based voting systems choose to use formulas based on registered voters and prior election turnout information when deciding how many ballots to print. However, this approach can result in ballot shortages when turnout for an election is higher than historical data suggests, such as in Lynchburg, Virginia, during a special election in January 2017. Many expect higher turnout this November compared to recent midterm elections.[18]

Develop procedures to deal with equipment failure. Poll workers should provide information to voters about how their ballot will be counted if equipment is not working while they are voting. Training should ensure that poll workers understand the process for counting ballots, including potential hand counting ballots, if an equipment failure cannot be resolved before voting ends. Poll workers should remind voters to check their ballots to prevent over votes, which occur when voters vote for more than the maximum candidates allowed. Recalibration of DRE touchscreens and any other necessary voting equipment repairs should be done in full view of observers. Preprinted signage to inform voters of equipment failures allows poll workers to communicate consistently with voters with messaging approved by the election office. This signage can be sent with other polling place materials, and training should include instructions for when to post the signage.

Take steps to prevent late polling place openings. Poll workers should be trained for dealing with equipment failures on Election Day morning. Voters should be allowed to vote using emergency paper ballots or paper ballots that will be scanned later in the day. 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.[19]

Plan to assist voters with disabilities if voting machines fail. If accessible voting machines fail, disabled voters may not be able to vote privately and independently on paper ballots. If jurisdictions have sufficient resources, they should have backup accessible voting equipment, with all ballot styles available (similar to what would be used in a central voting site for early voting), in geographically dispersed areas so that it can be rapidly delivered to any polling place where the accessible equipment has failed. Longer term, jurisdictions might want to consider providing each polling place with accessible tablets and printers to be used for voters with disabilities in the event of voting-equipment failure.[20]

MORE RESOURCES

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

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

Verified Voting Verifier
www.verifiedvoting.org/verifier/

Prevent and Recover from Voter Registration System Failures/Outages

The voter registration system maintains the official list of registered voters, including all the voter information and district assignment information. The statewide voter registration system usually serves additional election-management purposes, such as processing absentee ballots and other election-management processes. A failure of the registration system on or near Election Day can cause problems in producing files for paper voter rosters 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 updates and patches. These windows increase the likelihood that any programming errors, viruses, or other problems will be discovered in a timely manner prior to Election Day. Coordinating with state and local technology staff is imperative to determine effective and reasonable blackout windows. Sixty days provides sufficient time before the close of voter registration and the start of absentee voting to identify if installed patches or updates created unintended system issues. Even updates not affiliated with the voter registration database, such as server patching, networking equipment upgrades, and locality telecommunication system changes, may impact a local election official's ability to access the state voter registration database, so it is critical that these blackout dates be established and communicated with the 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 to independent vulnerability testing on a periodic basis. States can either partner with the U.S. 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, on at least a quarterly basis, to provide sufficient time to resolve any potential vulnerabilities that are discovered. While specific results of vulnerability testing should not be released so as to maintain system security, officials should be transparent about what entity is conducting the testing and what standards are being used to conduct the review.

Maintain backup copies of digital records offline 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 they have the most recent information in case the voter registration system becomes unavailable. This can be used to conduct research for provisional ballots after the election.

Provide tools to voters for looking up their voter registration status online and conduct outreach to urge voters to use the tool in advance of any registration deadline. Voters who check their registration can provide crucial insights about undesired changes to their registration, including address changes they did not request or other problems, serving as an early warning system for possible breach. Encouraging voters to check before a deadline ensures problems can be resolved in a timely fashion so that they can participate and may reduce pressure on poll workers on Election Day.

Provide tools to voters to look up their polling place information online and have alternative links available. In case of a voter lookup tool failure, election officials should be prepared to provide links to other polling place lookup tools, such as the Voter Information Project (VIP).[21] New Jersey successfully used VIP to provide information to voters after Hurricane Sandy made state systems unavailable and prompted a large number of polling place changes in advance of the 2012 election.[22] Using tools such as VIP for polling place lookups instead of sites that depend on the statewide registration system also reduces the load on servers at busy times in the election season. This requires providing accurate polling place data to the backup site in advance of the election and confirming that the backup site is working correctly. VIP expects to have polling place data from all 50 states and the District of Columbia for the November 2018 general election, and so it is a backup option available to all states.[23]

MORE RESOURCES

EAC Deep Dive: 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/

Prevent and Recover from Election Night Reporting System Failures/Outages

Officials usually post unofficial results on election night at the local and state level. While this information does not reflect the certified results, large changes 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 it is known when the high-use period will be on the site, and preventing access to unofficial results can create negative media attention about the process. In addition to purposeful DoS attacks, a hotly contested race can increase interest in the election results and create the same issue of a large increase in visitors to the site in a short period of time.

Establish redundancies. Several states, including Arizona and Virginia, experienced election night reporting failures in the 2014 midterm elections.[24] In making changes after the election to address the system failures, several states focused on establishing a redundant system that could be made available if the main system failed.[25]

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, including foreign nation-states. Bad actors have successfully attacked ENRs around the world, including in Ukraine and Bulgaria, and more recently, here in 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 the May 1, 2018, primary elections. The Knox County, Tennessee, deputy director of IT noted that the county's 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."[26]

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 retaining public confidence in the election administration system. Communication plans are important in all unexpected situations, from equipment failure to potential cyberattacks to unintentional errors.

Election officials should draft, review, and approve a communication plan prior to a negative development on Election Day. Keeping voters, poll workers, and others informed minimizes the negative impact of issues that arise on Election Day. The most basic communication plan includes key staff and contacts. A more detailed communication strategy may include various response options to different potential problems and more long-term considerations, such as notification requirements in the event personal voter information has been leaked.

Provide a public site for emergency communications. Officials should have a well-publicized link where emergency information will be posted on Election Day. This will provide an official source where voters, candidates, media, and advocacy organizations can go to find information regarding extended polling place hours, emergency polling place relocations, and other emergency information. Publishing a link in advance of the election will make emergency communications easier for election officials.

Be transparent but careful, as the Belfer Center 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.”[27]

MORE RESOURCES

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

Endnotes

1 *See* Miles Parks, "Russian Threat to Elections to Persist Through 2-18, Spy Bosses Warn Congress," *National Public Radio*, February 13, 2018, https://www.npr.org/2018/02/13/584672450/intelligence-leaders-testify-about-global-threats-in-senate-hearing.

2 Veronica Stracqualursi, "US Intelligence Chief: 'The Warning Lights Are Blinking Red Again' On Cyberattacks," *CNN*, July 14, 2018, https://www.cnn.com/2018/07/14/politics/director-of-national-intelligence-dan-coats-cyberattacks-russia/index.html.

3 *See* "Senate Intel Committee Releases Unclassified 1st Installment in Russia Report, Updated Recommendations on Election Security," Press Releases, Senator Mark R. Warner, May 8, 2018, https://www.warner.senate.gov/public/index.cfm/2018/5/senate-intel-committee-releases-unclassified-1st-installment-in-russia-report-updated-recommendations-on-election-security.

4 *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.

5 Senate Select Committee on Intelligence, *Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Draft SSCI Recommendations*, 115th Cong., 2d sess., 2018, S. Rep., https://www.burr.senate.gov/imo/media/doc/One-Pager%20Recs%20FINAL%20VERSION%203-20.pdf.

6 *See* Armis, "Protecting the System from BlueBorne,"(2017), https://go.armis.com/hubfs/BlueBorne%20Technical%20White%20Paper.pdf.

7 *See* "Cybersecurity Framework," National Institute of Standards and Technology, https://www.nist.gov/cyberframework.

8 "Electronic Poll Books/E-Poll Books," National Conference of State Legislators, http://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx; "A Look at How — and How Many — States Adopt Electronic Poll Books," Pew Charitable Trusts, http://www.pewtrusts.org/en/research-and-analysis/data-visualizations/2017/a-look-at-how-and-how-many-states-adopt-electronic-poll-books.

9 *See* Pam Fessler, "Russian Cyberattack Targeted Elections Vendor Tied to Voting Day Disruptions," *National Public Radio,* August 10, 2018, https://www.npr.org/2017/08/10/542634370/russian-cyberattack-targeted-elections-vendor-tied-to-voting-day-disruptions.

10 Ibid.

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

12 While Ohio has thorough provisional voting training materials, e-pollbook failure is not specified as a reason for issuing provisionals. *See* Jon Husted, "Provisional Voting Directive 2015-2018," in the *Ohio Election Official Manual*, December 15, 2015, 1-23, https://www.sos.state.oh.us/globalassets/elections/directives/2015/dir2015-28_eom-ch_06.pdf.

13 *See* Dana Chisnell and Maggie Ollove, "Provisional ballot suite," Center for Civic Design, https://www.elections.virginia.gov/Files/annualtraining/2018/Tuesday-EB/EB%2004-CCD_New%20provisional%20ballot%20suite.pdf.

14 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

15 *See* "The Verifier — Polling Place Equipment", Verified Voting, https://www.verifiedvoting.org/verifier; Lawrence Norden and Christopher Famighetti, *America's Voting Machines At Risk*, Brennan Center for Justice 2015, 30-31, https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf. This count of states does not include states that use DREs for accessible voting that supplements another type of machine or method of voting.

[16] *See* Danielle Root et al., *Election Security in All 50 States*, Center for American Progress, February 2018, 28, https://cdn.americanprogress.org/content/uploads/2018/02/21105338/020118_ElectionSecurity-report11.pdf#page=31. To be clear, Hawaii, Indiana and Tennessee require at least some "test[ing]" on some of their voting equipment. See, e.g. Haw. Admin. Code 3-176-6(b)(5) ("The official logic and accuracy test shall be performed on all computers to be used for elections.); Ind. Code Ann. § 3-11-14.5-1 (DRE voting system jurisdictions randomly select at least 3 percent to be tested); Tenn. Comp. R. & Regs. R. 1360-02-13-.14 (Officials in electronic voting machine counties select at least 1 percent of the precincts and have all machines used "prepared for a test election."). While Virginia does not statutorily require testing on all voting equipment, Va. Code § 24.2-653, the Department of Elections instructs election officials to perform testing on all voting equipment. The Handbook, June 1, 2018, available at https://www.elections.virginia.gov/GREBHandbook/Files/GREB%202018.pdf ("Each machine [not a sampling of machines] that will be used in an election must be tested prior to that election to ensure it has been programmed correctly and is functioning properly.").

[17] *See* "The Verifier — Polling Place Equipment", Verified Voting, https://www.verifiedvoting.org/verifier. We have identified the following states where there are no provisions that mandate paper ballots to be made available in the event of DRE failure: Delaware, Kansas, North Carolina, Nevada, Texas, Utah, Wyoming, West Virginia.

[18] Adam Pearce and Alexander Burns, "Energized Democrats Are Voting in Competitive Primaries in Droves," *New York Times*, June 25, 2018, https://www.nytimes.com/interactive/2018/06/25/us/politics/midterm-primaries-voter-turnout.html; Scott Clement, "Early Gauge of 2018 Turnout Shows Good Signs for Democrats," *Washington Post*, February 4, 2018, https://www.washingtonpost.com/news/the-fix/wp/2018/04/04/early-gauge-of-2018-turnout-shows-good-signs-for-democrats/?utm_term=.0ab15a156234; John Verhovek, "2018 Primaries See Democratic Turnout Surge, But GOP Shows Signs of Energy Too," *ABC News*, May 27, 2018, https://abcnews.go.com/Politics/2018-primaries-democratic-turnout-surge-gop-shows-signs/story?id=55439950.

[19] For example, during New York's recent 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.

[20] 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* "Voting Instructions for Voters with a Disability," State of Oregon, https://sos.oregon.gov/voting/Pages/instructions-disabilities.aspx.

[21] "Voter Information Project," Democracy Works, https://votinginfoproject.org/.

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

[23] Maria Bianchi (Director of VIP, Democracy Works) in discussion with Edgardo Cortés, July 15, 2018.

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

[25] Ibid.

[26] Sam Levine, "Hackers Tried To Breach A Tennessee County Server On Election Night: Report," *Huffington Post*, May 11, 2018, https://www.huffingtonpost.com/entry/knox-county-election-cyberattack_us_5af5ca21e4b032b10bfa56ee.

[27] Slobahan Gorman, Matt Chandler, Meredith D. Tavera and Chris Farley, *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.

Stay Connected to the Brennan Center

Visit our website at **www.brennancenter.org**.
Sign up for our electronic newsletters at **www.brennancenter.org/signup**.

Insider | Up-to-the-minute info on our work, publications, events, and more.

Justice Update | Snapshot of our justice work and latest developments in the field.

Money in Politics | Latest state and national developments and original analysis.

Redistricting Roundup | Analysis of current legal battles and legislative efforts.

Fair Courts | Comprehensive news roundup spotlighting judges and the courts.

Liberty & National Security | Updates on privacy, government oversight, and accountability.

Twitter | www.twitter.com/BrennanCenter
Facebook | www.facebook.com/BrennanCenter
Instagram | www.instagram.com/brennancenter

New and Forthcoming Brennan Center Publications

Purges: A Growing Threat to the Right to Vote
Jonathan Brater, Kevin Morris, Myrna Pérez, Christopher Deluzio

The State of Voting 2018
Wendy R. Weiser and Max Feldman

Liberty & National Security: An Election Agenda for Candidates, Activists, and Legislators
Faiza Patel, Elizabeth (Liza) Goitein, and Michael Price

Getting Foreign Funds Out of America's Elections
Ian Vandewalker and Lawrence Norden

Extreme Gerrymandering and the 2018 Midterm
Laura Royden, Michael Li, and Yurij Rudensky

Democracy & Justice: Collected Writings, vol. X
Brennan Center for Justice

The Fight to Vote
Michael Waldman

A Federal Agenda to Reduce Mass Incarceration
Ames Grawert, Natasha Camhi, and Inimai M. Chettiar

Extreme Vetting and the Muslim Ban
Harsha Panduranga, Faiza Patel, and Michael W. Price

For more information, please visit www.brennancenter.org.

BRENNAN CENTER FOR JUSTICE

at New York University School of Law

120 BROADWAY
17TH FLOOR
NEW YORK, NY 10271