alliance for securing democracy
G|M|F

# The Election Official's Handbook

## Six steps local officials can take to safeguard America's election systems

**David Levine,** Elections Integrity Fellow
February 13, 2020

## Protecting the 2020 Election

Intelligence and law enforcement agencies warn that Russia, China, Iran, and other foreign actors will seek to interfere in the 2020 presidential election.[1] Foreign actors are increasingly sophisticated at using cyber tools and social media to probe and penetrate electoral infrastructure, manipulate public opinion, and cast doubt on the integrity of the election process. On one hand, the United States is better prepared to address these threats now than during the 2016 presidential election. For example, after the Department of Homeland Security (DHS) designated election systems as critical infrastructure in 2017, it established the Elections Infrastructure Information Sharing and Analysis Center, which enabled states and localities to more easily share information about threats to elections. This mechanism has had the additional benefit of making DHS better at helping states manage risks, as well as distributing information from the federal government to the states about possible threats.[2]

On the other hand, in many states there are still vulnerabilities in election infrastructure that foreign actors can exploit. These vulnerabilities exist at almost every step of the election administration process, including registering voters, verifying their registration at polling places, securing the devices that capture and tally the vote, transmitting that data to a central location on election night, and executing an accurate recount.[3] While states usually make decisions about the rules of elections (policymaking),[4] localities are typically responsible for the "nuts and bolts" of running an election — such as finding polling places and recruiting poll workers.[5] Local election officials also help preserve the integrity of America's elections by protecting against hacks into voter rolls and local election websites and working closely with federal and state officials to ensure the security of their voting systems.[6]

As the February 3, 2020 Iowa Democratic caucuses demonstrated, such vulnerabilities are not merely theoretical. During the caucuses — which were administered by political party officials, not election officials — the new app that the Iowa Democratic Party planned to use to report its caucus results did not work. Many of the nearly 1,700

precinct chairs who were responsible for transmitting the results did not receive training on how to use the app, and a large number appear to have been unable to successfully download it.[7] Revisions and updates to the app were made as late as two days before the caucuses, making it nearly impossible to vet and test adequately.[8]

Although the federal government recently agreed to allocate an additional $425 million in election administration and security funds to state election offices,[9] federal resources will likely be insufficient to address all outstanding vulnerabilities before the 2020 presidential election. It is also unclear how much of this funding will be distributed to local elections officials in time for the 2020 presidential election. This handbook, therefore, provides a list of steps that local election officials can implement at relatively little cost to fortify their elections systems before the 2020 presidential election.

## 1. Add cyber expertise to your office

Having a chief information security officer (CISO) on staff can be critical to strengthening the security of local election infrastructure.[10] A CISO can help ensure that the development and implementation of policies, procedures, and training materials all support your office's information technology security needs, which all election offices have regardless of whether they've hired a CISO. Additionally, a CISO can help guarantee that appropriate information technology operational standards and controls are in place to ensure that all information technology assets managed by a local election office — such as electronic pollbooks, the voter registration system, the election management system, the election night website, and the voting system — are available, accurate, and secure. Finally, a CISO can help provide security briefings and statements on cybersecurity strategies, issues, and threats with counterparts across the national security apparatus, including local, state, and federal election officials, the Federal Bureau of Investigations (FBI), private industry, the media, law enforcement, and other stakeholders.

For jurisdictions that cannot afford to have a full-time CISO, they may be able to obtain cyber support from the state. For example, Illinois funds a cyber navigator program. Cyber navigators with responsibility for geographic zones across the state work with local election officials to conduct comprehensive risk assessments of each jurisdiction, including a review of the organization's security controls; analyze system and network documentation for accuracy; and provide guidance regarding software patches, system updates, email, and security software.[11] Multiple states have adopted similar programs, and more are expected to do so prior to the 2020 presidential election.

Counties could also consider forming consortiums with one another and negotiating an agreement with a CISO to split time between multiple counties. If neither of these options is possible, consider adopting a good neighbor policy, in which counties with more in-house expertise agree to help nearby jurisdictions.[12] Regardless of the arrangement, it is essential to have someone assisting the local election office who is familiar with the jurisdiction's infrastructure and internal strategies and has the relevant cybersecurity expertise to ensure that the office is sufficiently secure.

## 2. Form a local election cybersecurity working group

If they have not done so already, local election officials should strongly consider forming working groups with individuals outside of their office that include local law enforcement and emergency management personnel, as well as experts in cybersecurity and information technology, to complement efforts by federal and/or state officials to ensure that their election infrastructure is secure. When I previously served as the Ada County, Idaho, elections director, our office held regular meetings in the run up to an election with a similar group of individuals to flag any potential problems with administering the election and develop contingency processes to resolve them in case

they did arise.

The members of this group, collectively, could help election officials consider the whole election ecosystem. For example, they can help a locality determine whether it needs to deploy a malware detection system or other protective technologies and system reviews to improve their cybersecurity.[13] They can help ensure that local election officials are receiving up-to-date information and alerts about threats and vulnerabilities to their systems. And they can help guarantee that there are communicative relationships with all necessary stakeholders at the local level if those relationships don't already exist.

It is important that the local working groups complement, rather than duplicate, other efforts, including those by state and federal partners. A local working group will know its security environment better than outsiders and will be best positioned to appeal to state and federal partners for additional resources. For example, the Wisconsin Elections Commission has hired several additional informational technology staffers to examine the state's elections ecosystem, develop stronger security to prevent hacking of election systems, and provide additional security training to local election officials.[14] Since Wisconsin has more localities than any other state in the country and many of its local election officials are part-time employees,[15] the state's election cybersecurity efforts will likely be broader than in many other states. However, local Wisconsin election officials can still use local working groups to determine the baseline security improvements, technical support, training, and IT upgrades they need to make — and appeal to state IT officials for assistance — before the 2020 elections. DHS has also done a great deal to improve information sharing and raise cyber threat and incident awareness with state and local election officials.[16] However, DHS is highly unlikely to have the staffing and resources to provide tailored assistance to each and every local jurisdiction in the country ahead of the 2020 presidential election.[17] This is all the more reason for local election officials to form working groups, identify problems, and then appeal to state and federal entities for assistance as needed.

## 3. Secure the website

As of November 2019, many county election websites in at least four states — Florida,[18] Wisconsin,[19] Michigan,[20] and Texas[21] — were vulnerable to intrusion because their sites do not currently have HTTPS. HTTPS is a standard security protocol that makes it much harder for an adversary to hijack a website and provide false information about the election result, divert voters to phony sites that mimic the real ones, or steal voters' information. In states with close margins, such actions could swing an election or create broad doubts about the results.[22] One way any locality without HTTPS can take action to get an encrypted website is by visiting https://letsencrypt.org and applying for "https://".[23]

Most of the above county websites also do not have .gov Web addresses. This means that the federal government has not verified their authenticity and that voters cannot clearly tell whether the information on them is from an actual government agency. It appears to cost about $400 per year to have a .gov domain.[24] But the expense associated with securing your website is significantly cheaper than making more substantial election security upgrades, such as replacing outdated voting equipment.[25] Furthermore, having a .gov domain will lend the website legitimacy and credibility. Voters know it can be trusted because of its bureaucratic classification and official backing, and the branding can help the web user easily identify what you do. For example, a private company with the same name as your locality could have a .com website, but they could not have a .gov one. A .gov Web address will help ensure that people trust the information on a local election website. All localities that can should transition to a .gov Web address before the November 2020 presidential election.

These issues are not limited to the above states. A recent analysis found that just nine of the 99 counties in Iowa use

.gov addresses,[26] and a survey conducted on all county websites across 20 states before the 2018 midterm elections found a majority of them lacked both HTTPS and .gov protections.[27] Bad actors do not need to break into election systems to undermine confidence in our elections; rather, they could hack into the website that publishes the results of a vote and manipulate the results there.[28] It is critical that voters have trusted sources of information about the elections process and results, and having a secure website is a key means of ensuring a safe and fair election.

## 4. Mitigate the potential insider threat

While many conversations about election cybersecurity envision a hacker from a distant land breaching our election infrastructure through the Internet, an effective cyberattack could also be carried out by an insider.[29] According the Nucleus Cyber 2019 Insider Threat Report, at least 60 percent of organizations experience at least one insider attacker per year, which is particularly concerning since insiders often have elevated access privileges to sensitive data and applications.[30]

All current and prospective employees and vendors or contractors, permanent and temporary, who perform sensitive services for election localities should be required to undergo comprehensive background checks on an ongoing basis, preferably before each election. "Sensitive services" can be defined as those that (i) require access to customer/consumer/agency employee information; (ii) relate to the election computer networks, information systems, databases or secure facilities under circumstances that would permit modifications to such systems; or (iii) involve unsupervised access to secure facilities.[31] Ongoing screening ensures that employees remain suitable to access sensitive election-related information throughout their employment, before, during, and after each election.[32] They also help ensure the ongoing security of voting systems, including upgrades and changes.

These screenings should generally not include poll workers, unless a poll worker is also performing duties similar to a local election administrator. If there are concerns about whether such a policy would encompass poll workers, one idea is to limit their ability to access certain election data, so that they are generally not performing "sensitive services."

Vendors and contractors should also be required to perform and pay for background check services for their employees and submit the results of those tests to local election officials. They should also be required to describe how they screen prospective employees for security risks and to assess them on a periodic basis.[33] Vendors and contractors, not election officials, are the ones who build and maintain much of the country's election infrastructure,[34] and they need to be assessed for security risks just like election officials.[35] Since vendors are subject to little federal oversight, local election officials should ensure vendor compliance with personnel background check policies during the procurement process and require ongoing compliance in the final contract.

## 5. Work with state officials to protect the voter registration process

Following the 2016 presidential election, the U.S. Senate Select Committee on Intelligence found that voter registration databases were not as secure as they could have been,[36] and that in at least one state, Russian-affiliated cyber actors breached databases and could have altered or deleted voter registration data.[37] In its 2018 report "Securing the Vote: Protecting American Democracy," the National Academy of Sciences recommended that election administrators regularly review the integrity of their voter registration databases and the integrity of these databases connected to other applications. For example, the databases containing voter registration lists are often connected

directly or indirectly to the Internet or state computer networks. This connectivity raises concerns about unauthorized access to or manipulation of the registrant list or disruption of the registration system. For example, in Illinois, Russian actors targeted and breached an online voter database in 2016 by exploiting a coding error.[38] For three weeks, they maintained undetected access to the system and ultimately obtained personal information on more than 90,000 voters.[39]

One way election administrators can identify potential hacking or tampering in a voter database is to use a secure web application that deploys statistics, machine learning, and data visualization to analyze changes in the database and flag unusual activity.[40] In Iowa, for example, the Secretary of State's office uploads its voters data to a free, secure web application on a weekly basis, and the application organizes and presents the data with trend lines, demographics, and anomalies. Election officials can then review anything that seems out of the ordinary.[41] This application is currently in use in at least 14 states.[42]

Such an application could prevent a scenario in which voters are disenfranchised because of long lines or if provisional ballots are not available for voters when their name or other information does not match what is on file. Periodically analyzing voter registration data will better enable officials to uncover successful efforts to tamper with the voter registration data or technical errors or failures. For example, if there is a spike in voter registrations, officials should be able to explain the cause of the spike. Did a similar spike occur in similar previous elections? Is there is an impending voter registration deadline? Are outside organizations conducting large registration drives? Election officials should promptly conduct a more thorough analysis if the cause is not apparent.[43]

Another way to mitigate this threat is to work with your state, if necessary, to allow any voter who insists that they are registered in the jurisdiction to be able to cast a provisional ballot, even if some or all of their information is not in the poll book. This is not currently the case in all localities.[44] In the past, it was largely assumed that if a voter's information was not accurate in the poll book, it was because either the voter or the elections office erred. As a result of the successful breach of the Illinois' voter registration database by foreign adversaries before the 2016 election, we now know that the voter file used on Election Day could also contain inaccurate information due to hacking. Allowing a voter to vote by a provisional ballot in these circumstances allows the experts — local election officials — time to further investigate these ballots following Election Day and determine whether these votes should in fact count.

For states that require voters to re-register if their personal information does not match what is in the poll book, they should allow these voters to cast a provisional ballot if voters are not able to successfully re-register on Election Day. This will help ensure that an alteration of a voter's information through no fault of the voter or the elections office does not have the effect of disenfranchising that vote. Otherwise, confidence in those elections could be undermined, and/or it could become the target of disinformation efforts.

## 6. Test changes to election infrastructure in lower-risk settings

The recent Iowa Democratic Caucuses are the latest reminder that when localities adopt significant changes to election infrastructure, there should be simulations of threats during a mock election to test new policies, procedures, and equipment. These include changes to voter registration databases and associated information technology (IT) systems; IT infrastructure and systems used to manage elections (such as the counting, auditing, and displaying of election results, and post-election reporting to certify and validate results); voting systems and associated infrastructure; storage facilities for election and voting system infrastructure; and polling places, including

early voting locations.[45] In 2010, the Washington, D.C. Board of Elections developed a procedure to allow overseas absentee voters to cast their ballots using a website and held a mock election during which anyone was invited to test the system or compromise its security. Within 48 hours of the system going live, a team from the University of Michigan had successfully changed every vote and revealed almost every secret ballot, prompting the DCBOE to discontinue its plans to deploy digital ballot return.[46]

Any mock election should try to simulate Election Day as much as possible to determine which systems and processes work well, and white-hat security researchers should be invited to try to attack the election systems to evaluate their security and usability. If localities do not have adequate budgets to fund these elections themselves, they should look to partner with their vendors, local civic engagement groups, and/or local universities to make up the difference. Mock elections can also help with voter education and election research efforts, in addition to testing infrastructure.

Another way to test election infrastructure against potential threats is through tabletop exercises. Such exercises are discussion-based sessions where team members meet in an informal, classroom setting to discuss their roles during an emergency and their responses to different situations. An increasing number of election officials are gaming how adversaries could disrupt the 2020 election. For example, in September of 2019, New Jersey election officials from the state's 21 counties conducted tabletop exercises with state and federal authorities to determine how to respond if bad actors shut down voter registration databases, input incorrect information into voter files, or compromised social media accounts so that they started spreading inaccurate information about polling locations. They also reviewed what to do if adversaries use ransomware to lock election computers or shut down cellphone towers.[47] Conducting these exercises helps election officials hone their defenses against cyber threats and information operations designed to undermine public confidence in the electoral process more broadly.

A third way to assess changes to election infrastructure is to conduct pilot projects of new systems and processes. In elections, pilot projects are often rolled out during smaller elections with an anticipated lower turnout in order to assess how they would perform. For example, election officials in Pennsylvania, Michigan, Missouri, Virginia, Ohio, and Georgia,[48] have recently conducted risk-limiting audit (RLA) pilot projects following smaller elections to assess whether they can be deployed more regularly, including after the 2020 presidential election. Since an RLA provides strong statistical evidence that the election outcome is right and has a high probability of correcting an incorrect outcome, using it on a more regular basis likely hinges on how well a local jurisdiction can implement

# Conclusion

The U.S. national security and intelligence communities have stated that foreign actors will target our election infrastructure in 2020, just as they did during the 2016 presidential election and the 2018 midterm elections. It is critical that local election officials have the necessary personnel, tools, and infrastructure to repel attacks from increasingly sophisticated adversaries. Implementing the measures recommended in this handbook will improve local resilience to cyber threats ahead of November 2020.

# Acknowledgements

The author would like to recognize the following individuals and organizations for their invaluable feedback and support. The author also consulted publications by many of the individuals listed below, which were invaluable resources in developing the Election Official's Handbook. The contents of this report reflect exclusively the views of the author.

**Tonya Rice,** Amazon Web Services
**Matthew Weil,** Bipartisan Policy Center
**Edgardo Cortes,** Brennan Center for Justice
**Elizabeth Howard,** Brennan Center for Justice
**Maurice Turner,** Center for Democracy & Technology
**David Becker,** Center for Election Innovation & Research
**Ben Spear,** Center for Internet Security
**David Bjerke,** City of Falls Church, Virginia
**Stacey Scholl,** The Gober Group
**Barb Byrum,** Ingraham County, Michigan
**Grace Wachlarowicz,** Minneapolis, Minnesota
**Alysoun McLaughlin,** Montgomery County, Maryland
**Steven Daitch,** Ottawa County, Michigan
**Joshua M. Franklin,** OutStack Technologies
**Tom Connolly,** State of New York
**Steve Spaulding,** U.S. House Committee on House Administration
**Marian Schneider,** Verified Voting

# Endnotes

1. U.S. Department of Justice, U.S. Department of Defense, U.S. Department of Homeland Security, U.S. Department of National Intelligence, Federal Bureau of Investigation, National Security Agency, Cybersecurity and Infrastructure Security Agency, Ensuring Security of 2020 Elections, November 05, 2019, https://www.dni.gov/index.php/newsroom/press-releases/item/2063-joint-statement-from-doj-dod-dhs-dni-fbi-nsa-and-cisa-on-ensuring-security-of-2020-elections.
2. Gabriela Martinez. "How the U.S. is trying to improve election security ahead of 2020," *PBS News Hour,* July 26, 2019, https://www.pbs.org/newshour/politics/how-the-u-s-is-trying-to-improve-election-security-ahead-of-2020.
3. Elaine Kamarck. "States and localities are on the front lines of fighting cyber-crime in elections," Brookings Institution, August 15, 2019, https://www.brookings.edu/blog/fixgov/2019/08/15/states-and-localities-are-on-the-front-lines-of-election-security/.
4. U.S. Library of Congress, Congressional Research Service, The State and Local Role in Election Administration: Duties and Structures, by Karen L. Shanton, R45549 (2019).
5. "Election Administration at State and Local Levels," National Conference of State Legislatures, February 03, 2020, https://www.ncsl.org/research/elections-and-campaigns/election-administration-at-state-and-local-levels.aspx. Elections are often administered at the county level, but sometimes at the city and town level, particularly in certain New England and Midwestern states.
6. Doug Chapin. "NACo Letter To Congress Makes Case For Increased, Dedicate Local Election Funding," Election Academy, December 13, 2019, https://editions.lib.umn.edu/electionacademy/2019/12/13/naco-letter-to-congress-makes-case-for-increased-dedicated-local-election-funding/.
7. Shane Goldmacher and Nick Corasaniti. "'A Systemwide Disaster': How the Iowa Caucuses Melted Down," *The New York Times,* February 04, 2020, https://www.nytimes.com/2020/02/04/us/politics/what-happened-iowa-caucuses.html.
8. Jason Koebler and Emanuel Maiberg. "Here's the Shadow Inc. App That Failed in Iowa Last Night," *Vice*, February 04, 2020, https://www.vice.com/en_us/article/y3m33x/heres-the-shadow-inc-app-that-failed-in-iowa-last-night.
9. U.S. Election Assistance Commission, EAC Commissioners Welcome Deal to Make Available $425 Million in New Help America Vote Act Funds for Elections, by Kristen Muthig, Press Release (Silver Springs, Maryland, 2019), https://www.eac.gov/eac-commissioners-welcome-deal-to-make-available-425-million-in-new-help-america-vote-act-funds-for-elections.
10. Steve Morgan. "2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics" *Cybercrime Magazine*, February 06, 2019, https://cybersecurityventures.com/cybersecurity-almanac-2019/.To strengthen their security infrastructure and practices, protect their data, and manage and respond to cyber threats, it is expected that nearly 100 percent of large corporations (Fortune 500, Global 2000) globally will have a chief information security officer or equivalent position by 2021.
11. Christopher R. Deluzio, Liz Howard, Paul Rosenzweig, David Salvo, Rachael Dean Wilson. "Defend Elections: Federal Funding Needs for State Election Security," Brennan Center for Justice, July 18, 2019, https://securingdemocracy.gmfus.org/wp-content/uploads/2019/07/2019_07_DefendingElections_Final.pdf.
12. Andrew Westrope. "Cybersecurity and Democracy Collide: Looking for Down Elections," *Governing*, October 08, 2019, https://www.governing.com/news/headlines/GT-Cybersecurity-and-Democracy-Collide-Locking-Down-Elections.html.
13. Ibid.
14. Bill Theobald. "The 13 states where election security matters most," *The Fulcrum*, December 05, 2019, https://thefulcrum.us/election-security-battleground-states?rebelltitem=13#rebelltitem13.

15. Wisconsin Elections Commission. Wisconsin Remains among Top States in Elections, April 07, 2014, https://elections.wi.gov/node/3153.
16. U.S. Department of Homeland Security, Office of Inspector General, Progress Made, But Additional Efforts Are Needed to Secure the Election Infrastructure (Washington, DC, 2019), 19, https://www.oig.dhs.gov/sites/default/files/assets/2019-03/OIG-19-24-Feb19.pdf.
17. U.S. Government Accountability Office, Report to Congressional Committees, Election Security: DHS Plans Are Urgently Needed to Address Identified Challenges Before the 2020 Elections (Washington, DC, 2020), https://www.gao.gov/assets/710/704314.pdf.
18. Joseph Marks. "The Cybersecurity 202: Swing state election websites aren't secure against Russian hacking, McAfee says," *The Washington Post,* November 08, 2019, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/11/08/the-cybersecurity-202-swing-state-election-websites-aren-t-secure-against-russian-hacking-mcafee-says/5dc45ee4602ff1184c31635c/.
19. Ibid.
20. Ibid.
21. Grace Chimene. "League of Women Voters of Texas Finds only 20% of Texas Counties Following Website Security Best Practice!," League of Women Voters of Texas, November, 2019, https://my.lwv.org/texas/article/league-women-voters-texas-finds-only-20-texas-counties-following-website-security-best.
22. Marks, "The Cybersecurity 202: Swing state election websites aren't secure against Russian hacking, McAfee says."
23. Chimene, "League of Women Voters of Texas Finds only 20% of Texas Counties Following Website Security Best Practice!"
24. Miles Parks. "1 Simple Step Could Help Election Security. Governments Aren't Doing it," *NPR*, January 29, 2020, https://www.npr.org/2020/01/29/800131854/1-simple-step-could-help-election-security-governments-arent-doing-it.
25. Marks, "The Cybersecurity 202: Swing state election websites aren't secure against Russian hacking, McAfee says."
26. Miles Parks. "1 Simple Step Could Help Election Security. Governments Aren't Doing it," *NPR*, January 29, 2020, https://www.npr.org/2020/01/29/800131854/1-simple-step-could-help-election-security-governments-arent-doing-it.
27. Marks, "The Cybersecurity 202: Swing state election websites aren't secure against Russian hacking, McAfee says."
28. Mary Ellen Klas. "Website hack could be as bad as vote attack, warns Florida officials," *Tampa Bay Times*, December 04, 2019, https://www.tampabay.com/florida-politics/buzz/2019/12/04/web-site-hack-could-be-as-bad-as-vote-attack-warns-florida-officials/.
29. Lawrence Norden, Gowri Ramachandran, and Christopher Deluzio. "A Framework for Election Vendor Oversight," Brennan Center for Justice, November 12, 2019, https://www.brennancenter.org/our-work/policy-solutions/framework-election-vendor-oversight.
30. Cybersecurity Insiders, Insider Threat Report, 2019, https://nucleuscyber.com/wp-content/uploads/2019/07/2019_Insider-Threat-Report_Nucleus_Final.pdf.
31. The Office of the Ohio Secretary of State, Directive 2019-08, June 11, 2019, 5-6, https://www.ohiosos.gov/globalassets/elections/directives/2019/dir2019-08.pdf.
32. Matthew Burns. "Durham elections worker pleads guilty to altering vote counts in 2016 primary," *WRAL*, January 10, 2018, https://www.wral.com/durham-elections-worker-pleads-guilty-to-altering-vote-counts-in-2016-primary/17247689/; Matthew Burns, "Worker charged with trying to clear felons for voting in Granville," *WRAL*, April 5, 2017, https://www.wral.com/worker-charged-with-trying-to-clear-felons-for-voting-in-granville/16628503/.
33. Norden, Ramachandran, and Deluzio, "A Framework for Election Vendor Oversight."

34. Ibid.
35. The Blue Ribbon Commission on Pennsylvania's Election Security, Study and Recommendations, January, 2019, https://www.cyber.pitt.edu/sites/default/files/FINAL%20FULL%20PittCyber_PAs_Election_Security_Report_0.pdf.
36. U.S. Congress, Senate, Select Committee on Intelligence, Russian Active Measures Campaigns and Interference in the 106 U.S. Election, Volume 1: Russian Efforts Against Election Infrastructure with Additional Views, 116th Cong., 1st sess., 2019, 4, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.
37. Ibid, 22.
38. Brad Edwards. "Russian Hack into Illinois Election Database Was Worse Than Thought," *CBS Chicago*, June 13, 2017, http://chicago.cbslocal.com/2017/06/13/ russian-hack-into-illinois-election-database-worse-than-thought/; "Illinois Elections Board Offers More Information on Hacking Incident," *WSIU*, May 4, 2017, http://news.wsiu.org/post/illinois-elections-board-offers-more-information-hacking-incident#stream/0; and Joe Uchill. "Illinois Voting Records Hack Didn't Target Specific Records, Says IT Staff," *The Hill*, May 4, 2017, http://thehill.com/policy/cybersecurity/331981-ill-votingrecords-hack-didnt-target-specific-records-says-state-it.
39. "Illinois Elections Board Offers More Information on Hacking Incident."
40. One example of this is an app called VoteShield, which is described at https://www.govtech.com/security/Nonprofits-Free-App-Flags-Suspicious-Changes-to-Voter-Rolls.html. The app was developed with feedback and guidance from election administrators, including Iowa's.
41. Ibid.
42. Ibid.
43. Ibid.
44. "Provisional Ballots," National Conference of State Legislatures, October 15, 2018, https://www.ncsl.org/research/elections-and-campaigns/provisional-ballots.aspx.
45. U.S. Department of Homeland Security, Election Security, December 17, 2019, https://www.dhs.gov/topic/election-security.
46. Scott Wolchok, Eric Wustriw, Dawn Isabel, and J. Alex Halderman. "Attacking the Washington, D.C. Internet Voting System," Proc. 16th Intl. Conference on Financial Cryptography and Data Security (February, 2012), https://jhalderm.com/pub/papers/dcvoting-fc12.pdf.
47. Joseph Marks. "Cybersecurity 202: How counties are war-gaming Election Day cyberattacks," *The Washington Post*, September 11, 2019, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/09/11/the-cybersecurity-202-how-counties-are-war-gaming-election-day-cyberattacks/5d78307a88e0fa7bb93a8a8f/.
48. GCN Staff. "CISA partners on risk-limiting audit software for election systems," GCN, November 22, 2019, https://gcn.com/articles/2019/11/22/arlo-risk-limiting-audit-software.aspx.