Center for American Progress

KATHERINE FREY/GETTY IMAGES

Election Security in All 50 States

Defending America's Elections

By Danielle Root, Liz Kennedy, Michael Sozan, and Jerry Parshall February 2018

Center for American Progress

Election Security in All 50 States

Defending America's Elections

By Danielle Root, Liz Kennedy, Michael Sozan, and Jerry Parshall February 2018

Contents

Introduction and summary

In 2016, America's elections were targeted by a foreign nation-state intent on infiltrating and manipulating our electoral system. On September 22, 2017, it was reported that the U.S. Department of Homeland Security (DHS) notified 21 states that they were targeted by hackers during the 2016 election. Among those states notified by DHS were: Alabama, Alaska, Colorado, Connecticut, Delaware, Florida, Illinois, Maryland, Minnesota, Ohio, Oklahoma, Oregon, North Dakota, Pennsylvania, Virginia, and Washington.[2] Arizona, California, Iowa, Texas, and Wisconsin were also among those states originally contacted by DHS. However, those states have denied that their election systems were attacked.[3] Ultimately, hackers only reportedly succeeded in breaching the voter registration system of one state: Illinois.[4] And while DHS did not name those responsible for the attempted hacks, many believe the culprits can be traced back to Russia.[5] Experts have warned that a future attack on our election infrastructure, by Russia or other malicious actors, is all but guaranteed.[6]

By now, the American people have been alerted to many vulnerabilities in the country's election systems, including the relative ease of voting machine hacking,[7] threats to voter registration systems and voter privacy,[8] and disinformation campaigns waged by foreign nation-states aimed at confusing voters and inciting conflict.[9] If left unaddressed, these vulnerabilities threaten to undermine the stability of our democratic system.

Free and fair elections are a central pillar of our democracy. Through them, Americans make choices about the country's future—what policies will be enacted and who will represent their interests in the states, Congress, and beyond. The right of Americans to choose their own political destiny is in danger of being overtaken by foreign nation-states bent on shifting the balance of power in their favor and undermining American's confidence in election results. In our democracy, every vote counts, as evidenced by the race for Virginia's House of Delegate's

94th District, which was decided by lottery after being tied.[10] That contest illustrates the inherent worth and power behind each vote as well as the necessity of protecting elections from tampering on even the smallest scale.[11] Every vote must count, and every vote must be counted as cast.

Election security is not a partisan issue. As aptly noted by the chairman of the U.S. Senate Select Committee on Intelligence, Sen. Richard Burr (R-NC), "Russian activities during the 2016 election may have been aimed at one party's candidate, but … in 2018 and 2020, it could be aimed at anyone, at home or abroad."[12] Failing to address existing vulnerabilities and prepare for future attacks puts the nation's security at risk and is an affront to the rights and freedoms at the core of American democracy. Already, we are running out of time to prepare for the 2018 elections, while the 2020 presidential election is looming.[13] Another attack on our elections by nation-states such as Russia is fast approaching.[14] Leaders at every level must take immediate steps to secure elections by investing in election infrastructure and protocols that help prevent hacking and machine malfunction. In doing so, the United States will be well positioned to outsmart those seeking to undermine American elections and to protect the integrity of every vote.

To understand risks to our election systems and plan for the future, it is necessary to identify existing vulnerabilities in election infrastructure so we can properly assess where resources should be allocated and establish preventative measures and strategies. Only through understanding the terrain can the nation rise to the challenge of preventing voting machine malfunction and defending America's elections from adversarial attempts to undermine our election infrastructure.

In August 2017, the Center for American Progress released a report entitled "9 Solutions for Securing America's Elections," laying out nine vulnerabilities in election infrastructure and solutions to help improve election security in time for the 2018 and 2020 elections.[15] This report builds on that analysis to provide an overview of election security and preparedness in each state, looking specifically at state requirements and practices related to:

1. Minimum cybersecurity standards for voter registration systems
2. Voter-verified paper ballots
3. Post-election audits that test election results
4. Ballot accounting and reconciliation
5. Return of voted paper absentee ballots
6. Voting machine certification requirements
7. Pre-election logic and accuracy testing

This report provides an overview of state compliance with baseline standards to protect their elections from hacking and machine malfunction. Some experts may contend that additional standards, beyond those mentioned here, should be required of states to improve election security. The chief purpose of this report is to provide information on how states are faring in meeting even the minimum standards necessary to help secure their elections.

It is important to note at the outset that this report is not meant to be comprehensive of all practices that touch on issues of election security. We recognize that local jurisdictions sometimes have different or supplemental requirements and procedures from those required by the state. However, this report only considers state requirements reflected in statutes and regulations and does not include the more granular—and voluminous—information on more localized practices. Furthermore, this report does not address specific information technology (IT) requirements for voting machine hardware, software, or the design of pre-election testing ballots and system programming. And while we consider some minimum cybersecurity best practices, we do not analyze specific cyberinfrastructure or system programming requirements. These technical standards and protocols deserve analysis by computer scientists and IT professionals[16] who have the necessary expertise to adequately assess the sufficiency of state requirements in those specialized areas.[17]

This report is not an indictment of state and local election officials. Indeed, many of the procedures and requirements considered and contained within this report are created by statute and under the purview of state legislators rather than election officials. Election officials are tasked with protecting our elections, are the first to respond to problems on Election Day, and work diligently to defend the security of elections with the resources available to them. Unfortunately, funding, personnel, and technological constraints limit what they have been able to do related to election security. We hope that by identifying potential threats to existing state law and practice, this report helps lead to the allocation of much needed funding and resources to election officials and systems in the states and at the local level.

The U.S. Constitution grants states the authority to administer elections.[18] And although members of Congress may not have a direct hand in the processes and procedures for carrying out elections, they still have a role to play by ensuring elections are properly and adequately funded. Nearly three-quarters of states are estimated to have less than 10 percent of funding remaining from the Help America Vote Act, which allocated nearly $4 billion in 2002 to help states with elections.[19] According to a 2017 report, 21 states support receiving more funding from the federal government to help secure elections.[20]

All 50 states have taken at least some steps to provide security in their election administration. In recent examples:

- Virginia overhauled its paperless direct recording electronic voting machines and switched to a statewide paper ballot voting system just weeks before the 2017 elections.

- In 2017, Colorado became the first state to carry out mandatory risk-limiting post-election audits.

- In 2017, Rhode Island passed a bill requiring risk-limiting post-election audits for future elections.

- A new election vendor contract in Alabama requires election officials with access to the state's voter registration system to undergo cybersecurity training prior to elections.

- In December 2017, New York Gov. Andrew Cuomo (D) announced a new election security initiative as part of his 2018 State of the State agenda, including creating a state Election Support Center, developing an Elections Cyber Security Support Toolkit, and providing Cyber Risk Vulnerability Assessments and Support for Local Boards of Elections, among other things.

- At least 36 states are coordinating with or have already enlisted some help from DHS and/or the National Guard in assessing and identifying potential threats to voter registration systems.

Additionally, states such as Delaware and Louisiana are considering replacing their paperless voting systems with technology that produces voter verified paper ballots, and Indiana is considering implementing risk-limiting post-election audits for the 2018 elections. Florida Gov. Rick Scott (R) has requested millions of dollars in funding aimed at protecting election systems and software from attack. And on February 9, Gov. Tom Wolf's (D) administration in Pennsylvania—which still uses paperless voting machines in some jurisdictions—ordered counties looking to replace voting systems to purchase machines with paper records.

No state received an A; 11 states received a B; 23 states received a C; 12 states received a D; and five states received an F.

The main takeaway from the Center for American Progress' research and analysis is that all states have room for improvement:

- Fourteen states use paperless DRE machines in at least some jurisdictions. Five states rely exclusively on paperless DRE machines for voting.

- Thirty-three states have post-election audit procedures that are unsatisfactory from an election security standpoint, due either to the state's use of paperless DRE machines, which cannot be adequately audited, or other factors. At least 18 states do not legally require post-election audits or require jurisdictions to meet certain criteria before audits may be carried out.

- Thirty-two states allow regular absentee voters and/or U.S. citizens and service members living or stationed abroad to return voted ballots electronically, a practice deemed insecure by election and cybersecurity experts.

- At least 10 states do not provide cybersecurity training to election officials.

This point cannot be overemphasized: Even states that received a B or a C have significant vulnerabilities that leave them susceptible to hacking and infiltration by sophisticated nation-states. However, by making meaningful changes to how elections are carried out, states can improve their overall election security while supporting public confidence in election procedures and outcomes.

Glossary

Ballot tabulating equipment: Optical or digital electronic machines that count or tabulate paper ballots.[21] While some jurisdictions have ballot-tabulating equipment at each polling place, others use a single central tabulator that tabulates ballots delivered from every polling place within that jurisdiction.[22]

Direct recording electronic voting machine (DRE machine): An electronic voting machine that a voter uses to cast a vote.[23] The voter makes a selection using the machine's touch-screen or manual dial. The selection is then stored on the machine's memory drive.[24] Throughout the day on Election Day, the machine electronically stores and tabulates each vote cast on that machine. Machine totals are then aggregated to determine election results.[25]

Election certification: The official declaration of election results. On election night, states and localities usually announce only preliminary vote tallies. Election results often are not made official until days or weeks after Election Day when vote counts are certified.[26] This typically involves sending an official letter of certification to the winner of each ballot contest.[27]

Electronic poll books: Electronic copies of voter registration lists—typically housed on a laptop computer or electronic tablet—that poll workers use to check in voters during early voting and on Election Day, as opposed to relying on traditional paper voter registration lists.[28] Electronic poll books have been found to facilitate voter participation by streamlining the voter check-in process and reducing wait times at polling locations.[29]

Post-election audit: A review process taking place after an election that establishes evidence that the outcome is correct by manually sampling enough ballots to ensure that if the outcome is wrong—for any reason whatsoever—the audit has a high probability of detecting the problem and correcting an erroneous outcome. Some states claim that a rescanning of ballots counts as a proper post-election audit. However, this type of audit cannot verify that the outcome is correct

because its primary purpose is to test the functionality of tabulating equipment rather than the accuracy of election outcomes. Auditing other aspects of the election process or voting machines is important but is no substitute for verifying election results by manually auditing the tabulated results. Some states conduct post-election audits after an initial ballot count but before certification. Other states conduct post-election audits after certification. Mandatory post-election audits differ from recounts in that they are automatically conducted regardless of whether a candidate or party petitions for a review process.[30]

Pre-election logic and accuracy testing: A test conducted on voting machines to examine whether they will function properly and accurately count votes during voting periods.[31] Testing usually includes the actual voting machines as well as any ballot counting software and memory cards.[32] Most states conduct some form of logic and accuracy testing during the days and weeks leading up to an election.[33] In some states all electronic machines that will be used in an election are tested, while in other states only a small sample of machines undergo testing. Importantly, pre-election logic and accuracy testing is not guaranteed to detect hackers or prevent hacking on Election Day. However, pre-election logic and accuracy testing is one preventative measure that election officials can take to protect against potential machine malfunction on Election Day.

Risk-limiting audit: A type of post-election audit. A risk-limiting audit is a procedure that has a large, prespecified chance of correcting the election outcome if the outcome is wrong—no matter why it is wrong. "Wrong" means that a full hand count of the validly cast votes would show different winner(s). A risk-limiting audit requires a trustworthy paper trail, which are not produced by way of paperless DRE machines.

Importantly, a risk-limiting audit has a high probability of correcting a wrong outcome.[34] Specifically, it is a manual inspection and determination of voter intent, which may include a hand counting of randomly selected ballots that stops as soon as it is implausible that a full recount would alter the reported results. Risk-limiting audits demand that close races deserve more scrutiny. If the margin of victory is very close, a risk-limiting audit requires examining a larger sample of ballots. If the margin of victory is wide, generally fewer ballots need to be reviewed to ensure with high confidence that the outcome is correct—if it is correct. The risk limit is the largest chance that an incorrect outcome escapes correction. Example: If the risk limit is 5 percent and the outcome is wrong, the audit has at least a 95 percent chance of requiring a full hand count, which would correct the outcome.

Importantly, just because an audit is called "risk-limiting" does not mean that it is a risk-limiting audit in the true sense. In addition to testing the accuracy of election outcomes and correcting them if they are wrong, risk-limiting audits can play an important role in identifying and investigating potential problems in voting system performance.[35] For more information on risk-limiting audits, read "A Gentle Introduction to Risk-limiting Audits," by Mark Lindeman and Philip B. Stark.[36]

Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA): A federal law enacted in 1986 to facilitate absentee voting among military personnel and their families, along with U.S. citizens living or stationed overseas.[37] The act, which was expanded in 2009 by the Military and Overseas Voter Empowerment Act, authorizes the electronic transmission of blank ballots from the states to UOCAVA voters.[38] However, some states go further by also allowing UOCAVA voters to return completed ballots electronically, via email, fax, or web portal.

U.S. Election Assistance Commission (EAC): The federal agency responsible for providing recommendations and guidance for the administration of federal elections.[39] The EAC, created by Congress via the Help America Vote Act of 2002, is tasked with setting Voluntary Voting System Guidelines—including basic security, functionality, and accessibility standards—for voting machines.[40] The EAC is also called upon to certify, decertify, and recertify voting machines so that states can use machines that adhere to federally established standards and provides guidance on cybersecurity measures for protecting voter registration systems and other election infrastructure.[41]

U.S. Election Assistance Commission certification: Voting machine vendors may apply to have their voting machines certified by the EAC, meaning that the vendor's voting machine receives the EAC's official stamp of approval signifying that the machine meets the federal Voluntary Voting System Guidelines.[42] As of March 2017, the EAC had certified 38 voting systems or voting system modifications.[43] Once certified, the name of the voting system model and its vendor is posted on the EAC's website so that states can check to see whether a voting system they plan to purchase is EAC-certified.[44] States are not required to purchase and use voting systems certified by the EAC.[45]

Voluntary Voting System Guidelines: The set of standards, established by the EAC, against which voting systems may be tested.[46] The standards are voluntary and include baseline hardware and software requirements—including those related to functionality, security capabilities, usability, and accessibility—that the EAC

recommends for all voting machines.[47] Most states require some level of adherence to these federal guidelines.[48] For example, as described by the Brennan Center for Justice: "Some states contract out to the ITAs [Independent Testing Authorities] to test to these additional standards, some states have their own testing labs, some states hire consultants, and some states have boards of examiners that determine if state requirements are met."[49] The EAC anticipates finalizing a new set of voting system guidelines in 2018, which will take into account advances in technology and emphasizes auditable voting systems and evidence-based elections.[50]

Vote canvassing: The process before certification where votes are tallied and aggregated to determine official election results.[51]

Vote center: A centrally located voting station where eligible voters, residing anywhere within a jurisdiction, may come to vote. Vote centers are an alternative to traditional precinct polling places.[52] Vote centers are beneficial for voters who have trouble finding information on their designated polling place and for local election administrators who have difficulty staffing or providing voting equipment for multiple polling locations within their jurisdictions. Some states employ vote centers only during early voting periods or on Election Day.[53] Other states employ vote centers during and throughout all voting periods.[54]

Voter-verified paper audit trail (VVPAT): A permanent paper record of a voter's ballot selections that can be used to conduct post-election audits and recounts to confirm the accuracy of reported election outcomes. Examples include paper ballots or paper records produced by DRE machines with voter-verifiable paper record (VVPR) components.[55] With such a DRE machine, voters use the touch-screen or manual dial to select the candidates of their choosing. Before committing a vote to the machine's memory drive, the machine prints a paper record of the selection, which the voter can view under a transparent viewing screen. This gives voters the opportunity to review and verify the accuracy of their votes before casting them.[56] Once verified, the paper record is preserved and can be referred to by election officials in conducting post-election audits or recounts.[57]

Voting system test laboratories: Independent, nonfederal laboratories that are accredited by the Election Assistance Commission and tasked with testing voting machines to ensure that they comply with EAC's Voluntary Voting System Guidelines.[58] It is within a state's discretion whether to have its voting machines tested by a federally accredited voting system test laboratory.[59] Most of these laboratories are recommended and evaluated by the National Institute of Standards and Technology prior to receiving EAC accreditation.[60]

Factors and methodology

The election security factors considered in this report were selected based on their ability to evaluate election security and preparedness at the state level. They are:

1. Minimum cybersecurity standards for voter registration systems
2. Voter-verified paper audit trail
3. Post-election audits that test election results
4. Ballot accounting and reconciliation
5. Return of voted paper absentee ballots
6. Voting machine certification requirements
7. Pre-election logic and accuracy testing

The information included in this report is derived primarily from state statutes and regulations, as well as interviews with state and local election officials. A debt of gratitude is owed to several organizations for the work they've conducted on the seven categories considered in this report, including the Brennan Center for Justice, Common Cause, Verified Voting, the Pew Charitable Trusts, and the National Conference of State Legislators. We also drew from information supplied by the U.S. Election Assistance Commission.

As part of our research, we reached out to the offices of the top election official in all 50 states plus the District of Columbia, requesting phone interviews to verify research and provide election officials the opportunity to expand on state requirements. In addition to requesting phone conversations, we sent state election offices a survey covering our areas of interest, which we invited them to complete in the event that they were unable to speak over the phone. The authors requested a follow up phone interview with any state that opted to fill out the survey. Finally, each state was given the opportunity to review and comment on our assessments prior to the publication of this report.

For grading each state's level of election security preparedness, we awarded points based on a state's adherence to a set of best practices included within each category. Each of the seven categories was graded on either a 1-point or 3-point scale

so that the highest total score a state could receive was 13 points. In four categories, if a state adheres to all the best practices included within a category it received a "fair" score, and 1 point for that category. If the state adheres to some standards, but not others, it received a score of 0, or "unsatisfactory."

Three key categories were graded on a 3-point scale, those being voter-verified paper audit trail, post-election audits, and minimum cybersecurity standards for voter registration systems. The 3-point scale was assigned to categories that, if implemented correctly, are found to greatly improve election security and where the standards were numerous, so it made sense to supplement the category with the opportunities to earn additional points.

The point distribution varies slightly for these three categories. For example, states that carry out elections through the exclusive use of paper ballots received 3 points, or a "good" score, for that category. States that use VVPR-producing DRE machines statewide or in combination with paper ballots and/or ballot marking devices received a "fair" score. While recognizing that paper ballots are the most hack-proof way of conducting elections, we still wanted to recognize states using DRE machines that provide a paper record of votes cast. If a state uses paperless DRE machines in any of its jurisdictions, it received an "unsatisfactory" score for that category.

For the category of post-election audits, this report identifies nine best practices for carrying out such audits. Because robust post-election audits are considered particularly important for improving election security, states must adhere to all nine of those best practices to receive a "good" score for this category. States that meet seven or eight standards received a "fair" score, and meeting three to six standards earned a state a "mixed" score. Failing to adhere to at least two "best practices" resulted in the state receiving 0 points for this category. Even if a state met a majority of the best practices included in this category, it could still receive an "unsatisfactory" score if it failed to meet the best practices of making audits mandatory or controlling for erroneous preliminary outcomes, as these are particularly important for carrying out meaningful post-election audits. A state also automatically earned an "unsatisfactory" score for this category if it uses paperless DRE machines in any jurisdictions, as these machines are impossible to adequately audit.

The category of minimum cybersecurity standards for voter registration systems is one of those where the recommended minimum standards are so numerous that it made sense to provide states with the opportunity to earn additional points for adhering to all or almost all of the recommendations. The scoring for this category differed slightly depending on whether the state uses electronic poll books. Because we did not want to penalize states for their decision to use or not to use electronic poll books, the two recommended standards relating to electronic poll books were not considered for scoring states that do not use them. Thus, states that use electronic poll books were measured against a total of eight standards, while states that do not use electronic poll books—or are only in the early piloting stages of using electronic poll books—were measured against a total of six standards, as detailed further below.

Each individual best practice standard within a given category was given equal weight, aside from the exceptions mentioned above.

In some cases, information on a state's adherence to cybersecurity standards for voter registration systems was difficult to find. There are many reasons states may have for keeping information on specific cybersecurity requirements of state-run databases private and inaccessible to the public, including researchers. Throughout our research, we made numerous attempts to reach out to state officials about their states' cybersecurity requirements and practices for voter registration. Unfortunately, some states failed to respond to our requests for information and comment, while others refused to do so, citing legal or security reasons in some cases. As a result, we were unable to award these states credit for certain cybersecurity standards due to missing pieces of information. This is not to say that these states do not in fact require these important security measures, but rather that we were unable to award credit to the state for information that was not provided. In such cases, states received an "incomplete" for the cybersecurity category with missing information, but were awarded credit where possible based on the information we did have. We felt that this was the fairest way to handle the point distribution, as we did not want to deter states from sharing information with us or punish those states that did share information on voter registration cybersecurity. To increase transparency and public confidence in U.S. elections, it is important that the public have access to information about the measures that states are taking to protect voter data. Notably, states with an "incomplete" score in the cybersecurity category may have a higher score overall if they are in fact carrying out the missing standards. However, at most, a state with an "incomplete" score in the cybersecurity category would raise its grade by only one letter grade

if it adheres to all the missing best practices standards in that category. In most cases, a state's grade would not change at all given the point distribution for other categories. We indicate that a state's grade may be higher by way of a solidus or forward slash (Example: D/C) if there was information missing on a state's voter registration cybersecurity requirements and if the state's overall grade would change if it is carrying out the missing cybersecurity best practices.

The issue of election security is expansive and fast-moving. As such, it is always possible that certain data points may need updating as state laws and practices change or more information becomes available. Information contained in this report reflects research and analysis at the point of publication.

The grades for each state were assigned per the following point distribution:

- A = 13 points
- B = 10 points to 12 points
- C = 7 points to 9 points
- D = 4 points to 6 points
- F = 1 point to 3 points

A more comprehensive description of the standards and explanation of the best practices against which states were graded is below.

Category 1: Cybersecurity standards for voter registration systems

Some states still use voter registration databases that are more than a decade old, leaving them susceptible to modern-day cyberattacks.[61] If successfully breached, hackers could alter or delete voter registration information, which in turn could result in eligible voters being turned away at the polls or prevented from casting ballots that count. Hackers could, for example, switch just a few letters in a registered voter's name without detection.[62] In states with strict voter ID laws, eligible voters could be prevented from voting because of discrepancies between the name listed in an official poll book and the individual's ID. In addition, by changing or deleting a registered individual's political affiliation, hackers could prevent would-be voters from participating in partisan primaries.

There are serious privacy implications associated with breaches to voter registration databases. Voter registration lists contain myriad personal information about eligible voters—including names, addresses, dates of birth, driver's license numbers, political affiliations, and partial Social Security numbers—that could be used by foreign or domestic adversaries in any number of ways.[63] Moreover, while electronic poll books have been shown to increase efficiency and reduce wait times at polling places, they are subject to tampering and malfunction, as is true with any electronic system.[64] Guarding voter registration systems against hacking and manipulation is therefore critically important to protecting the right to vote and voter privacy.

It is worth noting that the recommendations listed below represent minimum cybersecurity standards that states should have in place to protect their voter registration systems. We sought to frame our inquiry into state voter registration systems broadly to avoid providing any kind of road map to potential malicious actors. We know that there are cybersecurity standards beyond those listed below that states should adopt in order to protect voter information, and we recommend that election officials work with cybersecurity experts in implementing them. For example, all states should have a backup voter registration database available in case emergencies arise.

The factors considered for grading in this category are:

- **Whether the state's voter registration system provides access control to ensure that only authorized personnel can access the voter registration database.** Access control is perhaps the most basic cybersecurity requirement that all states should implement to prevent unauthorized access to voter registration databases and sensitive voter information.[65] Access control measures can consist of anything from single or multifactor authentication to IP-recognition software, ensuring that only those with permission have access to the voter registration system.

- **Whether the state's voter registration system has logging capabilities to track modifications to the voter registration database.** Logging capabilities allow cyberprofessionals to monitor activity—innocent and malicious—on databases containing sensitive information.[66] When used, the software records all changes made to a database, oftentimes along with the name or IP address of the user responsible. A timestamp of when the change was made is also often provided.[67] Logging capabilities assist with investigations into suspicious cyberactivity by allowing cyberanalysts to identify and track those responsible.

- **Whether the state's voter registration system includes an intrusion detection system that monitors a network of systems for irregularities.** As the name suggests, intrusion detection systems monitor networks and computers for malicious or anomalous activity and alert relevant parties when potential problems arise.[68] Intrusion detection systems can include firewalls, anti-virus software, and spyware detection programs, to name just a few.[69] Given the increasing frequency and growing sophistication of modern-day cyberattacks, state officials must be alerted to potential breaches as soon as they occur so that they can respond accordingly to prevent the loss or alteration of sensitive information.

- **Whether the state performs regular vulnerability analysis on its voter registration system.** To understand the full extent of election-related risk, vulnerability assessments should be carried out continuously on voter registration databases. By conducting regular vulnerability assessments, the state can identify the existence and extent of potential weakness within its voter registration system. By doing so, election officials can better determine where government resources should be allocated and plan for preventative measures and strategies.

- **Whether the state has enlisted DHS or the National Guard to help identify and assess potential threats to its voter registration system.** While it is important for states to retain a level of autonomy over the administration of their elections, many states lack the personnel and resources necessary to thoroughly probe and analyze complex cybervulnerabilities in election databases and machines. Federal agencies and military personnel with expertise in cybersecurity and who may be privy to classified information on contemporaneous cyberthreats should be responsible for carrying out comprehensive threat assessments on election infrastructure.[70] By combining their expertise on cyberthreats and insight into the unique qualities of localized election infrastructure, state and federal officials can better assess and deter attempts at electoral disruption.[71] DHS services—which can include cyberhygiene scans, risk and vulnerability assessments, and incident response assistant, among other things[72]—come at no cost to the states.[73]

- **Whether the state provides cybersecurity training to election officials.** Election officials are on the front lines of guarding U.S. elections against attack by foreign and domestic actors, as well as a host of other potential Election Day problems. However, few election officials possess the kind of cybersecurity expertise necessary to detect and protect against potential attacks.[74] Even basic training to identify spear-phishing attempts and respond to other suspicious cybernetwork activity can go a long way toward improving election security.

For states that use electronic poll books, additional considerations are:

- **Whether the state requires that all electronic poll books undergo testing before Election Day.** As with all voting machines, electronic poll books should be tested prior to Election Day to ensure that they are in good and proper working order. In doing so, election officials can avoid machine malfunctions on Election Day that result in long lines for voters, which can hinder voter participation.

- **Whether backup paper voter registration lists are available at polling places using electronic poll books on Election Day.** To ensure that voter registration lists are accessible during voting periods, states should establish paper-based contingency plans during early voting and on Election Day in case electronic poll books experience malfunctions or hacking. Each polling place that uses electronic poll books should be required to have paper copies of its voter registration lists available that can be consulted throughout the voting process in case of emergency.

Points were distributed for this category as follows, depending on whether the state uses electronic poll books:

States using electronic poll books:

- State adheres to eight best practices: **Good, 3 points**
- State adheres to six or seven best practices: **Fair, 2 points**
- State adheres to three to five best practices: **Mixed, 1 point**
- State adheres to zero to two best practices: Unsatisfactory, **0 points**

States not using electronic poll books:

- State adheres to six best practices: Good, **3 points**
- State adheres to four or five best practices: **Fair, 2 points**
- State adheres to two or three best practices: **Mixed, 1 point**
- State adheres to zero or one best practices: **Unsatisfactory, 0 points**

We also provide information on the estimated age of a state's voter registration system. This information was not factored into the point distribution. However, we felt it was important to include in order to provide a fuller picture of voter registration system cybersecurity.

- **Estimated age of a state's voter registration system.**[75] One of the most important steps that a state can take to improve election security is updating its voter registration system to support software upgrades that guard against and prevent modern-day cyberattacks. Research has been done on the threat posed by outdated voting registration systems. Outdated voter registration systems often lack the specific hardware and software components necessary to adequately guard against modern-day cyberthreats, leaving states vulnerable to hacking and system crashes. Some state voter registration systems, for example, still run on outdated and unsupported software such as Windows XP or Windows 2000. However, even an updated voter registration system can be vulnerable to attack if the state fails to put into place other basic cybersecurity standards that monitor and protect the system.

Category 2: Voter-verified paper audit trail

Confirmation that votes were correctly counted cannot be provided unless a reliable auditable paper trail exists that can be checked against the official election outcome. Paper ballots that are tabulated by optical scanning machines and voter-verified paper records produced by DRE machines offer a record of voter intent, which will exist even if voting machines are attacked and data are altered. Admittedly, paper ballots and records can only help detect malicious activity after votes are cast, and only if robust post-election audits are conducted with the ability to detect and remedy erroneous preliminary outcomes. However, conducting elections with paper-based voting systems is one of the most important steps states can take to improve election security. They are necessary both to conduct meaningful post-election audits that can confirm the election outcomes and to enable post hoc correction in the event of malfunction or security breaches.

Given the importance of having a voter-verified paper audit trail, states received "good" scores—a full 3 points—if they carry out elections using paper ballots statewide. Because evidence has shown that all electronic voting machines are vulnerable to manipulation, voting on paper is the most hack-proof way of conducting elections. Of course, even electronic tabulating equipment such as optical scan machines can be hacked. However, at least with a paper ballot, election officials have a hard copy to go back to in order to verify the voter's selection. As such, paper ballots are preferable from an election security standpoint even to DRE machines with VVPR, which allow voters to review the machine's reading of their vote prior to casting, although it is uncertain that all voters do so.

However, because DRE machines with VVPR leave a paper record that can be used in post-election audits, we awarded states that use such machines exclusively or in combination with paper ballots some points for this category. States that use VVPR-producing voting machines statewide or in combination with paper ballots and/or ballot marking devices received a "satisfactory" score. If a state uses paperless DRE machines in any of its jurisdictions, it automatically received an "unsatisfactory" score for this category.

Federal law requires all states to have a minimum number of electronic voting machines available for accessibility purposes. Because those machines are necessary in order to accommodate and facilitate voting among people with disabilities and comply with requirements set out in the Help America Vote Act of 2002, their use in states for this limited purpose was not considered for grading purposes.

Points were distributed for this category as follows:

- State only uses paper ballots statewide: **Good, 3 points**
- State uses VVPR-producing DRE machines statewide or in combination with paper ballots and/or ballot marking devices: **Fair, 2 points**
- State uses paperless DRE machines in any of its jurisdictions: **Unsatisfactory, 0 points**

**States that allow voting by mail were awarded a full 3 points for this category given that the overwhelming majority of voters in those states use paper ballots. This is true even though most vote-by-mail states make some DRE machines with VVPR available at vote centers, though mostly for accessibility purposes.*

Category 3: Post-election audits

Because all voting machines are vulnerable to hacking, misprogramming, and even to using the wrong kind of pen to mark ballots, it is of the utmost importance that election officials conduct robust post-election audits that have a large chance of catching and correcting wrong outcomes. Even jurisdictions that hand-count all ballots should carry out post-election audits, as the counting process can be mired in human error. Importantly, an audit is only as good as the reliability of the ballots it tests. Therefore, meaningful post-election audits can only be conducted in states with strong voter-verified paper audit trails.

After an election, many states carry out vote tabulations audits, which tests vote tabulation machines to ensure they have been properly aggregated on a fixed-percentage or fixed-number of audit units. Risk-limiting audits—considered the "gold standard" of post-election audits—increase the efficiency of the auditing process by testing only the number of ballots needed to determine the accuracy of election outcomes. Risk-limiting audits include an initial sample of ballots, based on the margin of victory, which are interpreted by hand. Depending on the results of the initial manual count, the audit may expand. As a result, risk-limiting audits offer election administrators an effective and efficient way to test the accuracy of an election without breaking the bank. Risk-limiting audits are the only kind of audit that can determine with a high degree of confidence that election outcomes are correct and have not been manipulated. However, as risk-limiting audits are a relatively new proposal and are just being adopted by states, we graded states for the existence of the audit practices they do have that function to confirm that ballots have been counted as cast.

The factors considered for grading in this category include:

- **Whether post-election audits are mandatory.** Post-election audits must be carried out after every election to confirm the accuracy of election outcomes. By only conducting audits after certain elections, states leave themselves vulnerable to hackers who can target unaudited races and election years. Moreover, tabulating machines can malfunction at any time and during any election. Audits must be carried out any time election results matter, meaning after every single election.

- **Whether the audit is conducted by a manual hand count.** Some states use the term "audit" to describe the process of simply rescanning batches of ballots after an election. Relying on these electronic scans—which are as vulnerable as any other computer data—limits the kinds of problems these reviews can detect. The scans aren't like photographs; they can differ due to machine error, tampering, or human error.[79] To trust that audit results are correct, auditing procedures must be software-independent. As long as an audit depends on electronic tabulators or devices, it can be hacked or manipulated. We recognize that manual audits can require resources—funding and personnel—that some localities may lack. However, in this day and age, where cyberintrusions by nation-states are an ever-growing threat, post-election audits—which are vitally important to election security—must be carried out by hand. The threat is simply too great to leave audits in the control of hackable machines and devices.

- **Whether the audit includes a minimum number of ballots based on a statistically significant number tied to the specific margin of victory in one or more ballot contests.** Tying the number of ballots included in a post-election audit to the margin of victory in one of more ballot contests—rather than a fixed-percentage or number—ensures that enough ballots are examined to create convincing evidence that the outcome is correct, and it also saves resources. For example, if the margin of victory between the winner and loser of a ballot contest is quite large, there is a high likelihood that the auditing of even a small batch of ballots will confirm the accuracy of the election outcome, which saves election officials time and resources. Alternatively, if the margin of victory is small, more ballots need to be audited because there is less room for error. While a more expansive audit requires expending more time and resources on the auditing process, doing so results in greater certainty that the election outcome is correct.

- **Whether the ballots, machines, or jurisdictions selected for the audit are chosen at random.** Random selection of the election components included in a post-election audit is necessary in order to prevent hackers from putting in place plans and procedures to rig the post-election audit process or from targeting specific machines or ballot categories that they know will not be included in the audit.

- **Whether all categories of ballots—regular, early voting, absentee, provisional, and UOCAVA—are eligible for auditing.** All ballot types should be eligible for inclusion in post-election audits. By only auditing certain categories of ballots, election officials may fail to detect anomalies in the tabulation of other ballot types. This is particularly important in states where absentee, early voting, or provisional voting is popular among voters. For example, in North Carolina, at least 56,000 provisional and absentee ballots were cast during the 2016 election.[80] By failing to include all ballot types in the auditing process, states can exclude from testing and analysis ballots that have the potential to alter election outcomes.

- **Whether the audit escalates to include more ballots.** If an audit fails to find strong enough evidence that the preliminary outcome is right, it should escalate to include more ballots to ensure confidence in election results. Escalation should lead to a full recount if necessary.

- **Whether the audits are conducted in a public forum or the results made immediately available for public review.** Post-election audits should either be open to public observance or the results made publicly available in order to increase transparency and public confidence in the accuracy of election outcomes.

- **Whether audits are conducted in a timely manner before certification of official election results.** Post-election audits should be carried out after preliminary outcomes are announced, but before official certification of election results. This gives election officials enough time for escalation and correction of preliminary results if preliminary election outcomes are found to be incorrect. That said, post-election audits conducted after certification can still be useful if they have the ability to overturn the certified results if the audit finds they are wrong.

- **Whether the audit can correct the preliminary result of an audited contest if it discovers that the preliminary result was wrong.** In other words, do audits control the overall results? To be meaningful, post-election audit results must be able to reverse preliminary outcomes if the audit determines they are incorrect. The utility of post-election audits depends on their ability to correct incorrect election results.

Points were distributed for this category as follows:

- State adheres to nine best practices: **Good, 3 points**
- State adheres to seven or eight best practices: **Fair, 2 points**
- State adheres to three to six best practices: **Mixed, 1 point**
- State adheres to zero to two best practices: **Unsatisfactory, 0 points**

**A state received an "unsatisfactory" score for this category if (1) the state's post-election audits are not mandatory, (2) the results are not binding on official election outcomes, or (3) the state uses paperless DRE machines—which are not auditable—in any jurisdiction. This was true even if the state adheres to a majority of the other best practices included within this category. The added weight does not work in reverse. For example, if a state met only six of the standards—including that the audit is mandatory and binding—its score would not be raised from "mixed" to "fair."*

Category 4: Ballot accounting and reconciliation

A paper-based voting system must be combined with strong ballot accounting and reconciliation requirements and procedures. Ensuring that all ballots—used and unused—are accounted for at the close of Election Day and that all votes are included in the final vote tally is one of the most basic and important ways that election officials can improve the security of their elections. By doing so, election officials can protect against voted ballots being lost, causing incomplete vote counts,

or invalid ballots being added, causing incorrect vote counts. A great deal of the research on state ballot accounting and reconciliation included in this section is derived from a comprehensive 2012 report from Common Cause, Verified Voting, and Rutgers School of Law entitled "Counting Votes 2012: A State by State Look at Voting Technology Preparedness."[81] While we relied on the research by the authors of that report, we conducted a thorough review to update the research where there had been changes in the law.

The factors considered for grading in this category include:

- **Whether all ballots are accounted for at the precinct level.** Before vote totals can be accumulated by the state, local election officials must tally and account for all ballots—used and unused—at individual polling places or at vote centers. Precinct officials are best positioned to account for the ballots they received and ballots that have been cast, spoiled, or unused, or that were submitted provisionally. As such, this process should be completed at the local level.

- **Whether precincts are required to compare and reconcile the number of ballots cast with the number of voters who signed in at the polling place.** Part of the ballot accounting and reconciliation process involves comparing the number of ballots to the number of voters who showed up to the polls to participate in the electoral process. Only through comparing the number of votes to the number of voters can election officials be confident that ballots have not been removed or brought into the polling place from elsewhere. In reconciling these numbers, poll workers should be prohibited from randomly discarding any excess ballots. As the authors of "Counting Votes 2012" found, and as our independent review confirmed, some states still allow this ill-advised practice and lost a point for this category as a result.[82]

- **Whether county officials are required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct number.** Once they receive and conglomerate vote totals, county officials should examine and compare the countywide results to tallies submitted by the precincts to make sure that they add up to the correct number. Doing so provides election officials with some assurance that the results are correct and can help to detect a computing error if one exists.

Points were distributed for this category as follows:

- State adheres to three best practices: **Fair, 1 point**
- State adheres to zero to two best practices: **Unsatisfactory, 0 points**

We provide additional information on state ballot accounting and reconciliation procedures that was not factored into the point distribution as wide variation and lack of visibility make them difficult to evaluate; however, we felt it was important to include the information in order to provide a fuller picture of state practices in this area.

- **Whether counties are required to review and account for all voting machine memory cards and flash drives to ensure that they have been properly loaded onto the tally server.** Our democracy depends on every valid vote being counted on Election Day. As such, it is critically important that election officials review status reports from electronic tally servers in states that use them in order to ensure that all voting machine memory cards and flash drives are properly uploaded and counted. In some states, the electronic management software that tabulates results provides a warning if all memory cards or flash drives that were created for an election are not properly uploaded. Electronic systems are more convenient, but they are prone to hacking or manipulation by sophisticated actors. As such, any review process should ideally be software-independent.

- **Whether the state requires that vote tallies and any ballot reconciliation information be made public.** Transparency is necessary for all election processes—especially those involving vote totals—in order to establish public confidence in the electoral system and election outcomes. By making information available on election results for each candidate and ballot issue, as well as the ballot reconciliation processes that were used to reach those results, states can improve public confidence in their elections.

Category 5: Return of voted paper absentee ballots

Electronic absentee voting—or the return of voted absentee ballots electronically via email, fax, or web portal—is risky because there is no way for absentee voters to know whether the votes they cast are being accurately recorded. While 29 states only allow electronic submission for UOCAVA voters, three states allow any absentee voter to return completed ballots electronically.[83]

Most experts agree that returning voted ballots electronically is not safe. An official from DHS's Cyber Security Division warned that "online voting, especially online voting in large scale, introduces great risk into the election system by threatening voters' expectations of confidentiality, accounting and security of their votes and provides an avenue for malicious actors to manipulate the voting results."[84] The National Institute of Standards and Technology has also warned against online voting.[85] Furthermore, it is impossible to carry out meaningful post-election audits on voted ballots submitted electronically because there is no reliable paper record that can be referenced during the auditing process.

Of course, it is of utmost importance that military personnel and U.S. citizens stationed and living overseas are provided opportunities to vote and have their voices heard in our democracy. It is equally important, however, that their votes be delivered securely and their privacy protected. Currently, that means returning a hard copy paper ballot via U.S. mail. Requiring UOCAVA voters to return ballots by mail does not appear to have a significant impact on ballot return rates. If we base projections of UOCAVA ballot return rates on information contained in Pew surveys of unreturned UOCAVA ballots in the states in 2012 and 2014,[86] we see that states requiring UOCAVA voters to return voted ballots via mail actually had a slightly higher return rate those years than states that permit voted ballots to be returned electronically."[87]

For this category, states were graded simply on whether they require voted absentee ballots to be returned by mail. If so, a state received a "fair" score—or 1 point—for that category. If the state allows any voters, including regular absentee or UOCAVA voters, to return ballots electronically—via email, fax, or web portal—it received an "unsatisfactory" score, or 0 points.

Some feel that the return of voted ballots electronically constitutes a significant threat to election security, on par with use of paperless DRE machines, lack of minimum cybersecurity standards for voter registration systems, and inadequate auditing procedures.[88] While we share concerns over electronic absentee voting, we reserved the weighted point distribution for those three categories listed above.

Category 6: Voting machine certification requirements

This category is concerned more with preventing machine malfunction than hacking. Even new machines that are certified and tested to federal requirements are vulnerable to hacking and manipulation by sophisticated actors. Even so, for the purposes of preventing Election Day disruptions, the basic technological requirements that voting machines must adhere to before being purchased and used in a state are worth consideration.[89]

States should ensure that any machine they purchase adheres to the Election Assistance Commission's Voluntary Voting System Guidelines. The EAC's guidelines require voting machines and components to meet minimum security, functionality, and accessibility standards. Some states have their own certification requirements that either substitute or supplement the EAC's voluntary guidelines, and indeed some experts feel the federal certification process as a whole needs updating. However, we feel that adherence to a uniform set of standards helps to ensure basic functioning and efficiency for voting machinery and equipment. The EAC anticipates finalizing a new set of voting system guidelines in 2018, which will take into account advances in technology and emphasizes auditable voting systems and evidence-based elections.[90] Leaving the standard-setting process to the states can be an overwhelming task for state officials and can result in a mishmash of voting machine requirements across the country with varying degrees of thoroughness and stringency. Indeed, in speaking about federal voting machine standards, Rhode Island Secretary of State Nellie Gorbea said, "We in Rhode Island could not come up with as good and as fast a process for what the EAC already had with regards to general voting equipment guidelines."[91] As an alternative to requiring that all voting machines be EAC-certified, states may require that voting machines undergo review by a federally accredited laboratory or have statutory requirements that all voting machines must meet or exceed the federal standards.

Abiding by the EAC's Voluntary Voting System Guidelines is not foolproof against hacking or malfunction. Even EAC-certified voting machines can be hacked or experience problems. Therefore, it is again important to emphasize the importance of paper-based voting systems with voter-verified paper audit trails, which can be referred to if complications arise.

For this category, a state was graded on whether it requires its voting machines to be EAC certified, adhere to federal standards, or undergo testing by an EAC accredited laboratory. If so, a state received a "fair" score—or 1 point—for this category. If not, a state received an "unsatisfactory" score—or 0 points—for this category.

While not graded, we also provided information on whether the state still uses voting machines that are at least a decade old.[92] Old voting machines pose serious security risks and are susceptible to system crashes, "vote flipping," and hacking, as many rely on outdated computer operating systems that do not accommodate modern-day cybersecurity protections.[93] Moreover, upkeep for outdated machines is becoming increasingly difficult, because many parts are no longer manufactured. According to experts, the predicted lifespan for most voting machine models is around 10 years.[94] Adding to this, experiments conducted by computer scientists on electronic voting machines have shown that they are easily hacked, can be reprogrammed to predetermine electoral outcomes, and are susceptible to malicious vote-stealing software.[95] While more long-term solutions to fixing flaws in voting machine architecture may be required,[96] one thing states can do right now to better protect against machine malfunction and Election Day disruptions is to invest in replacing all outdated voting machines. This would include switching to a paper ballot system with new optical scan machines.

As stated previously, just because a voting machine is new does not mean that it is safe from hacking and malfunction. While newer machines may include updated software components that lend some protection against system failure, all electronic voting machines are potentially vulnerable to problems and disruption. It is for this reason that any new voting machine must be accompanied by a paper ballot component or voter-verified paper trail that can be referred to in case problems arise.

We recognize that in many states new voting machines are purchased by the counties rather than at the state level. Even when this is the case, however, states and the federal government should assist localities in purchasing new machines by providing adequate funding.

Category 7: Pre-election logic and accuracy testing

As with the previous section, this category is concerned more with preventing machine malfunction than hacking. Logic and accuracy testing is not foolproof. Indeed, sophisticated hackers can manipulate pre-election testing procedures by installing malware that remains inactive during pre-election tests but activates during voting periods. Even so, pre-election testing remains a basic step that election officials can take to help detect possible machine errors and address machine-related problems prior to Election Day.

The purpose of pre-election logic and accuracy testing is to examine, before a single vote is cast, whether the machines that will be used on Election Day or during early voting will function correctly when voters show up to vote. Pre-election logic and accuracy testing should be mandatory and should be conducted on all machines that will be used for voting or to tabulate ballots during an election. Most states already have laws in place requiring state officials to test voting machines and equipment in the weeks and months leading up to an election, although their scope varies depending on the jurisdiction.[97] Some states require that all voting machines be tested, while others limit testing to only a small sample.

It is important that all voting machines that will be used in an upcoming election be tested prior to Election Day to ensure that they will accurately read and tabulate votes during voting periods. By testing only a small number or percentage of machines, states may allow other machines with potential problems to slip through the cracks.

For this category, states were graded on whether election officials are required to perform pre-election logic and accuracy testing on all voting machines that will be used in an election. If so, the state received a "fair" score—or 1 point—for this category. If not, the state received an "unsatisfactory" score—or 0 points—for this category.

We also provide information on some specific pre-election logic and accuracy testing procedures. This information was not factored into the point distribution; however, we felt it was important to include it in order to provide a fuller picture of state practices related to pre-election machine testing.

- **Whether the testing is open to the public.**[98] Pre-election logic and accuracy testing should take place in a public forum with appropriate public notice, thereby increasing transparency and public confidence in the election process.

- **Whether testing is conducted close to the election, but with enough time to allow for effective remediation.** Testing should be carried out close enough to an election to ensure that the machines are in a similar condition to Election Day as they were at the time of testing, but with enough time for election officials to reprogram or replace voting machines that exhibit problems during testing.

State	Minimum cybersecurity for voter registration systems	Voter-verified paper audit trail	Post-election audits	Ballot accounting and reconciliation	Paper absentee ballots	Voting machine certification requirements	Pre-election logic and accuracy testing	Grade
Alabama	Good	Good	Unsatisfactory	Fair	Unsatisfactory	Fair	Fair	C
Alaska	Good	Good	Fair	Fair	Unsatisfactory	Fair	Fair	B
Arizona	Mixed	Good	Unsatisfactory	Unsatisfactory	Unsatisfactory	Fair	Fair	D
Arkansas	Incomplete	Unsatisfactory	Unsatisfactory	Unsatisfactory	Fair	Fair	Fair	F/D*
California	Fair	Fair	Mixed	Unsatisfactory	Unsatisfactory	Fair	Fair	C
Colorado	Fair	Good	Good	Fair	Unsatisfactory	Fair	Fair	B
Connecticut	Fair	Good	Mixed	Fair	Fair	Fair	Fair	B
Delaware	Good	Unsatisfactory	Unsatisfactory	Unsatisfactory	Unsatisfactory	Fair	Fair	D
District of Columbia	Good	Good	Fair	Unsatisfactory	Unsatisfactory	Fair	Fair	B
Florida	Incomplete	Unsatisfactory	Unsatisfactory	Unsatisfactory	Unsatisfactory	Unsatisfactory	Fair	F*
Georgia	Fair	Unsatisfactory	Unsatisfactory	Fair	Fair	Fair	Fair	D
Hawaii	Incomplete	Fair	Fair	Unsatisfactory	Unsatisfactory	Fair	Unsatisfactory	D/C*
Idaho	Fair	Good	Unsatisfactory	Unsatisfactory	Unsatisfactory	Fair	Fair	C
Illinois	Mixed	Fair	Fair	Unsatisfactory	Fair	Fair	Fair	C
Indiana	Incomplete	Unsatisfactory	Unsatisfactory	Unsatisfactory	Unsatisfactory	Fair	Unsatisfactory	F*
Iowa	Incomplete	Good	Unsatisfactory	Fair	Unsatisfactory	Fair	Fair	C*
Kansas	Incomplete	Unsatisfactory	Unsatisfactory	Unsatisfactory	Unsatisfactory	Fair	Fair	F/D*
Kentucky	Good	Unsatisfactory	Unsatisfactory	Unsatisfactory	Fair	Fair	Fair	D
Louisiana	Fair	Unsatisfactory	Unsatisfactory	Fair	Unsatisfactory	Fair	Fair	D
Maine	Fair	Good	Unsatisfactory	Unsatisfactory	Unsatisfactory	Fair	Fair	C
Maryland	Good	Good	Unsatisfactory	Fair	Fair	Fair	Fair	B
Massachusetts	Fair	Good	Unsatisfactory	Fair	Unsatisfactory	Fair	Fair	C
Michigan	Fair	Good	Unsatisfactory	Unsatisfactory	Fair	Fair	Fair	C
Minnesota	Fair	Good	Fair	Unsatisfactory	Fair	Fair	Fair	B
Mississippi	Fair	Unsatisfactory	Unsatisfactory	Fair	Unsatisfactory	Fair	Fair	D
Missouri	Incomplete	Fair	Mixed	Unsatisfactory	Unsatisfactory	Fair	Fair	D*
Montana	Fair	Good	Unsatisfactory	Fair	Unsatisfactory	Fair	Fair	C
Nebraska	Good	Good	Unsatisfactory	Unsatisfactory	Unsatisfactory	Fair	Fair	C
Nevada	Mixed	Fair	Fair	Unsatisfactory	Unsatisfactory	Fair	Fair	C
New Hampshire	Incomplete	Good	Unsatisfactory	Fair	Fair	Unsatisfactory	Fair	C*
New Jersey	Good	Unsatisfactory	Unsatisfactory	Unsatisfactory	Fair	Unsatisfactory	Fair	D

State	Minimum cybersecurity for voter registration systems	Voter-verified paper audit trail	Post-election audits	Ballot accounting and reconciliation	Paper absentee ballots	Voting machine certification requirements	Pre-election logic and accuracy testing	Grade
New Mexico	Fair	Good	Fair	Fair	Unsatisfactory	Fair	Fair	B
New York	Good	Good	Mixed	Fair	Fair	Fair	Fair	B
North Carolina	Good	Fair	Fair	Fair	Unsatisfactory	Fair	Fair	B
North Dakota	Incomplete	Good	Unsatisfactory	Fair	Unsatisfactory	Fair	Fair	C*
Ohio	Incomplete	Fair	Fair	Unsatisfactory	Fair	Fair	Fair	C/B*
Oklahoma	Incomplete	Good	Unsatisfactory	Unsatisfactory	Unsatisfactory	Fair	Fair	C*
Oregon	Good	Good	Fair	Unsatisfactory	Unsatisfactory	Fair	Fair	B
Pennsylvania	Fair	Unsatisfactory	Unsatisfactory	Unsatisfactory	Fair	Fair	Fair	D
Rhode Island	Good	Good	Good	Unsatisfactory	Unsatisfactory	Fair	Fair	B
South Carolina	Good	Unsatisfactory	Unsatisfactory	Fair	Unsatisfactory	Fair	Fair	D
South Dakota	Incomplete	Good	Unsatisfactory	Fair	Fair	Fair	Fair	C*
Tennessee	Incomplete	Unsatisfactory	Unsatisfactory	Unsatisfactory	Fair	Fair	Unsatisfactory	F/D*
Texas	Mixed	Unsatisfactory	Unsatisfactory	Fair	Unsatisfactory	Fair	Fair	D
Utah	Fair	Fair	Fair	Unsatisfactory	Unsatisfactory	Fair	Fair	C
Vermont	Fair	Good	Unsatisfactory	Fair	Fair	Unsatisfactory	Fair	C
Virginia	Fair	Good	Unsatisfactory	Unsatisfactory	Fair	Fair	Unsatisfactory	C
Washington	Good	Good	Unsatisfactory	Unsatisfactory	Unsatisfactory	Fair	Fair	C
West Virginia	Good	Fair	Fair	Unsatisfactory	Unsatisfactory	Fair	Fair	C
Wisconsin	Good	Fair	Unsatisfactory	Unsatisfactory	Fair	Fair	Fair	C
Wyoming	Fair	Fair	Unsatisfactory	Unsatisfactory	Fair	Fair	Fair	C

* Indicates states that either failed to share certain pieces of information regarding minimum cybersecurity practices with us, refused to share information with us citing legal or security reasons, or declined to participate in our research. A few states with "incomplete" scores in the cybersecurity category may have higher overall grades if they are in fact carrying out the missing standards in that category, as illustrated by a solidus or forward slash. However, in no case would a state's overall grade increase by more than one letter grade.

Alabama

Although Alabama conducts its elections with paper ballots and adheres to a number of minimum cybersecurity best practices for voter registration systems, it fails to require post-election audits that confirm the accuracy of election outcomes, leaving the state vulnerable to hacking and manipulation. Adding to this is the fact that Alabama permits UOCAVA voters to return voted ballots via web portal, a practice that election security experts warn as being notoriously insecure and vulnerable to manipulation. It is commendable that even though the state does not currently offer cybersecurity training to election officials, a new vendor contract requires personnel with access to the voter registration system will receive cybersecurity training in time for the 2018 elections. It is also worth recognizing that Alabama requires that all voting machine be tested to EAC Voluntary Voting System Guidelines before being purchased or used in the state, and also requires election officials to carry out pre-election logic and accuracy testing on all machines that will be used in an upcoming election.

To improve its overall election security, Alabama must require robust post-election audits that can detect errors in election outcomes and provide ad hoc corrections. In doing so, the state should look to risk-limiting audits like those in Colorado as a potential model. Alabama should also prohibit voters stationed or living overseas from returning voted ballots electronically.

Minimum cybersecurity standards for voter registration system: Good

- The state's voter registration system has been updated within the past 10 years.[99]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[100]
- The state's voter registration system has logging capabilities to track modifications to the database.[101]
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[102]
- The state performs vulnerability assessments on its voter registration system.[103]
- The state has enlisted DHS to help assess and identify potential threats to its voter registration system.[104]

- Officials within the Election Division of the Office of the Secretary of State completed cybersecurity training in 2017.[105] The state does not currently require cybersecurity training for election officials, but will by the 2018 elections.[106]
- In May 2016 the state legislature enacted SB 200, which established an electronic poll book pilot program.[107] Electronic poll books were used in some counties during the 2016 general election. Paper copies of voter registration lists were available at the polling places that used them.[108] In May 2017 the Alabama secretary of state began soliciting bids for electronic poll books that can be used statewide.[109] Because Alabama's electronic poll books are still in the piloting phase, the state was not graded on e-pollbook best practices.

While Alabama does not currently require election officials operating the state's voter registration system to receive any cybertraining, a new vendor contract requires that all personnel with access to the voter registration system receive cybersecurity training prior to an election. Training is scheduled to be provided in time for the 2018 elections.[110]

Voter-verified paper audit trail: Good

- Elections are carried out with paper ballots and optical scanning machines.[111]

Post-election audits: Unsatisfactory

- The state does not require post-election audits.[112]

Ballot accounting and reconciliation: Fair

- Ballots are fully accounted for at the precinct level.[113]
- Precincts are required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[114]
- Counties are required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[115]
- There is no statutorily mandated review process to ensure that all voting machine memory cards have been properly loaded onto the tally server at the county level.[116]
- While state law requires that election results be made public, it is unclear whether the same is true of information regarding ballot reconciliation processes and results.[117]

Paper absentee ballots: Unsatisfactory

- The state allows UOCAVA voters to submit completed ballots electronically, via web portal.[118]

Voting machine certification requirements: Fair

- Before being purchased and used for any election in the state, all voting machines must undergo testing by a federally accredited laboratory.[119]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[120]

Pre-election logic and accuracy testing: Fair

- **Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.**[121]
- Testing is open to the public.[122]
- The tests must be carried out "as close as is practical to the date of an election," but no more than 14 days before Election Day.[123]

Alaska

The state should be applauded for its adherence to minimum cybersecurity best practices related to voter registration systems and its statewide use of paper ballots, but Alaska's post-election audit procedures are lacking important criteria. The audit does not currently include UOCAVA ballots and the total number of ballots included in the audit is based on a fixed amount, rather than a statistically significant number tied to the margin of victory in one or more ballot contests. Adding to this is the fact that Alaska allows voters stationed or living overseas to return voted ballots electronically, a practice that election security experts say is notoriously insecure. Unlike most states, Alaska allows all absentee voters—not just UOCAVA voters—to return voted ballots via fax. Alaska's broad allowance of the practice leaves it vulnerable to Election Day problems. Alaska did receive points for requiring election officials to carry out pre-election logic and accuracy testing on all machines that will be used in an upcoming election.

To improve its overall election security, Alaska should expand its audit requirements to ensure that UOCAVA ballots—delivered by mail—are included in the audit, and base the number of ballots selected for the audit on a statistically significant number tied to margins of victory rather than a flat percentage. Additionally, even though all voting machines currently in use either meet or exceed the EAC's Voluntary Voting System Guidelines, state law should explicitly require that all future voting machines abide by EAC standards. The state should also prohibit absentee voters from returning voted ballots electronically. Going forward, all voted ballots should be returned by mail (or in person).

Minimum cybersecurity standards for voter registration system: Good

- The state's voter registration system was replaced with a new system in 2015. The new system went live November 2015.[124]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[125]
- The state's voter registration system has logging capabilities to track modifications to the database.[126]

- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[127]
- The state performs regular vulnerability assessments on its voter registration system.[128]
- The state has enlisted DHS to help assess and identify potential threats to its voter registration system.[129]
- The state provides cybersecurity training to election officials at the state level.[130]
- The state does not use electronic poll books, and therefore was not graded on e-pollbook best practices.[131]

Voter-verified paper audit trail: Good

- The state's main method of voting is with paper ballots. While each polling place is provided with a DRE machine with VVPR, those machines are intended for voters with disabilities.[133]

Alaska's voter registration system was replaced with a new system in 2015. The new system went live in November 2015.[132]

Post-election audits: Fair

- The state conducts mandatory post-election audits.
- The state's post-election audits are conducted through manual hand count.[134]
- The State Ballot Counting Review Board selects one precinct that accounts for at least 5 percent of the votes cast in each house district.[135]
- The precincts included in the audit are randomly selected.[136]
- UOCAVA ballots are not eligible for auditing.[137]
- State law requires that if there is a discrepancy of more than a 1 percent, all ballots for the district must be hand counted.[138]
- Audit results are publicly available.[139]
- State law requires that audits begin no later than 16 days after an election, prior to certification.[140]
- An audit can reverse the preliminary outcome of an audited contest if an error is detected.[141]

Ballot accounting and reconciliation: Fair

- All ballots are accounted for at the precinct level.[142]
- Precincts are required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[143]
- The Director of Elections, with the assistance and in the presence of the State Ballot Counting Review Board, reviews precinct vote tallies and compares them to countywide results for any discrepancies.[144]

- There is no statutorily mandated review process to ensure that all voting machine memory cards have been properly loaded onto the tally server at the county level.[145]
- State law requires that election results and ballot reconciliation information be posted online for public review.[146]

Paper absentee ballots: Unsatisfactory

- The state allows any absentee voter to return voted ballots electronically.[147] However, "in light of recent cyber threats to election systems," the state is in the process of adopting regulations that would prohibit absentee voters from returning completed ballots through a web portal "until a more secure solution is available." Absentee voters will still be allowed to return voted ballots by fax.[148]

"In light of recent cyber threats to election systems," Alaska is in the process of adopting regulations that would prohibit absentee voters from returning completed ballots through a web portal "until a more secure solution is available."[149]

Voting machine certification requirements: Fair

- State law does not require voting machines to meet federal requirements before they are purchased and used in elections in the state. The state can consider federal standards in purchasing and authorizing the use of voting machines, but there is no requirement to do so.[150] In practice, all voting machines currently in use meet the federal standards.[151]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[152]

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[153]
- The law does not specifically require that testing be open to public observance.
- Testing is carried out two months prior to an election.[154]

Arizona

Arizona uses paper ballots and voting machines that provide paper records, but the state's post-election audits do not include provisional ballots and are based on a fixed percentage of precincts rather than the margin of victory in one or more ballot contests. Most troublesome, however, is that post-election audits are only conducted if the political parties designate at least two election board members to carry out the audit by 5 p.m. on the Thursday preceding an election. And while we have been told that the state's largest county—Maricopa County—has always been able to meet these requirements since the law's enactment in 2006, it is unclear whether this is true of Arizona's other 14 counties. The state also fails to adhere to some important best practices for voter registration system cybersecurity, and its ballot accounting and reconciliation procedures could use improvement. Adding to this is the fact that Arizona allows voters stationed or living overseas to return voted ballots electronically, a practice that election security experts say is notoriously insecure. The state did earn points for requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines before being purchased or used in the state, and for requiring election officials to carry out pre-election logic and accuracy testing on all machines that will be used in an upcoming election.

To improve its overall election security, Arizona should strengthen its post-election audit requirements. Elections in Arizona will remain vulnerable until the state requires robust post-election audits after every election. These audits must be comprehensive and capable of determining—with a high degree of confidence—that election outcomes are correct. Additionally, Arizona should require electronic poll books to undergo pre-election testing before voting periods. Backup paper voter registration lists should also be required at polling places that use electronic poll books. Although the state requires that backup electronic poll books be provided, these electronic backups will do nothing to ensure that eligible voters can cast ballots that count if there is widespread system failure or a major cyberbreach that corrupted the entire electronic database. Moreover, Arizona should prohibit electronic absentee voting and strengthen its ballot accounting and reconciliation procedures by requiring counties to compare and reconcile precinct totals with composite results to ensure they add up to the correct number.

Minimum cybersecurity standards for voter registration system: Mixed

- The state's voter registration system is estimated to be at least 10 years old.[155]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[156]
- The state's voter registration system has logging capabilities to track modifications to the database.[157]
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[158]
- The state performs regular vulnerability assessments on its voter registration database.[159]
- The state has enlisted DHS to help assess and identify potential threats to its voter registration system.[160]
- Election officials are updating training regimens for election officials to include cybersecurity training.[161]
- Electronic poll books are used by some, but not all, jurisdictions in the state.[162] State law requires that at least two electronic poll books—capable of printing voter registration lists—be provided to polling places that choose to use them.[163] Paper copies of voter registration lists are not available at all polling places that use electronic poll books.[164] Testing is carried out on at some—but not all—electronic poll books prior to Election Day.[165]

According to State Election Director Eric Spencer, Arizona has "made a number of upgrades in Arizona's plan for election integrity and those improvements have enhanced the security of election information."[166]

Voter-verified paper audit trail: Good

- Arizona almost exclusively uses paper ballots, though some counties employ limited use of VVPR-producing DRE machines intended for voters with disabilities.[168]

For the November 2017 elections, Arizona's Maricopa County switched from a third-party electronic poll book vendor to an electronic check-in terminal programmed and designed in-house by the county's information technology staff. These check-in terminals were deployed and paired with a ballot-on-demand system that, upon check-in, allowed county election officials to systematically print any ballot version needed for a given voter.[167]

Post-election audits: Unsatisfactory

- While the state has a post-election audit requirement, the law also specifies that an audit can only be carried out if the political parties designate at least two election board members to carry out the audit. The names of these people must be provided, in writing, to the recorder or officer in charge of elections by 5 p.m. on the Thursday preceding the election. Since the audit requirement was passed in 2006, Maricopa County always has had a sufficient number of board members provided by the political parties to conduct the audit. However, this may not always be true of the state's other 14 counties.[169]
- The state's post-election audits are conducted through manual hand count.[170]

- In each county at least 2 percent of precincts are tested, or two precincts total, whichever is greater.[171] Audits examine up to five contested races, though for a general presidential election audits must include the presidential contest, one statewide ballot measure if any exist, one contested race for statewide office, one contested U.S. House or Senate race, and one contested race for state legislative office.[172]
- The precincts and contests included in the audit are randomly selected.[173]
- Audits do not examine provisional ballots, conditional provisional ballots, or write-in votes.[174]
- An audit escalates in the event that preliminary outcomes are found to be incorrect.[175]
- Unlike other aspects of the election process, state law does not require post-election audits to be recorded by live video for public viewing. Party representatives who observe the hand count may bring their own video cameras to record the proceedings.[176] However, in Maricopa County, audits are open for observation and the results are immediately available for public review through the Arizona secretary of state's office and website.[177]
- Audits are conducted prior to certification of official election results.[178]
- The results of an escalated audit may reverse the preliminary outcome of an audited contest if an error is detected.[179]

Ballot accounting and reconciliation: Unsatisfactory

- All ballots are accounted for at the precinct level.[180]
- Precincts are required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[181]
- Counties are not explicitly required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[182]
- There is no statutorily mandated review process to ensure that all voting machine memory cards have been properly loaded onto the tally server at the county level.[183]
- Counties using automatic vote tabulating equipment are required to make vote tally and reconciliation results public, although the law is vague on the process for doing so.[184] All other counties are required to post vote tallies for each candidate and ballot issue, along with the number of ballots that were cast and rejected, outside each polling place.[185]

Paper absentee ballots: Unsatisfactory

- The state permits UOCAVA voters to submit completed ballots electronically via fax or web portal.[186]

Voting machine certification requirements: Fair

- Before they may be purchased and used in the state, all voting machines must be certified by the Election Assistance Commission.[187]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[188]

Pre-election logic and accuracy testing: Fair

- Counties conduct mandatory logic and accuracy testing on all voting machines prior to an election.[190]
- Testing is open to the public.[191]
- For touchscreen and ADA accessible equipment, testing takes place within seven business days before early voting, while optical and digital scan equipment is tested within 10 business days before the election.[192]

According to State Election Director Eric Spencer, "We acknowledge our state will have to develop and implement a plan to replace aging voting equipment over the next decade. … Perhaps the most compelling reason to update our elections equipment is to further ensure that the security of these systems is up to date."[189]

Arkansas

Arkansas allows voting using machines that do not provide a paper record and fails to mandate post-election audits, which does not provide confirmation that ballots are cast as the voter intends and counted as cast. Despite numerous attempts to speak to someone in state government about the cybersecurity standards for the state's voter registration system, state officials did not respond to our requests for information and comments and we were unable to locate it independently. If Arkansas is adhering to all of the minimum cybersecurity best practices for voter registration systems, it would receive a "good" score—worth 3 points—for that category, bringing its grade up to a D. The state exercises good practices by requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines prior to being purchased or used in the state, and by requiring election officials to carry out pre-election logic and accuracy testing on all voting machines that will be used in an upcoming election. The fact that the state prohibits voters stationed or living overseas from returning voted ballots electronically is also commendable. In Arkansas, all voted ballots must be returned by mail or delivered in person.

To improve its overall election security, Arkansas should stop using paperless DRE machines in some jurisdictions and should require mandatory post-election audits in all jurisdictions. Until Arkansas requires statewide use of paper ballots and robust post-election audits that test the accuracy of election outcomes with a high degree of confidence, its elections will remain a potential target of sophisticated nation-states. Arkansas should also strengthen its post-election ballot accounting and reconciliation procedures by enacting precinct-level accounting requirements for DRE machines that mirror those required for jurisdictions with ballot tabulators. Whereas state law currently requires ballot tabulating precincts to compare the number of ballots cast with the number of voters who signed into the polling place, it is unclear whether the same is true for jurisdictions using DRE machines.

Minimum cybersecurity standards for voter registration system: Incomplete

**State officials did not respond to our requests for information and comments on cybersecurity requirements for the state's voter registration system. Information gathered for this section derives from independent research. If Arkansas does require the cybersecurity best practices about which we are missing, its grade would be raised from an F to a D.*

- The state's voter registration system is estimated to be at least 10 years old.[193]
- State officials were unable to provide us with information on whether the state's voter registration system provides access control to ensure that only authorized personnel have access to the database.
- State officials were unable to provide us with information on whether the state's voter registration system has logging capabilities to track modifications to the database.
- State officials were unable to provide us with information on whether the state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.
- State officials were unable to provide us with information on whether the state performs regular vulnerability assessments on its voter registration system.
- State officials were unable to provide us with information on whether the state has enlisted the National Guard or DHS to help assess and identify potential threats to its voter registration system.
- State officials were unable to provide us with information on whether the state provides cybersecurity training to election officials.
- The state permits the use of electronic poll books.[194] Unfortunately, state officials were unable to provide us with information on whether the state requires pre-election logic and accuracy testing on electronic poll books before an election or backup paper voter registration lists in jurisdictions that use them in case of emergency.

Voter-verified paper audit trail: Unsatisfactory

- Depending on the jurisdiction, some voters in Arkansas cast paper ballots, while others vote using DRE machines.[195] Some voting machines in the state are DRE machines with VVPR, while others are paperless DRE machines.[196]

Post-election audits: Unsatisfactory

- State law does not require post-election audits.[197]

Ballot accounting and reconciliation: Unsatisfactory

- All ballots are accounted for at the precinct level.[198]

- Precincts using optical scan machines are required by law to compare the number of ballots cast with the number of voters who signed into the polling place.[199] It is unclear whether the same is true of jurisdictions using DRE machines.[200]
- Counties are required to compare and reconcile DRE and paper return totals to countywide election records.[201]
- Counties review and account for all voting machine memory cards or flash drives to ensure they have been properly loaded onto the tally server at the county level.[202]
- For jurisdictions that use DRE machines, all results are posted at polling sites.[203] For jurisdictions using paper ballots and optical scanners, the law merely states that the results must be made public, without going into specifics.[204]

Paper absentee ballots: Fair

- The state does not permit voters—including UOCAVA voters—to submit completed ballots electronically. All ballots must be returned by mail or delivered in person.[205]

Voting machine certification requirements: Fair

- Before being purchased and used for any election in the state, all voting machines must be certified by a federal agency or undergo testing by a federally accredited laboratory.[206]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[207]

Arkansas has funding plans in place that would allow the state to replace its voting machines.[208]

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[209]
- Testing is open to the public.[210]
- Testing is carried out at least seven days before voting begins.[211]

California

Although California adheres to a number of minimum cybersecurity best practices related to voter registration systems and uses paper ballots and machines that produce an auditable paper record, the state's post-election audits are lacking important criteria. For example, the audits do not automatically escalate to include more ballots if necessary. Instead, escalation is within the discretion of election officials. Also, a law passed in 2017 will weaken the state's post-election audits by excluding provisional ballots from the auditing process. Adding to this is the fact that California allows voters stationed or living overseas to return voted ballots electronically, a practice that election security experts say is notoriously insecure. Its ballot accounting and reconciliation procedures also need improvement. California did receive points for requiring that all voting machines be tested against the EAC Voluntary Voting System Guidelines before they may be purchased or used in the state, and for requiring election officials to conduct pre-election logic and accuracy testing on all machines that will be used in an election. Los Angeles County's innovative "Voting System Assessment Project" is worth considerable recognition.[212]

To improve its overall election security, California should strengthen its post-election audit requirements by including all ballot types in the audit and basing the audit's scope on a statistically significant number tied to margins of victory. Given the threat posed by sophisticated nation-states and attempts to infiltrate U.S. elections, it is imperative that post-election audits be comprehensive enough to test the accuracy of election outcomes with a high degree of confidence and detect any possible manipulation. California should also require backup paper voter registration lists at polling places that use electronic poll books in case problems arise on Election Day. While this practice may already be carried out by some counties in the state, a statewide requirement would ensure uniformity and compliance. In addition, California should prohibit voters stationed or living overseas from returning voted ballots electronically. Going forward, all voted ballots should be returned by mail or delivered in person. The state can also strengthen its ballot

accounting and reconciliation procedures by explicitly requiring counties to compare and reconcile precinct totals with composite results to ensure they add up to the correct amount.

Minimum cybersecurity standards for voter registration system: Fair

- The state's voter registration system has been updated within the past 10 years.[213]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[214]
- The state's voter registration system has logging capabilities to track modifications to the database.[215]
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[216]
- The state performs regular vulnerability assessments on its voter registration system.[217]
- The state has enlisted DHS to help assess and identify potential threats to its voter registration system.[218]
- The state provides cybersecurity training to election officials.[219]
- Electronic poll books are used by some, but not all, jurisdictions in the state.[220] The state does not require polling places using electronic poll books to have backup paper copies of voter registration lists available in case of emergency.[221] The state requires jurisdictions using electronic poll books to perform pre-election testing on the equipment prior to an election.[222]

California Gov. Jerry Brown (D) has requested $134.3 million for new voting equipment as part of his 2018-2019 state budget.[223]

California Secretary of State Alex Padilla is a member of the U.S. Department of Homeland Security's Election Infrastructure Cybersecurity Working Group.[224]

Voter-verified paper audit trail: Fair

Depending on the jurisdiction, some voters in California cast paper ballots and others vote using DRE machines with VVPR, though most jurisdictions vote using paper ballots.[225]

Post-election audits: Mixed

- The state conducts mandatory post-election audits.[226]
- The state's post-election audits are conducted through manual hand count.[227]
- Audits consist of testing 1 percent of precincts in addition to one precinct for each race not included in the randomly selected precincts.[228]
- The precincts included in the audit are randomly selected.[229]
- Provisional ballots are no longer included in post-election audits.[230]
- Additional precincts may be included in the audit upon discretion of election officials.[231]
- Audits are open to the public.[232]
- Audits are conducted prior to certification.[233]
- Audit results can reverse the preliminary outcome of an audited contest if an error is detected.[234]

Ballot accounting and reconciliation: Unsatisfactory

- All ballots are accounted for at the precinct level.[236]
- Precincts are required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[237]
- Counties are not explicitly required to reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[238]
- There is no statutorily mandated review process to ensure that all voting machine memory cards have been properly loaded onto the tally server at the county level.[239]
- While state law requires that election results be made public, it is unclear whether the same is true of information regarding ballot reconciliation processes and results.[240]

Assembly Bill 840, which was passed by the California legislature in 2017 and signed by Gov. Jerry Brown, will weaken California's post-election audit procedures by excluding provisional ballots from inclusion in post-election audits.[235]

Paper absentee ballots: Unsatisfactory

- The state permits UOCAVA voters to submit completed ballots electronically via fax.[241]

Voting machine certification requirements: Fair

- Before being purchased and used for an election, all voting machines must be shown to meet or exceed federal voting system standards.[242]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[243]

Los Angeles is in the process of developing its own unique voting system. The project, known as the "Voting System Assessment Project," is aimed at building a voting machine that is accessible, secure, and customizable for modern-day voting.[244] The development process has involved interviews with voters, focus groups, and community workshops for the purposes of designing a system that is both efficient and effective from the voters' perspective.[245] The voting machine will create hard paper copies of all voted ballots that can later be used in post-election audits.[246]

Pre-election logic and accuracy testing: Fair

- Election officials are required to perform logic and accuracy testing on all voting machines prior to an election.[247]
- Testing is open to the public.[248]
- Testing begins at least seven days before an election.[249]

Colorado

Colorado receives a **B**

Colorado earned high marks in the three most important categories, but the fact that it allows electronic absentee voting undermines these practices in certain respects. Colorado receives kudos for being the first state in the nation to carry out mandatory risk-limiting audits. But even though Colorado's post-election audit procedures are "good," the fact that the state allows some electronic absentee voting undermines the overall effectiveness of these audits. Voted ballots that are submitted electronically via email, for example, cannot be properly audited because there is a low degree of confidence in electronically submitted ballots, as they are vulnerable to manipulation. In addition to carrying out its elections with paper ballots, post-election audits, and adherence to a number of minimum cybersecurity best practices related to voter registration systems, Colorado earned points for requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines prior to being purchased and used in the state. The fact that the state requires election officials to carry out pre-election logic and accuracy testing on all machines that will be used in an upcoming election is also commendable.

To improve its overall election security, Colorado should require that backup paper voter registration lists be made available at vote centers that use electronic poll books on Election Day in case of emergency. While we were told that many counties do this in practice, a statewide requirement would ensure uniformity and compliance. Colorado uses vote centers, where a person can vote at any site in the state, and has same day registration, voter access modernization policies that CAP supports. These provisions may require specially designed procedures for providing paper backup voter registration lists at places using electronic poll books as failsafes, should electronic poll books become inaccessible. Finally, Colorado should prohibit voters stationed or living overseas from returning voted ballots electronically. Regardless of the state's secure ballot return system for electronically voted ballots, we recommend that all voted ballots be returned by mail or delivered in person.

Minimum cybersecurity standards for voter registration system: Fair

- The state's voter registration system has been updated within the past 10 years.[250]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[251]
- The state's voter registration system has logging capabilities to track modifications to the database.[252]
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[253]
- The state performs regular vulnerability assessments and penetration testing on its voter registration system.[254]
- The state has enlisted DHS to help assess and identify potential threats to its voter registration system.[255]
- All election administrators—at the state, local, and municipal levels—receive cybersecurity training prior to using the state's voter registration system and receive ongoing training quarterly.[256]
- A single electronic poll book, which is built into the state's voter registration database, is used at all vote centers in Colorado and is tested prior to each election.[257] Paper voter registration lists are not required to be made available at vote centers on Election Day.[258] Many counties do provide backup paper lists in practice, but there is no requirement that they do so. Colorado has established contingency plans in case of emergency; In the event of an electronic poll book failure, all voters would shift to provisional ballots, which would be checked against the voter registration system once it is restored.[259]

Colorado offers anti-malware endpoint protection software—at no cost to users of the state voter registration system—to monitor and defend against Election Day attacks. The state purchased the software from a third-party vendor and then customized it to fits its unique needs.[260]

Voter-verified paper audit trail: Good

- The state is a vote-by-mail state, meaning that most votes are cast using paper ballots.[261] The state's vote centers house a limited number of DRE machines with VVPR.[262]

Colorado is the first state in the nation to require risk-limiting audits after every election.

Post-election audits: Good

- The state conducts mandatory post-election audits.[263]
- The state's post-election audits are conducted through manual hand count.[264]
- The state was the first in the nation to carry out mandatory risk-limiting audits, beginning in 2017.[265] The number of ballots included in the audit is determined by a statistical formula based on the likelihood that a change in the outcome of a race would lead to a new winner.[266]
- The ballots included in the audit are randomly selected.[267]
- All categories of ballots—regular, early voting, absentee, provisional, and UOCAVA—are eligible for auditing.[268]

- If discrepancies are discovered in an initial audit, the audit escalates to include a fresh set of ballots that are subjected to testing.[269] If discrepancies continue and are significant enough that they could lead to a potential change in outcome, a full hand count of ballots is conducted.[270]
- Audits are open to public observance and the results are made publicly available.[271]
- Audits, which may take several days to complete, begin 13 days after a primary election and 17 days after all other elections, prior to certification.[272]
- An audit can reverse the preliminary outcome of an audited contest if an error is detected.[273]

* *Although Colorado's post-election audit procedures are good, the state's allowance of electronic absentee voting undermines the audits' overall effectiveness.*

Ballot accounting and reconciliation: Fair

- Because the state is a vote-by-mail state, it is not necessary that all ballots be accounted for at the precinct level, specifically. There is a precinct-level accounting of all ballots by counties, conducted on a central count rather than a precinct count.[274]
- Because the state is a vote-by-mail state, it is not necessary that the number of ballots be compared to the number of voters at the precinct level, specifically. Vote centers do not reconcile by precinct. Instead, county offices reconcile the number of ballots with the number of voters who signed in at the polling place for each vote center.[275]
- Central count centers are required to compare and reconcile vote center totals with countywide results to ensure that they add up to the correct amount.[276]
- Central count centers are required to review and account for all voting machine memory cards and flash drives to ensure that they have been properly loaded onto the tally server.[277]
- The state requires that all election results and reconciliation procedures be made public.[278]

Paper absentee ballots: Unsatisfactory

- The state permits UOCAVA voters to submit completed ballots electronically, via email or fax. Colorado's secure ballot return portal allows eligible voters stationed or living overseas to upload their voted ballots onto the portal, after which time county officials log on to retrieve the ballots. We are told that only 0.006 percent of ballots are received electronically.[279]

Voting machine certification requirements: Fair

- **Before being purchased and used for any election in the state, all voting machines must undergo testing by a federally accredited laboratory.[280]**
- Two counties in Colorado still use voting machines that were purchased more than a decade ago.[281] However, both counties are scheduled to purchase new equipment for use in the 2020 elections.

Voting system vendors are required by state law to notify the secretary of state of any software incident no later than 72 hours after a software incident has occurred.[282]

Pre-election logic and accuracy testing: Fair

- **Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[283]**
- Testing is open to the public.[284]
- Testing is carried out at least 18 days before an election.[285]

Connecticut

Connecticut adheres to a number of minimum cybersecurity best practices related to voter registration systems and conducts its elections with paper ballots, but its post-election audits lack important criteria. Currently, the number of voting districts included in the state's audits is tied to a fixed percentage—5 percent—regardless of the margin of victory, while absentee ballots counted at central locations are excluded entirely from the auditing process. In addition, audits may be carried out through electronic automated retabulation, which is vulnerable to manipulation by hackers. Connecticut did earn points for its ballot accounting and reconciliation procedures and for prohibiting voters stationed or living overseas from returning voted ballots electronically, a practice that election security experts say is notoriously insecure. In Connecticut, all voted ballots are returned by mail or delivered in person. The state also exercises good practices by requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines before being purchased or used in the state, and by requiring election officials to carry out pre-election logic and accuracy testing on all machines that will be used in an upcoming election.

To improve its overall election security, Connecticut must refine its post-election audits by requiring the number of ballots included in an audit to be tied to a statistically significant number based on the margin of victory between one or more ballot races; ensuring that all ballot types are included in audits; and requiring that all audits be carried out through manual hand count. Given the threat posed by sophisticated nation-states seeking to disrupt U.S. elections, it is imperative that post-election audits test the accuracy of election outcomes and detect any possible manipulation.

Minimum cybersecurity standards for voter registration system: Fair

- The state's voter registration system is estimated to be at least 10 years old.[286]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[287]
- The state's voter registration system has logging capabilities to track modifications to the database.[288]

- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[289]
- The state performs regular vulnerability assessments on its voter registration system.[290]
- The state has enlisted DHS to help assess and identify potential threats to its voter registration system.[291]
- The state does not provide cybersecurity training to election officials.[292]
- While the state has authorized the study of electronic poll books, Secretary of the State Denise W. Merrill has not permitted their use based on product reviews done by the Center for Voting Technology at the University of Connecticut.[293]

Voter-verified paper audit trail: Good

- Elections are carried out using paper ballots and optical scan machines.[294]

Post-election audits: Mixed

- The state conducts mandatory post-election audits.[295]
- The state's poste-election audits may be conducted by manual hand count or electronically through automated retabulation.[296]
- A minimum of 5 percent of voting districts are included in an audit.[297] The precise number of ballot contests to be tested depends on the election. For example, for a presidential election, at least three offices must be audited, including "all offices required to be audited by federal law" plus one additional office randomly selected by the secretary of state.[298] In a municipal election, three offices or 20 percent of the total number of offices on the ballot—whichever is greater—are audited.[299]
- The voting districts and ballot contests included in the audit are randomly selected.[300]
- Absentee ballots counted at central locations are not included in audits, while absentee ballots counted at the voting districts are included in audits.[301]
- An audit can escalate if a discrepancy arises between the initial audit results and preliminary outcome that could affect election results.[302]
- Audits are open to the public.[303]
- Audits must be carried out no earlier than 15 days after an election, but no later than two days before election results are certified.[304]
- If a tabulating error is found to have occurred, another machine would likely be tested.[305] If the problem persists, audit results could reverse preliminary outcomes.[306]

Ballot accounting and reconciliation: Fair

- All ballots are accounted for at the precinct level.[307]
- Precincts are required to compare and reconcile the number of ballots used and the number of voters who signed into the polling place.[308]
- Municipalities are required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[309]
- The state does not use a tally server. As such, a memory card review process is unnecessary.[310]
- The state requires that election results and ballot reconciliation processes and information be made public.[311]

Paper absentee ballots: Fair

- The state does not permit voters—including UOCAVA voters—to submit completed ballots electronically. All ballots must be returned by mail or delivered in person.[312]

Voting machine certification requirements: Fair

- Before they may be purchased and used in the state, all voting machines must be certified by the Election Assistance Commission.[313]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[314]

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[317]
- Testing is open to the public.[318]
- Testing occurs 10 days before an election.[319]

The state maintains a close partnership with the University of Connecticut's Center for Voting Technology and Research (VoTeR Center), which provides the state with "in-house" testing and IT support for election machines and equipment.[315] The center also has conducted pre-election and post-election random audits of the memory cards used in every primary and election.[316] State officials have found this partnership valuable for several reasons, including the fact that university staffers who conduct voting system testing are intimately familiar with Connecticut's election process, which allows them to make practical assessments of equipment usage and functionality.

Delaware

Delaware allows voting using machines that do not provide a paper record and fails to mandate post-election audits, which does not provide confirmation that ballots are cast as the voter intends and counted as cast. The state's ballot accounting and reconciliation procedures also need improvement, and the fact that Delaware allows some absentee voters to return voted ballots electronically leaves its elections vulnerable to manipulation. The state did earn points for adhering to recommended cybersecurity best practices related to voter registration systems, including requiring cybersecurity training for election officials. Delaware also exercises good practices by requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines prior to being purchased or used in the state, and by requiring election officials to carry out pre-election logic and accuracy testing on all machines that will be used in an upcoming election.

To improve its overall election security, Delaware should stop using paperless DRE machines that leaves the state vulnerable to cyberattacks and prevents it from carrying out meaningful post-election audits to confirm the accuracy of election results. It is encouraging that the state is currently seeking bids to replace all voting machines by 2020 and also is looking at potentially switching over to a system that produces a voter-verified paper audit trail. By switching to a paper-based voting system and carrying out robust post-election audits—ideally risk-limiting audits—that test the accuracy of election outcomes, Delaware can drastically improve the security of its elections. Additionally, Delaware should strengthen its ballot accounting and reconciliation procedures by requiring that all ballots—used, unused, and spoiled—be accounted for at polling places. Part of this involves comparing and reconciling the number of ballots with the number of voters who signed in at a given polling place, among other things. Finally, the state should prohibit voters stationed or living overseas from returning voted ballots electronically, as the electronic return of voted ballots is a practice warned by election security experts as notoriously insecure.

Minimum cybersecurity standards for voter registration system: Good

- The state's voter registration system is estimated to be at least 10 years old.[320]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[321]
- The state's voter registration system has logging capabilities to track modifications to the database.[322]
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[323]
- The state performs regular vulnerability assessments on its voter registration system.[324]
- The state has enlisted DHS to help assess and identify potential threats to its voter registration system.[325]
- The state provides cybersecurity training to election officials.[326]
- The state does not use electronic poll books, and therefore was not graded on e-pollbook best practices.[327]

Delaware is reportedly in the process of moving its outdated voter registration database onto a more updated platform.[328]

Voter-verified paper audit trail: Unsatisfactory

- Elections are carried out using paperless DRE machines.[329]

Post-election audits: Unsatisfactory

- Delaware does not carry out mandatory post-election audits that confirm the accuracy of election outcomes. Instead, the state conducts a hand-to-eye review of DRE machine results as part of its official canvassing process.[330] That process occurs two days after Election Day.[331] If discrepancies of 0.5 percent or more is discovered, further investigation is required and absentee ballots may be hand counted to confirm results.[332] After certification, counties can decide to conduct their own review, but there is no requirement that they do so.[333]

Ballot accounting and reconciliation: Unsatisfactory

- Some ballot accounting is conducted at the precinct level, but some is conducted at the county level.[334]
- Precincts are not required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[335]
- Counties are required to review and account for precinct totals with countywide results to ensure that they add up to the correct amount.[336]
- Counties are required to review account for all voting machine memory cards or flash drives to ensure they have been properly loaded onto the tally server.[337]
- State law requires that election results be made public, and while information regarding ballot reconciliation processes and results is not published on the state's website, it is available upon request.[338]

Paper absentee ballots: Unsatisfactory

- The state permits UOCAVA voters and those with disabilities to return voted ballots electronically, via email and fax.[339]

Voting machine certification requirements: Fair

- Before being purchased and used for an election, all voting machines must be shown to meet or exceed federal voting system standards.[340]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[341] However, we are told that Delaware is in the process of seeking bids to update and replace all voting systems in time for the 2020 elections.[342] As part of the bidding process, the state will consider voting systems that produce a voter-verified paper audit trail.[343]

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[347]
- Testing is open to the public.[348]
- Testing occurs within five days before an election.[349]

Delaware is in the process of seeking bids to update and replace all voting systems in time for the 2020 electionas.[344] As part of the bidding process, the state will consider voting systems that produce a voter-verified paper audit trail.[345]

"[W]e are in the RFP process of the potential purchase of new voting machines, electronic poll books and a new absentee system."[346]

District of Columbia

The District of Columbia adheres to minimum cybersecurity best practices for voter registration systems and conducts its elections with paper ballots. However, the number of ballots included in post-election audits are based on a fixed percentage rather than a statistically significant number tied to the margin of victory in one or more ballot contests. The district also allows voters stationed or living overseas to return voted ballots electronically, a practice that election security experts say is notoriously insecure. Its ballot accounting and reconciliation procedures also need improvement. The district did earn points for requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines before being purchased or used in the state, and for requiring election officials to conduct pre-election logic and accuracy testing on all machines that will be used in an upcoming election.

To improve the overall security of its elections, the district should update its post-election audit requirements to ensure that the number of ballots included be based on a statistically significant number tied to the margin of victory in one or more ballot contests rather than a fixed amount. Given the threat posed by sophisticated nation-states seeking to disrupt U.S. elections, it is imperative that post-election audits test the accuracy of election outcomes and detect any possible manipulation. The district should also strengthen its ballot accounting and reconciliation procedures. For example, precincts—not central counting centers—should be responsible for comparing and reconciling the number of ballots and number of voters who signed into a given polling place. Finally, the district should prohibit voters stationed or living overseas from returning voted ballots electronically. Going forward, all voted ballots should be returned by mail or delivered in person.

Minimum cybersecurity standards for voter registration system: Good

- The district's voter registration system is at least 10 years old.[350]
- The district's voter registration system provides access control to ensure that only authorized personnel have access to the database.[351]
- The district's voter registration system has logging capabilities to track modifications to the database.[352]

- The district's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[353]
- The district performs regular vulnerability assessments on its voter registration system.[354]
- The district has enlisted DHS to help assess and identify potential threats to its voter registration system.[355]
- The district provides cybersecurity training to election officials.[356]
- Electronic poll books are used throughout the district.[357] The district conducts pre-election testing on electronic poll books prior to an election.[358] Paper voter registration lists are available at polling places that use electronic poll books on Election Day.[359]

Voter-verified paper audit trail: Good

- Elections are carried out using paper ballots and optical scan machines.[360]

Post-election audits: Fair

- The district conducts mandatory post-election audits.
- The district's post-election audits are conducted through manual hand count.[361]
- Audits include at least 5 percent of precincts with precinct-level vote tabulation machines and at least 5 percent of the voter-verified paper records that are tabulated centrally.[362] Of the ballot contests to be tested, at least one must be a District-wide contest and at least two must be ward-wide races.[363] The Board of Elections can audit additional precincts, voter-verified paper records, or contests if it so chooses.[364]
- The precincts chosen for an audit are selected randomly.[365]
- All categories of ballots—regular, early voting, absentee, provisional, and UOCAVA—are eligible for auditing.[366]
- If an audit initially reveals a discrepancy that yields an error rate greater than 0.25 percent or 20 percent of the margin of victory—whichever is less—a second count is conducted.[367] If that audit also reveals a discrepancy, a randomly selected precinct in each ward where the particular ballot contest was voted on is audited, along with an additional 5 percent of centrally tabulated ballots.[368] If a discrepancy of more than 0.25 percent or 20 percent of the margin of victory—whichever is less—arises from that audit, all relevant precincts and centrally tabulated ballots are audited.[369]
- Audits are open to the public and the results are made publicly available.[370]
- Audits are carried out prior to certification of the official election results.[371]
- An audit can reverse the preliminary outcome of an audited contest if an error is detected.[372]

Ballot accounting and reconciliation: Unsatisfactory

- All ballots are accounted for at the precinct level.[373]
- Although poll workers are required to record the number of ballots and voters who signed in at the polling place, they are not required to compare or reconcile the two numbers.[374] That process is conducted at the central counting location.[375]
- Workers at the central counting location compare and reconcile polling place vote totals and central vote counts.[376]
- There is no statutorily mandated review process at the central counting location to ensure that all voting machine memory cards and flash drives have been properly loaded onto the tally server.[377]
- While the district requires that election results be made public, it does not require information regarding ballot reconciliation processes and results to be made publicly available.[378]

Paper absentee ballots: Unsatisfactory

- The district allows UOCAVA voters to deliver completed ballots electronically, via email or fax.[379]

Voting machine certification requirements: Fair

- Before being purchased and used for an election, all voting machines must be shown to meet or exceed federal voting system standards.[380]
- The district updated all of its voting machines in 2016.[381]

Washington, D.C., updated all of its voting machines in 2016.[382]

Pre-election logic and accuracy testing: Fair

- The district conducts mandatory logic and accuracy testing on all voting machines prior to an election.[383]
- Testing is open to the public.[384]
- District law does not specify when testing must be carried out.

Florida

Florida allows voting using machines that do not provide a paper record and fails to mandate robust post-election audits that test the accuracy of election outcomes, which does not provide confirmation that ballots are cast as the voter intends and counted as cast. Currently, post-election audits may be conducted by electronic automated retabulation, which is vulnerable to hacking. Moreover, the scope of an audit is tied to a fixed percentage rather than a statistically significant number based on the margin of victory in one or more ballot contests. Also problematic is the fact that audits are carried out after certification and are not binding on election outcomes even if they are found to be erroneous. Adding to this is the fact that voters stationed or living overseas are permitted to return voted ballots electronically by fax, a practice warned by election security experts as notoriously insecure. Furthermore, state law does not explicitly require voting machines to be tested to EAC Voluntary Voting System Guidelines before being purchased or used in the state. Its ballot accounting and reconciliation procedures also need improvement. Florida did earn points for requiring election officials to carry out logic and accuracy testing on all voting machines that will be used in an upcoming election.

Despite numerous attempts to speak to someone in state government about the cybersecurity standards for the state's voter registration system, state officials told us they would not provide information or comment on our research; the state receives an incomplete, as we were unable to locate all the information for the category independently. Even if Florida is adhering to all of the minimum cybersecurity best practices for voter registration systems its overall grade would not change, given the point distribution for the other categories.

To improve its overall election security, Florida should stop using paperless DRE machines and strengthen its post-election audit requirements. Florida's elections will remain vulnerable to sophisticated nation-states so long as jurisdictions continue using voting machines that do not provide a paper record and the state fails to carry out robust post-election audits that test the accuracy of election outcomes. By requiring statewide use of paper ballots and strengthening its

post-election audit procedures, the security of Florida's elections could be greatly improved. Florida should also explicitly require all voting machines to be tested to EAC Voluntary Voting System Guidelines prior to being purchased and used in the state. Even if all voting machines are currently EAC-certified, this requirement should be codified by law for future purchases. Finally, regarding ballot accounting and reconciliation, officials at the county level should be required to compare and reconcile precinct totals with composite results to confirm that they add up to the correct number.

Minimum cybersecurity standards for voter registration system: Incomplete

**State officials told us they would not participate in our research and therefore were unable to provide us information on cybersecurity requirements for the state's voter registration system. Information gathered for this section derives from independent research.*

- The state's voter registration system is estimated to be at least 10 years old.[385]
- The state's voter registration system provides access control to ensure that only authorized personnel can access the database.[386]
- State officials were unable to provide us with information on whether the state's voter registration system has logging capabilities to track modifications to the database.
- State officials were unable to provide us with information on whether the state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.
- The state performs regular vulnerability assessments on its voter registration system.[387]
- The state has enlisted DHS to help assess and identify potential threats to its voter registration system and election infrastructure.[388]
- State officials were unable to provide us with information on whether the state provides cybersecurity training to election officials.
- Electronic poll books are used by some, but not all, jurisdictions in the state.[389] Some localities provide backup paper copies of voter registration lists at polling places that use electronic poll books, while others are entirely paperless.[390] Pre-election testing of electronic poll books is left up to the counties that use them.[391]

In his 2018-2019 budget, Florida Gov. Rick Scott (R) requested nearly $2.4 million for cybersecurity requirements aimed at protecting election systems and software from potential attacks.[392] Gov. Scott requested $1.9 million in grant funding to be set aside for election officials to monitor security threats and suspicious activity.[393] Gov. Scott also requested nearly $500,000 to hire employees for a new cybersecurity unit, which will be focused on elections along with other "critical" systems and be housed within the Department of State.[394]

Voter-verified paper audit trail: Unsatisfactory

- Depending on the jurisdiction, some voters in Florida cast paper ballots, while others vote using paperless DRE machines.[395]

Post-election audits: Unsatisfactory

- While Florida conducts a form of post-election review, its use of paperless DRE machines prevents it from carrying out audits that can confirm the accuracy of election outcomes.
- The audit may be conducted by manual hand count or electronically through automated retabulation.[396] The process differs slightly depending on the method.
- A manual audit consists of a hand count of the votes cast in one randomly selected ballot contest.[397] Such audits include at least 1 percent but no more than 2 percent of precincts.[398] An automated audit consists of a retabulation of votes cast across every ballot contest.[399] Such audits include at least 20 percent of precincts.[400]
- The precincts included in the audit are randomly selected.[401]
- All categories of ballots—regular, early voting, absentee, provisional, and UOCAVA—are eligible for auditing.[402]
- There is no statutory requirement that an audit escalate in the event that preliminary outcomes are found to be incorrect.
- Audits are open to the public and results are made public within seven days following certification.[403]
- Audits take place after certification of the official election results.[404]
- There is no statutory requirement on whether an audit can reverse election results if an error is detected.[405]

Ballot accounting and reconciliation: Unsatisfactory

- All ballots are accounted for at the precinct level.[406]
- Precincts are required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[407]
- Counties are not explicitly required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[408]
- There is no statutorily mandated review process at the county level to ensure that all voting machine memory cards have been properly loaded onto the tally server.[409]
- The state requires that all election results and reconciliation procedures be made public.[410]

Paper absentee ballots: Unsatisfactory

- Florida permits UOCAVA voters to submit completed ballots electronically via fax.[411]

Voting machine certification requirements: Unsatisfactory

- The state does not require voting machines to meet federal requirements before they are purchased and used in elections in the state.[412]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[413]

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[414]
- Testing is open to the public.[415]
- Testing occurs within 10 days before early voting begins.[416]

Georgia

Although Georgia adheres to a number of minimum cybersecurity best practices for voter registration systems, its practice of voting using machines that do not provide a paper record and its failure to mandate post-election audits do not provide confirmation that ballots are cast as the voter intends and counted as cast. The state did earn points for prohibiting absentee voters from returning voted ballots electronically, a practice that election security experts say is notoriously insecure. In Georgia, all voted ballots are returned by mail or delivered in person. The state also exercises good practices by requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines before being purchased or used in the state and for its ballot accounting and reconciliation procedures. Additionally, Georgia requires election officials to conduct pre-election logic and accuracy testing on all machines that will be used in an upcoming election.

To improve its overall election security, Georgia should switch over to a paper-based voting system and require mandatory post-election audits that test the accuracy of election results after every election. Encouragingly, a new piece of bipartisan legislation would require paper ballots and establish risk-limiting audits. The state should also work alongside DHS for the purposes of identifying and assessing vulnerabilities in its voter registration system. While recognizing the importance of state autonomy when it comes to elections, federal agencies with expertise in cybersecurity and access to classified information on contemporaneous cyberthreats have the personnel and resources necessary to thoroughly probe and analyze complex election databases, machines, and cybervulnerabilities. By combining their expertise on cyberthreats and their insight into the unique qualities of localized election infrastructure, state and federal officials can better assess and deter attempts at electoral disruption. These provisions, if implemented correctly, would significantly affect the security of Georgia's elections.

Minimum cybersecurity standards for voter registration system: Fair

- The state implemented a new voter registration system in 2013.[417]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[418]

- The state's voter registration system has logging capabilities to track modifications to the database.[419]
- The state's voter registration system is protected by an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[420]
- The state performs regular vulnerability assessments on its voter registration system.[421]
- The state has not enlisted DHS to help assess and identify potential threats to its voter registration system.[422]
- The state provides cybersecurity training to election officials.[423]
- Electronic poll books are used statewide in Georgia.[424] The state conducts pre-election testing on electronic poll books prior to an election.[425] Paper voter registration lists are available at polling places that use electronic poll books on Election Day.[426]

Georgia implemented a new voter registration system in 2013.[427]

In addition to conducting its own vulnerability testing on its voter registration system, Georgia also contracts with third-party vendors to conduct regular vulnerability assessments that include penetration testing.[428]

Voter-verified paper audit trail: Unsatisfactory

- Elections are carried out using paperless DRE machines.[429]

Post-election audits: Unsatisfactory

- State law does not require post-election audits.

Ballot accounting and reconciliation: Fair

- All ballots are accounted for at the precinct level.[432]
- Precincts are required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[433]
- Counties are required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct number.[434]
- There is no statutorily mandated review process to ensure that all voting machine memory cards have been properly loaded onto the tally server at the county level.[435] However, the election management software that tabulates results provides a warning if all memory cards that were created for the election are not properly uploaded.[436]
- The state requires that all election results and reconciliation procedures be made public.[437]

Bipartisan legislation would require that paper ballots be used statewide in Georgia and provide for post-election risk-limiting audits.[430]

"I think it is important that we have a paper ballot trail that ensures that accuracy is there, and that there are no games that potentially could be played."
—Lt. Gov. Casey Cagle (R)[431]

Paper absentee ballots: Fair

- The state does not permit voters—including UOCAVA voters—to submit completed ballots electronically. All ballots must be returned by mail or delivered in person.[438]

Voting machine certification requirements: Fair

- Before they may be purchased and used in the state, all voting machines must be certified by the Election Assistance Commission.[439]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[440]

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[441]
- Testing is open to the public.[442]
- Testing occurs at least three days before an election.[443]

Hawaii

Although Hawaii conducts its elections using paper ballots and voting machines that provide a paper record, its post-election audits lack important criteria. Currently, the number of ballots included in an audit is based on a fixed percentage—10 percent of precincts using electronic voting systems—rather than a statistically significant number tied to the margin of victory in one or more ballot contests. Also, the results of the audit are only made public upon request. Adding to this is the fact that Hawaii allows absentee voters to return voted ballots electronically, a practice that election security experts say is notoriously insecure Moreover, pre-election logic and accuracy testing is left to the discretion of local election officials. Unfortunately, state officials—citing legal reasons—refused to provide us with information on cybersecurity standards for the state's voter registration system and we were unable to locate much of the information independently. If Hawaii is adhering to all of the minimum cybersecurity best practices for voter registration systems, it would receive a "good" score—worth 3 points—for that category, bringing its grade up to a C. Hawaii did earn points for requiring that all voting machines be tested against EAC Voluntary Voting System Guidelines before being purchased or used in the state.

To improve its overall election security, Hawaii would do well to tie the number of ballots included in an audit to a statistically significant number based on the margin of victory between one or more ballot contests, and automatically make audit results public in the interest of transparency. Hawaii should also require that all voting machines undergo logic and accuracy testing prior to an election rather than leaving the number of machines tested to the discretion of election officials. The state can also strengthen its ballot accounting and reconciliation procedures by requiring election officials at individual polling places to account for all ballots—used, unused, and spoiled—on election night. Part of this involves comparing the number of ballots to the number of people who signed into the polling place. Finally, the state should prohibit absentee voters—including UOCAVA voters—from returning voted ballots electronically. Going forward, all voted ballots should be returned by mail or delivered in person.

Minimum cybersecurity standards for voter registration system: Incomplete

**State officials –citing legal reasons—refused to share information on cybersecurity requirements for the state's voter registration system. Information gathered for this section derives from independent research. If Hawaii does require the missing cybersecurity best practices, its grade would be raised from a D to a C.*

- The state migrated to a new voter registration system in 2017.[444]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[445]
- State officials were unable to provide us with information on whether the state's voter registration system has logging capabilities to track modifications to the database.
- State officials were unable to provide us with information on whether the state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.
- State officials were unable to provide us with information on whether the state performs regular vulnerability assessments on its voter registration system.
- State officials were unable to provide us with information on whether the state has enlisted the National Guard or DHS to help assess and identify potential threats to its voter registration system.
- State officials were unable to provide us with information on whether the state provides cybersecurity training for election officials.
- The state does not use electronic poll books, and therefore was not graded on e-pollbook best practices.[446]

Hawaii migrated to a new voter registration system in 2017.[447]

Voter-verified paper audit trail: Fair

- Depending on the jurisdiction, some voters in Hawaii cast paper ballots, while others vote using DRE machines with VVPR.[448]

Post-election audits: Fair

- The state conducts mandatory post-election audits.[449]
- The state's post-election audits are conducted through manual hand count.[450]
- Audits are conducted on at least 10 percent of precincts.[451]
- The precincts included in the audit are randomly selected.[452]
- All categories of ballots—regular, early voting, absentee, provisional, and UOCAVA—are eligible for auditing.[453]
- An audit escalates in the event that preliminary outcomes are found to be incorrect.[454]
- Audit results are publicly available upon request.[455]

- Audits are carried out on Election Day before certification of official election results.[456]
- An audit can reverse the preliminary outcome of an audited contest if an error is detected.[457]

Ballot accounting and reconciliation: Unsatisfactory

- Ballots are not fully accounted for at the precinct level. Some ballot accounting procedures occur at the polling place, while others occur at the central counting center.[458]
- Precincts are not required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[459] That process takes place at the central counting center.
- After an election, central counting centers compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[460]
- Counting centers review and account for all voting machine memory cards to ensure that they have been properly loaded onto the tally server.[461]
- The state requires that all election results and reconciliation procedures be made public.[462]

Paper absentee ballots: Unsatisfactory

- In addition to UOCAVA voters, all permanent absentee voters who do not receive a mailed ballot within five days of the election are permitted to submit completed ballots electronically, via email.[463]

Voting machine certification requirements: Fair

- Before they may be purchased and used in the state, all voting machines must be certified by the Election Assistance Commission.[464]
- All voting machines in Hawaii have been replaced within the past 10 years.[465]

Pre-election logic and accuracy testing: Unsatisfactory

- Election officials conduct logic and accuracy testing on at least some voting machines prior to an election.[466] The number of machines tested is left to the discretion of election observers, who are responsible for carrying out testing.[467]
- Testing is open to the public.[468]
- Tabulating machines used for counting absentee ballots must be tested one week before an election, while all other voting machines are tested one month before an election.[469]

Idaho

Idaho adheres to a number of minimum cybersecurity best practices related to voter registration systems and conducts its elections with paper ballots, but it fails to mandate post-election audits, leaving the state's elections vulnerable to potentially erroneous election outcomes that could go undetected and uncorrected. Idaho also allows absentee voters to return voted ballots electronically, a practice that election security experts say is notoriously insecure. Its ballot accounting and reconciliation procedures also need improvement. Idaho did earn points for requiring all voting machines to be tested to EAC Voluntary Voting System Guidelines before being used in the state and for requiring election officials to carry out pre-election logic and accuracy testing on all machines that will be used in an upcoming election.

To improve its overall election security, Idaho should immediately adopt robust post-election audit requirements that test the accuracy of election results. In doing so, the state should look to risk-limiting audits like those in Colorado as a potential model. Given the threat posed by sophisticated nation-states seeking to disrupt U.S. elections, it is imperative that post-election audits test the accuracy of election outcomes and detect any possible manipulation. Idaho should require cybersecurity training for election officials and prohibit electronic absentee voting, which has been deemed insecure by election security experts and federal entities. Going forward, all voted ballots should be returned by mail or delivered in person. Idaho's ballot accounting and reconciliation procedures can also be improved. For example, after comparing the number of ballots cast with the number of voters on the poll roster at polling places, poll workers should be required to reconcile any discrepancies if they occur.

Minimum cybersecurity standards for voter registration system: Fair

- The state's voter registration system is estimated to be at least 10 years old.[470]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[471]
- The state's voter registration system has logging capabilities to track modifications to the database.[472]

- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[473]
- The state performs regular vulnerability assessments on its voter registration system.[474]
- The state has enlisted DHS to help assess and identify potential threats to its voter registration system.[475]
- The state does not require election officials to receive cybersecurity training prior to elections.[476]
- The state permits the use of electronic poll books.[477] The state conducts pre-election testing on electronic poll books prior to an election and paper voter registration lists are available at polling places that use electronic poll books on Election Day.[478]

Voter-verified paper audit trail: Good

- Elections are carried out using paper ballots and optical scan machines.[479]

Post-election audits: Unsatisfactory

- The state does not require post-election audits.[480]

Ballot accounting and reconciliation: Unsatisfactory

- All ballots are accounted for at the precinct level.[481]
- While a comparison of the number of ballots cast and the number of voters on the poll roster is required at polling places, poll workers are not explicitly required to reconcile any discrepancies if they arise.[482]
- Counties are required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[483]
- The state does not use a tally server. As such, a memory card review process is unnecessary.[484]
- While state law requires that election results be made public, it is unclear whether the same is true of information regarding ballot reconciliation processes and results.[485]

Paper absentee ballots: Unsatisfactory

- The state allows some absentee voters to return completed ballots electronically, via email.[486]

Voting machine certification requirements: Fair

- Before being purchased and used for any election in the state, all voting machines must undergo testing by a federally accredited laboratory.[487]

- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[488]

Pre-election logic and accuracy testing: Fair

- **Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[489]**
- State law does not specifically require that testing be open to public observance, though public notice is required.[490]
- Testing is carried out between five and 10 days before an election.[491]

Illinois

Illinois adheres to a number of minimum cybersecurity best practices related to voter registration systems and has made system upgrades and made improvements in security protocols since its voter registration system was attacked in 2016. And while the state conducts its elections using paper ballots and voting machines that provide a paper record, the state's post-election audits lack important criteria. State law currently allows audits to be conducted electronically through automatic retabulation, which is vulnerable to hacking. In addition, the number of ballots included in an audit is tied to a fixed amount, regardless of the margin of victory in a ballot contest. The state's ballot accounting and reconciliation procedures also need improvement. Illinois did earn points for prohibiting voters from returning voted ballots electronically, a practice that election security experts say is notoriously insecure. Encouragingly, although the state does not currently provide cybersecurity training to election officials, it is working to develop an online training program, which will include a cybercomponent specific to election security. In addition to offering this training to election officials, the state plans to open the program to other local officials who often share facilities with election administrators. Illinois also exercises good practices by requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines before being purchased or used in the state and for requiring election officials to carry out pre-election logic and accuracy testing on all machines that will be used in an upcoming election.

To improve its overall election security, Illinois must strengthen its post-election audit requirements, adopting more comprehensive measures that test the accuracy of election outcomes. In doing so, the state should look to risk-limiting audits like those in Colorado as a potential model. Illinois should also require pre-election testing for electronic poll books in jurisdictions that use them to ensure that they are in good working order before Election Day. At the same time, backup paper voter registration lists must be made available at these locations in case of emergency. The state can also refine its ballot accounting and reconciliation requirements by requiring counties to compare and reconcile precinct totals with composite results to confirm they add up to the correct number. Precincts should be barred from removing excess voted ballots at random if discrepancies are found between the number of ballots and the number of voters who signed into a polling place.

Minimum cybersecurity standards for voter registration system: Mixed

- The state's voter registration system has been updated within the past 10 years.[492] The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[493]
- The state's voter registration system has logging capabilities to track modifications to the database.[494]
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[495] The state is upgrading its intrusion detection system to use the latest hardware and software.[496]
- The state performs regular vulnerability assessments on its voter registration system.[497]
- The state has enlisted DHS to help assess and identify potential threats to its voter registration system.[498]
- While the state does not currently provide cybersecurity training to election officials, it is working with another state agency to develop an optional online training program that will include a cybercomponent specific to election security.[499] In addition to offering the training to election officials, the state plans to open the program to other local officials who often share facilities with election administrators.[500]
- Electronic poll books are used by some, but not all, jurisdictions in Illinois.[501] Pre-election testing of electronic poll books is left up to the counties that use them.[502] Some counties provide backup paper copies of voter registration lists on Election Day, while others don't.[503]

The Department of Homeland Security performs weekly penetration tests on Illinois's voter registration system. Illinois has a membership with the Multi-State Information Sharing & Analysis Center.[504]

After learning it had been targeted by hackers in 2016, state officials reportedly took Illinois' entire voter registration system offline to identify potential problems and make necessary security upgrades.[505]

Voter-verified paper audit trail: Fair

- Depending on the jurisdiction, some voters in Illinois cast paper ballots, while others vote using DRE machines with VVPR.[506]

Post-election audits: Fair

- The state conducts mandatory post-election audits.
- For votes cast on DRE machines with VVPR, audits may be conducted by manual hand count or electronically through automated retabulation. For paper ballots, audits are conducted electronically through automated retabulation.[508]
- Audits are conducted on 5 percent of precincts in every election jurisdiction across the state, along with 5 percent of the voting devices used during early voting.[509]
- The precincts and devices included in the audit are randomly selected.[510]
- All categories of ballots—regular, early voting, vote by mail, provisional, and UOCAVA—are eligible for auditing.[511]
- State law requires that there be zero discrepancies between a post-election audit and the initial tally before election results can be certified. An audit can escalate if preliminary outcomes are found to be incorrect.[512]

- Audits are open to the public.[513]
- Audits must be carried out by local election officials prior to certification of election results, but the precise timing varies depending on the jurisdiction.[514] Illinois permits UOCAVA and vote-by-mail voters to submit ballots up to 14 days after an election, meaning that some jurisdictions wait to conduct their audits until after this 14-day deadline, while others begin conducting audits immediately after the preliminary outcomes are determined.[515]
- An audit can reverse the preliminary outcome of an audited contest if an error is detected.[516]

In December 2017, Noah Praetz, director of elections for Cook County, unveiled "2020 Vision: Election Security in the Age of Committed Foreign Threats," with recommendations for policymakers and election officials related to election security, including replacing paperless voting machines nationwide; collaboration between federal, state and local officials; conducting public audits; and putting in place certain cybersecurity measures.[507]

Ballot accounting and reconciliation: Unsatisfactory

- All ballots are accounted for at the precinct level.[517]
- Precincts are required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[518] However, to the extent that a discrepancy is found, the discrepancy is resolved by removing excess voted ballots at random in jurisdictions using optical scan machines.[519]
- Counties are not explicitly required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[520]
- There is no statutorily mandated review process to ensure that all voting machine memory cards have been properly loaded onto the tally server at the county level.[521]
- The state requires that all election results and reconciliation procedures be made public.[522]

Paper absentee ballots: Fair

- The state does not permit voters—including UOCAVA voters—to submit completed ballots electronically. All ballots must be returned by mail or delivered in person.[523]

Voting machine certification requirements: Fair

- Before being purchased and used for any election in the state, all voting machines must undergo testing by a federally accredited laboratory.[524]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[525]

Pre-election logic and accuracy testing: Fair

- The election authority conducts mandatory logic and accuracy testing on all voting machines prior to an election.[526]
- Testing is open to the public.[527]
- Testing is carried out at least five days before an election.[528]

Even before the public logic and accuracy testing, local election officials are tasked with inspecting election equipment to ensure that they meet eligibility standards. Additionally, officials from the Illinois State Board of Elections are authorized to design and carry out their own pre-election tests on voting machines in the state. In theory, then, a single voting machine could undergo three separate tests prior to an election. An estimated 10 percent of all voting machines underwent all three tests during the 2016 election cycle.[529]

Indiana

Indiana allows voting using machines that do not provide a paper record and fails to mandate robust post-election audits that test the accuracy of election outcomes, which leaves the state susceptible to hacking and manipulation by sophisticated nation-states. Unfortunately, state officials—citing security concerns—refused to provide us with information on whether the state is working with DHS to identify and assess vulnerabilities in its voter registration system. Even if Indiana is working with DHS, its overall grade would not be raised, given the point distribution for the other categories. For example, the state allows voters stationed or living overseas to return voted ballots electronically, a practice that election security experts say is notoriously insecure. In addition, the state only requires pre-election logic and accuracy testing for some voting machines, as opposed to all machines that will be used in an upcoming election. Indiana did receive points for requiring all voting machines to be tested to EAC Voluntary Voting System Guidelines before being purchased or used in an election.

To improve its overall election security, all jurisdictions should be required to use paper ballots in administering their elections and to carry out mandatory post-election audits that adequately test the accuracy of election outcomes. Encouragingly, we were told that the state is considering implementing risk-limiting audits for the 2018 elections.[530] Indiana should also require backup paper voter registration lists at any polling place that uses electronic poll books to check in voters. Currently, state law only requires backup electronic poll books to be available on Election Day at polling places where they are used. These electronic backups, however, will do nothing to ensure that eligible voters can cast ballots that count when they show up to the polls if there is widespread system failure or a major cyberbreach, which would corrupt the entire electronic database. Indiana should also prohibit electronic absentee voting and require that all voting machines that will be used in an upcoming election undergo pre-election logic and accuracy testing, rather than only testing a sampling of machines. Furthermore, Indiana can strengthen its ballot accounting and reconciliation procedures by requiring that all ballots—used, unused, and spoiled—be accounted for at polling places and by requiring jurisdictions using DRE machines to compare and reconcile the number of ballots with the number of voters who signed into the polling place.

Minimum cybersecurity standards for voter registration system: Incomplete

**The Indiana secretary of state's office declined to provide information regarding cybersecurity requirements for the state's voter registration system, citing increased security risks in doing so. Information gathered for this section derives from independent research and interviews with other election officials in Indiana.*

- The state's voter registration system is estimated to be at least 10 years old.[531]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[532]
- The state's voter registration system has logging capabilities to track modifications to the database.[533]
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[534]
- The state performs regular vulnerability assessments on its voter registration system.[535]
- State officials were unable to provide us with information on whether the state has enlisted the National Guard or DHS to help assess and identify potential threats to its voter registration system.
- The state has provided some cybersecurity training to election officials and is working toward developing more robust training opportunities for county-level officials who have access to the state's voter registration system.[536] At the Indiana Election Division's annual conference in 2017, the department set time aside for additional cybersecurity-related presentations.[537]
- Electronic poll books are used by some, but not all, jurisdictions in the state.[538] The state conducts pre-election testing on electronic poll books prior to an election.[539] Although state law requires that backup electronic poll books are available on Election Day at polling places where they are used, it does not require paper backup voter registration lists to be available.[540] Some counties that use electronic poll books do provide paper voter registration lists that election workers can refer to if necessary.[541]

Indiana is working toward developing more robust cybersecurity training opportunities for county officials with access to the state's voter registration system.[542]

At the Indiana Election Division's annual conference in 2017, the department set time aside for additional cybersecurity-related presentations.[543]

Indiana has received or is expected to receive additional funding for cybersecurity at their election agencies.[544]

Voter-verified paper audit trail: Unsatisfactory

- Depending on the jurisdiction, some voters in Indiana cast paper ballots, while others vote using paperless DRE machines.[545]

Post-election audits: Unsatisfactory

- Indiana's use of paperless DRE machines prevents it from carrying out audits that can confirm the accuracy of election outcomes. Even though post-election audits are not required in Indiana,[547] an audit on paper ballots may be requested by a county chairman for either of the major political parties.[548] Audits consist of 5 percent of precincts or five precincts—whichever is greater—and are only carried out in jurisdictions that use paper ballots.[549] For counties using paperless DRE machines, if the county election board determines that the total number of votes cast at a polling place differs from the number of voters who received a ballot at the polls or returned an absentee ballot by five or more an audit is carried out on that precinct.[550] The audit is carried out within 13 days after an election and is open to public observance.[551]
- The state is considering implementing risk-limiting audits for the 2018 elections.[552]

Legislation introduced in 2018 would prohibit jurisdictions from purchasing DRE voting machines after June 30, 2018. DRE machines would be phased out completely by December 31, 2022.[546]

Ballot accounting and reconciliation: Unsatisfactory

- Ballots are not fully accounted for at the precinct level.[554] For example, unused, uncounted, and defective ballots are not counted at polling places. They are simply gathered and returned to the county along with other voting materials.[555]
- Precincts using paper ballots are required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[556] No such requirements apply to jurisdictions using DRE machines.[557]
- Counties are required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[558]
- Counties are required to review and ensure that all voting machine memory cards have been properly loaded onto the tally server.[559]
- The state requires that all election results and reconciliation procedures be made public.[560]

Indiana is considering implementing risk-limiting audits for the 2018 elections.[553]

Paper absentee ballots: Unsatisfactory

- The state permits UOCAVA voters to submit completed ballots electronically, via email or fax.[561]

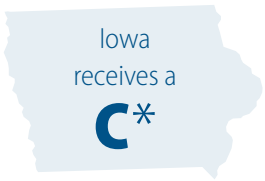
Voting machine certification requirements: Fair

- Before being purchased and used for an election, all voting machines must be shown to meet or exceed federal voting system standards.[562]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[563]

Pre-election logic and accuracy testing: Unsatisfactory

- Jurisdictions using DRE machines conduct mandatory logic and accuracy testing on at least some voting machines prior to an election.[564] DRE machines are tested in at least three randomly selected precincts in each county.[565] For jurisdictions using optical scan paper ballot cards, 10 percent of tabulating machines that will be used in the election and up to 15 percent of all tabulating machines are tested if an individual attending the public test requests additional machines to be tested.[566]
- Testing is open to the public.[567]
- Testing must take place at least 28 days before Election Day.[568]

Iowa



Iowa carries out its elections with paper ballots, but the state's post-election audit law is inadequate from an election security standpoint. The scope of the audits is based on a fixed number of counties and precincts rather than a statistically significant number tied to the margin of victory in one or more ballot contests. At the same time, the audits do not appear to include provisional ballots and there is no escalation requirement in the event that preliminary outcomes are found to be incorrect. Also problematic is the fact that audit results are not binding on the official election outcome, regardless of what they reveal. Adding to this is the fact that Iowa allows voters stationed or living overseas to return voted ballots electronically, a practice that election security experts say is notoriously insecure. The state did receive points for its ballot accounting and reconciliation procedures and for requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines before being purchased or used in the state. Election officials are also required to conduct logic and accuracy testing on all voting machines that will be used in an upcoming election.

Despite numerous attempts to speak to someone in state government about cybersecurity standards for the state's voter registration system, state officials told us they would not provide information or comment on our research, and we were unable to locate all of the information independently. Even if Iowa is adhering to all of the minimum cybersecurity best practices for voter registration systems, its overall grade would not increase given the point distribution for the other categories.

To improve its overall election security, Iowa should immediately update its post-election audit law to ensure that audits test the accuracy of election outcomes and are binding on any erroneous results. In updating its audit requirements, Iowa should look to risk-limiting audits like those in Colorado as a potential model. Given the threat posed by sophisticated nation-states seeking to disrupt U.S. elections, it is imperative that post-election audits test the accuracy of election outcomes and detect any possible manipulation. Iowa should also require that all electronic poll books receive pre-election testing to ensure that they are in

good working order before Election Day. Furthermore, the state should prohibit electronic absentee voting of any kind, even by UOCAVA voters. Going forward, all voted ballots should be returned by mail or delivered in person.

Minimum cybersecurity standards for voter registration system: Incomplete

**State officials told us they would not provide information or comment on our research and were therefore unable to share information on cybersecurity requirements for the state's voter registration system. Information gathered for this section derives from independent research.*

- The state's voter registration system is estimated to be at least 10 years old.[569]
- State officials were unable to provide us with information on whether the state's voter registration system provides access control to ensure that only authorized personnel have access to the database.
- State officials were unable to provide us with information on whether the state's voter registration system has logging capabilities to track modifications to the database.
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[570]
- The state performs regular vulnerability assessments on its voter registration system.[571]
- State officials were unable to provide us with information on whether the state has enlisted the National Guard or DHS to help assess and identify potential threats to its voter registration system.
- State officials were unable to provide us with information on whether the state provides cybersecurity training to election officials.
- Electronic poll books are used by some, but not all, jurisdictions in the state.[572] Pre-election testing of electronic poll books is left up to the counties that use them.[573] Paper voter registration lists are available at polling places that use electronic poll books on Election Day.[574]

Voter-verified paper audit trail: Good

- Elections are carried out using paper ballots and optical scan machines.[575]

Post-election audits: Unsatisfactory

- In 2017, Iowa adopted House File 516, which requires a manual hand count of all ballots cast in randomly selected precincts after every general election.[576] Currently, there are no requirements regarding escalation procedures or for making the audit open to public observance or for making the results publicly

available, though the law does state that the 'hand count shall be observed by a representative selected by each of the two political parties whose candidates received the highest number of votes statewide in the preceding general election."[577] The audit law states explicitly that audit results "shall not change the results, or invalidate the certification, of an election."[578]

Ballot accounting and reconciliation: Fair

- All ballots are accounted for at the precinct level.[579]
- Precincts are required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[580]
- Counties are required to compare and reconcile precinct totals with county-wide results to ensure that they add up to the correct amount.[581]
- State law requires a review process to ensure that all voting machine memory cards have been properly loaded onto the tally server at the county level.[582]
- The state requires that all election results and reconciliation procedures be made public.[583]

Paper absentee ballots: Unsatisfactory

- The state allows UOCAVA voters and other absentee voters to return completed ballots electronically via fax or email.[584]

Voting machine certification requirements: Fair

- Before being purchased and used for an election, all voting machines must be shown to meet or exceed federal voting system standards.[585]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[586]

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[587]
- Testing is open to the public.[588]
- Testing must be completed not later than 12 hours before the opening of the polls on Election Day.[589]

Kansas

Kansas receives a **F/D***

Kansas adheres to a number of minimum cybersecurity best practices related to voter registration systems, but the state allows voting using machines that do not provide a paper record and fails to mandate post-election audits, which does not provide confirmation that ballots are cast as the voter intends and counted as cast. Kansas also allows voters stationed or living overseas to return voted ballots electronically, a practice that election security experts say is notoriously insecure. Its ballot accounting and reconciliation procedures also need improvement. The state did earn points for requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines before being used in the state, and for requiring election officials to carry out logic and accuracy testing on all voting machines before an election.

Despite numerous attempts to speak to someone in state government about the cybersecurity standards for the state's voter registration system, state officials did not respond to our requests for information or comment, and we were unable to locate all of the information independently. If Kansas is adhering to all of the minimum cybersecurity best practices for voter registration systems, it would receive a "good" score—worth 3 points—for that category, bringing its grade up to a D.

Kansas's reliance on machines that do not provide a paper record, coupled with its failure to carry out post-election audits even in jurisdictions with voter-verified paper trails, leaves the state open to undetected hacking and other Election Day problems. Going forward, Kansas should switch to a statewide paper-based voting system that can be audited through robust procedures that test the accuracy of election outcomes. In doing so, the state should look to risk-limiting audits like those in Colorado as a potential model. To improve its overall election security, Kansas should require that electronic poll books receive pre-election testing to ensure that they are in good working order before Election Day. The state would also be wise to partner with DHS to identify and assess vulnerabilities in its voter registration system, if it's not doing so already. While recognizing the importance of state autonomy when it comes to elections, federal agencies with

expertise in cybersecurity and access to classified information on contemporaneous cyberthreats have the personnel and resources necessary to thoroughly probe and analyze complex election databases, machines, and cybervulnerabilities. By combining their expertise on cyberthreats and their insight into the unique qualities of localized election infrastructure, state and federal officials can better assess and deter attempts at electoral disruption. Kansas should also prohibit electronic absentee voting and instead require that all voted ballots be returned by mail or in person. Regarding ballot accounting and reconciliation, all ballots—used, unused, and spoiled—must be accounted for at individual polling places.

Minimum cybersecurity standards for voter registration system: Incomplete

**State officials did not respond to our requests for information and comment on cybersecurity requirements for the state's voter registration system. Information gathered for this section derives from independent research.*

- The state's voter registration system is estimated to be at least 10 years old.[590]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[591]
- The state's voter registration system has logging capabilities to track modifications to the database.[592]
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[593]
- The state performs regular vulnerability assessments and penetration testing on its voter registration system.[594]
- The state has engaged in conference calls with DHS regarding election security matters, but it is unclear whether the state has enlisted DHS's help in monitoring its voter registration system.[595]
- State officials were unable to provide us with information on whether the state provides cybersecurity training to election officials.
- Electronic poll books are used by some, but not all, jurisdictions in the state.[596] Pre-election testing of electronic poll books is left up to the counties that use them.[597] Paper voter registration lists are available at polling places that use electronic poll books on Election Day.[598]

Voter-verified paper audit trail: Unsatisfactory

- Depending on the jurisdiction, some voters in Kansas cast paper ballots, while others vote using DRE machines.[599] Some DRE voting machines in the state produce a VVPR, while others are entirely paperless.[600]

Post-election audits: Unsatisfactory

- The state does not require mandatory post-election audits.[601]

Ballot accounting and reconciliation: Unsatisfactory

- Ballots are not fully accounted for at the precinct level.[603]
- Precincts are required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[604]
- Counties are required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[605]
- There is no statutorily mandated review process to ensure that all voting machine memory cards or flash drives have been properly loaded onto the tally serve at the county level.[606]
- While election results are made public, it is unclear whether the same is true of information regarding ballot reconciliation processes and results.[607]

Paper absentee ballots: Unsatisfactory

- The state permits UOCAVA voters to submit completed ballots electronically, via email or fax.[608]

Voting machine certification requirements: **FAIR**

- Before being purchased and used for an election, all voting machines must be shown to meet or exceed federal voting system standards.[609]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[610]

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[611]
- Testing is open to the public.[612]
- Testing occurs within five days prior to an election.[613]

Legislation introduced in 2017 would require county election officials to carry out post-election audits prior to certification on 1 percent of precincts or 1 precinct in the county, whichever is greater. The precincts included in the audit would be selected randomly, and the audit carried out in a public setting. The audit would be able to escalate if discrepancies arose and could correct incorrect preliminary election outcomes. The legislation would also require Kansas to transition to voting systems that produce paper records of votes cast.[602]

Kentucky

Kentucky adheres to recommended minimum cybersecurity best practices related to voter registration systems, but the state allows voting using machines that do not provide a paper record, which makes it impossible to carry out meaningful post-election audits that test the accuracy of election outcomes. Even in places with a voter-verified paper trail, the state's audits lack important criteria. For example, audits are tied to a fixed percentage regardless of the margin of victory, and there is no requirement that an audit escalate if necessary. Furthermore, state law limits public observance to members of the media. The state's ballot accounting and reconciliation procedures also need improvement. Kentucky did receive points for prohibiting voters stationed or living overseas from returning voted ballots electronically, a practice that election security experts say is notoriously insecure. In Kentucky, all voted ballots are returned by mail or delivered in person. The state also exercises good practices by requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines before being purchased and used in the state, and by requiring election officials to carry out logic and accuracy testing on all voting machines that will be used in an upcoming election.

To improve its overall election security, Kentucky should switch over to a paper-based voting system and require robust post-election audits that can confirm election outcomes with a high degree of confidence to strengthen defenses against malicious actors seeking to manipulate U.S. elections. In adopting post-election audit procedures, the state should look to risk-limiting audits like those in Colorado as a potential model. Kentucky should strengthen its ballot accounting and reconciliation procedures by requiring precincts to compare and reconcile the number of ballots with the number of voters who signed in at the polling place and by requiring counties to compare and reconcile precinct totals with composite results to confirm they add up to the correct number.

Minimum cybersecurity standards for voter registration system: Good

- The state's voter registration system is estimated to be at least 10 years old.[614]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[615]

- The state's voter registration system has logging capabilities to track modifications to the database.[616]
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[617]
- The state performs regular vulnerability assessments and penetration testing on its voter registration system.[618]
- The state has enlisted DHS to help assess and identify potential threats to its voter registration system and election infrastructure.[619]
- The state provides cybersecurity training to election officials.[620]
- The state does not currently use electronic poll books, but has issued a Request for Proposals (RFP) with hopes of having electronic poll books available for the 2018 elections.[621]

State election officials work closely with the U.S. Department of Homeland Security, the Kentucky Department of Homeland Security, and the Commonwealth Office of Technology to prepare for and respond to potential threats to Kentucky's election infrastructure.[622]

Voter-verified paper audit trail: Unsatisfactory

- Depending on the jurisdiction, some voters in Kentucky cast paper ballots, while others vote using paperless DRE machines.[623]

Post-election audits: Unsatisfactory

- The state conducts mandatory post-election audits as part of its county certification process.[624] However, Kentucky's use of paperless DRE machines prevents it from carrying out audits that can confirm the accuracy of election outcomes.
- The state's post-election audits are conducted through manual hand count.[625]
- There are two state laws on the books for post-election audits. One audit consists of a manual recount of randomly selected precincts. The selected precincts must represent between 3 percent and 5 percent of all ballots cast in the election.[626] Another law requires the Attorney General to conduct an "independent inquiry" in at least 5 percent of the state's counties.[627]
- All categories of ballots—regular, absentee, provisional, and UOCAVA—are eligible for auditing.[628]
- There is no statutory requirement on whether an audit escalates to include more voting components in the event that preliminary outcomes are found to be incorrect.
- State law does not require audits to be open to the public, but does permit the media to be present.[629]
- Audits occur as part of the state's certification process.[630]
- An audit can reverse the preliminary outcome of an audited contest if an error is detected.[631]

Ballot accounting and reconciliation: Unsatisfactory

- All ballots are accounted for at the precinct level.[632]
- Precincts are not required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[633]
- Counties are not explicitly required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[634]
- There is no statutorily mandated review process to ensure that all voting machine memory cards have been properly loaded onto the tally server at the county level.[635]
- The state requires that all election results and reconciliation procedures be made public.[636]

Paper absentee ballots: Fair

- The state does not permit voters—including UOCAVA voters—to submit completed ballots electronically. All ballots must be returned by mail or delivered in person.[637]

Voting machine certification requirements: Fair

- State law requires that before being purchased and used for an election, all voting machines must be shown to meet or exceed federal voting system standards.[638] In practice, all voting machines are EAC-certified.[639]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[640] However, Jefferson County—the state's largest county—will have all new machines in place for the 2018 elections.[641]

Jefferson County—Kentucky's largest county—will have all new machines in place for the 2018 elections.[642]

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[643]
- Testing is open to the public.[644]
- Testing must be carried out no more than 30 days but no fewer than five days before Election Day.[645] Testing on in-house absentee voting machines must be conducted no fewer than three days before the machine is used for absentee voting.[646]

Louisiana

Louisiana adheres to a number of minimum cybersecurity best practices related to voter registration systems, but the state allows voting using machines that do not provide a paper record and fails to mandate post-election audits, which does not provide confirmation that ballots are cast as the voter intends and counted as cast. Louisiana also allows voters stationed or living overseas to return voted ballots electronically, a practice that election security experts say is notoriously insecure. The state did receive points for requiring that voting machines be tested to EAC Voluntary Voting System Guidelines before being purchased or used in the state and for requiring election officials to conduct pre-election logic and accuracy testing on all voting machines that will be used in an upcoming election.

Louisiana's use of paperless DRE machines and failure to carry out post-election audits that test the accuracy of election outcomes leaves it open to undetected hacking and other Election Day problems. Given the threat posed by sophisticated nation-states seeking to disrupt U.S. elections, it is imperative that post-election audits test the accuracy of election outcomes and detect any possible manipulation. Encouragingly, we were told that Louisiana is seeking bids for new voting technology that will include a voter-verified paper audit trail, which—if combined with robust post-election audits—would greatly improve the state's overall election security. Furthermore, Louisiana should prohibit electronic absentee voting, even for UOCAVA voters. Going forward, all voted ballots should be returned by mail or delivered in person.

Minimum cybersecurity standards for voter registration system: Fair

- The state's voter registration system is estimated to be at least 10 years old.[647] However, the system receives regular cybersecurity updates and maintenance several times each year.[648]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[649]
- The state's voter registration system has logging capabilities to track modifications to the database.[650]

- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[651]
- The state performs regular vulnerability assessments on its voter registration system.[652]
- State officials have met with local and regional representatives from DHS to discuss the possibility of performing future audits to identify vulnerabilities but has not yet received assistance.[653] According to the Louisiana Secretary of State's office, the state has not received DHS assistance because such assistance would be duplicative of the state's own in-house capabilities.[654]
- The state provides annual cybersecurity training to election officials.[655]
- The state does not use electronic poll books, and therefore was not graded on e-pollbook best practices.[656]

Voter-verified paper audit trail: Unsatisfactory

- Elections are carried out using paperless DRE machines.[658] However, Louisiana has issued a Request for Proposals (RFP) for new voting technology that will include a voter verified paper ballot.[659]

Post-election audits: Unsatisfactory

- The state does not require post-election audits.[661]

Ballot accounting and reconciliation: Fair

- Ballots are fully accounted for at the precinct level.
- Precincts are required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[664]
- Counties are required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[665]
- There is no statutorily mandated review process to ensure that all voting machine memory cards have been properly loaded onto the tally server at the county level.[666] However, Louisiana's tally system will not complete the election and produce an unofficial turnout statistic until all machine memory cards for a county have been properly loaded or hand entered.[667]
- While state law requires that election results be made public, while ballot reconciliation procedures are performed during open public meetings.[668]

Paper absentee ballots: Unsatisfactory

- Louisiana permits UOCAVA voters to submit completed ballots electronically via fax.[669]

In the lead-up to the 2016 election, Louisiana partnered with outside entities to perform the same kind of vulnerability assessments on the state's public-facing systems that was later offered by DHS to all 50 states. Louisiana also contracted with a private contractor to perform real-time traffic analysis as well as quarterly vulnerability assessments on these systems. Louisiana Secretary of State Tom Schedler has applied for security clearance as part of an information-sharing initiative between the states and federal government on the issue of election security.[657]

Louisiana has issued a Request for Proposals (RFP) for new voting technology that will include a voter verified paper ballot.[660]

Voting machine certification requirements: Fair

- **Before being purchased and used for any election in the state, all voting machines must undergo testing by a federally accredited laboratory.[670]**
- Some jurisdictions in Louisiana still use voting machines that were purchased in 2005, more than a decade ago.[671] However, the machines' firmware has been upgraded twice since 2005, while the machines' software has been updated each year since the time of purchase.[672]

Pre-election logic and accuracy testing: Fair

- **Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[673]**
- Testing is open to the public.[674]
- Testing is carried out at least 36 hours before an election.[675]

Maine

Maine adheres to a number of minimum cybersecurity best practices related to voter registration systems and conducts its elections with paper ballots, but its failure to carry out post-election audits that test the accuracy of election outcomes leaves the state open to undetected hacking and other Election Day problems. Maine also allows voters stationed or living overseas to return voted ballots electronically, a practice that election security experts say is notoriously insecure. Improvements can also be made to Maine's ballot accounting and reconciliation procedures. The state did earn points for requiring election officials to carry out pre-election logic and accuracy testing on all machines that will be used in an upcoming election.

To improve its overall election security, Maine must put into place meaningful post-election audits that can confirm election outcomes with a high degree of confidence. In doing so, the state should look to risk-limiting audits like those in Colorado as a potential model. Maine should also require election officials to receive cybersecurity training prior to elections and should move forward with its plan to partner with DHS to identify and assess vulnerabilities in its voter registration system. While recognizing the importance of state autonomy when it comes to elections, federal agencies with expertise in cybersecurity and access to classified information on contemporaneous cyberthreats have the personnel and resources necessary to thoroughly probe and analyze complex election databases, machines, and cybervulnerabilities. By combining their expertise on cyberthreats and their insight into the unique qualities of localized election infrastructure, state and federal officials can better assess and deter attempts at electoral disruption. Maine should also prohibit electronic absentee voting, even for UOCAVA voters, and require that all voted ballots be returned by mail or delivered in person. Additionally, even though all voting machines currently in use may have been certified by the Election Assistance Commission, state law should explicitly require that all voting machines be tested to ensure that they meet or exceed federal standards related to functionality, security, and accessibility. Finally, polling places must reconcile the number of ballots cast with

the number of ballots that were spoiled, unused, or—in the case of absentee ballots—issued but not returned by the deadline. As part of the post-election ballot accounting, precincts should also compare and reconcile the number of ballots with the number of voters who signed in at the polling place to ensure that no ballots were lost and no invalid ballots were added.

Minimum cybersecurity standards for voter registration system: Fair

- The state's voter registration system is estimated to be at least 10 years old.[676]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[677]
- The state's voter registration system has logging capabilities to track modifications to the database.[678]
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[679]
- The state performs regular vulnerability assessments and penetration testing on its voter registration system.[680]
- In 2017, state officials met with the Maine National Guard and were introduced to the DHS staff from the New England region and the DHS staff member assigned to Maine. Although the state is not currently working with DHS, it does have the ability to enlist DHS's help as needed.[681]
- The state does not currently provide cybersecurity training to election officials.[682]
- The state does not use electronic poll books, and therefore was not graded on e-pollbook best practices.[683]

Voter-verified paper audit trail: Good

- Elections are carried out using paper ballots and digital scan tabulators.[684]

Post-election audits: Unsatisfactory

- The state does not require post-election audits.[685]

Ballot accounting and reconciliation: Unsatisfactory

- Ballots are not fully accounted for at the precinct level.[686] For example, there is no formal reconciliation required of the number of ballots cast versus those spoiled, unused, or—in the case of absentee ballots—issued but not returned by the deadline.[687]
- Precincts are not required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[688]
- Municipalities with more than one precinct are required to compare and reconcile precinct totals with the municipal-wide results to ensure that they add up to the correct amount.[689]

- The state does not use a tally server. As such, a memory card review process is unnecessary.[690]
- The state requires that all election results and reconciliation procedures be made public.[691]

Paper absentee ballots: Unsatisfactory

- The state permits UOCAVA voters to submit completed ballots electronically, via email or fax.[692]

Voting machine certification requirements: Fair

- Although the state does not require tabulating machines to meet federal requirements before they are purchased and used in elections in the state,[693] all voting machines currently in use have been certified by the Election Assistance Commission.[694]
- All tabulating machines in Maine have been replaced within the past 10 years.[695]

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all tabulating machines prior to an election.[696]
- Testing is open to the public.[697]
- Testing must be completed at least one week before the election.[698]

Maryland

Maryland adheres to recommended minimum cybersecurity best practices related to voter registration systems and conducts its elections with paper ballots, but its failure to carry out post-election audits that test the accuracy of election outcomes leaves the state open to undetected hacking and other Election Day problems. Currently, post-election audits are conducted through electronic retabulation, rather than manual hand count. The number of ballots included in an audit is tied to a fixed amount—the greater of three randomly selected precincts with at least 300 registered voters or 5 percent of all precincts used in an election—and any error is resolved simply by retabulating the ballots with a different automated machine. Perhaps most troublesome is the fact that the results of an audit cannot reverse the preliminary outcome of an audited contest if an error is detected. The state did receive points for its ballot accounting and reconciliation procedures and for prohibiting voters stationed or living overseas from returning voted ballots electronically, a practice that election security experts say is notoriously insecure. In Maryland, all voted ballots must be returned by mail or delivered in person. The state also exercises good practices by requiring that all voting machines to be tested to EAC Voluntary Voting System Guidelines before being purchased or used in the state, and by requiring election officials to conduct pre-election logic and accuracy testing on all machines that will be used in an upcoming election.

Despite scoring well in the other six categories, Maryland should immediately update its post-election audit procedures to ensure that audits are carried out through manual hand count and tied to a statistically significant number based on the margin of victory in one or more ballot contests. To be effective, audit results must be binding on official election results, with the ability to reverse the preliminary outcome of an audited contest if an error is detected.

Minimum cybersecurity standards for voter registration system: Good

- The state's voter registration system is estimated to be at least 10 years old.[699] However, the system's platform has been replaced and the server and supporting hardware have been upgraded three times since its inception.[700] According to state officials, the system's "software is continuously being enhanced."[701]

- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[702]
- The state's voter registration system has logging capabilities to track modifications to the database.[703]
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[704]
- The state performs regular vulnerability assessments and penetration testing on its voter registration system.[705]
- The state has enlisted DHS to help assess and identify potential threats to its voter registration system.[706]
- The state requires cybersecurity training for all election officials at the state and county level.[707] The state offers monthly online trainings as well as in-person classes.[708]
- Electronic poll books are used statewide in Maryland.[709] The state conducts pre-election testing on electronic poll books prior to an election.[710] Paper voter registration lists are available at polling places that use electronic poll books on Election Day.[711]

Voter-verified paper audit trail: Good

- Elections are carried out using paper ballots and optical scan machines.[712]

Post-election audits: Unsatisfactory

- The state conducts mandatory post-election audits.[713]
- The state's post-election audits are conducted electronically through automated retabulation.[714]
- State law requires auditing the greater of two precincts with at least 300 registered voters or 5 percent of all precincts used in an election.[715] Additionally, the state audited through retabulation 100 percent of the ballots cast in the 2016 election.[716]
- The precincts included in the audit are selected randomly.[717]
- All ballot types—regular, early voting, absentee, provisional, and UOCAVA—are eligible for auditing.[718]
- If a discrepancy of more than 0.5 percent arises, additional review and investigation is required.[719] If upon investigating it appears to be an error in the tabulating equipment, the ballots are retabulated using a different automated machine.[720]
- Audit results are publicly available.[721]
- Audits are carried out prior to certification of official election results.[722]
- An audit cannot reverse the preliminary outcome of an audited contest if an error is detected.[723]

Ballot accounting and reconciliation: Fair

- All ballots are accounted for at the precinct level.[724]
- Precincts are required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[725]
- The state compares and reconciles precinct totals with countywide results to ensure that they add up to the correct amount.[726]
- State law requires a review process to ensure that all voting machine memory cards have been properly loaded onto the tally server at the county level.[727]
- While state law requires that election results be made public, it is unclear whether the same is true of information regarding ballot reconciliation processes and results.[728] Election officials have made information and results from the post-election ballot tabulation audit available to the public.[729]

Paper absentee ballots: Fair

- The state does not permit voters—including UOCAVA voters—to submit completed ballots electronically. All ballots must be returned by mail or delivered in person.[730]

Voting machine certification requirements: Fair

- In practice, before they may be purchased and used in the state, all voting machines must be certified by the Election Assistance Commission.[731]
- All voting machines in Maryland have been replaced within the past 10 years.[732]

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[733]
- Testing is open to the public.[734]
- Machines used during early voting must be tested at least 14 days before Election Day.[735] For machines that will be used on Election Day and for counting absentee or provisional ballots, testing must begin at least 10 days before Election Day.[736]

Massachusetts

Massachusetts conducts its elections with paper ballots, but its failure to carry out mandatory post-election audits after every election leaves the state open to undetected hacking and other Election Day problems. State law only requires post-election audits to be carried out after presidential elections. Also, the number of ballots included in the audit is based on a fixed percentage—3 percent—rather than a statistically significant number tied to the margin of victory in one or more ballot contests. Escalation is left within the discretion of the Massachusetts secretary of state rather than being automatically triggered under particular circumstances. Adding to this is the fact that Massachusetts allows voters stationed or living overseas to return voted ballots electronically, a practice that election security experts say is notoriously insecure. The state did earn points for its ballot accounting and reconciliation procedures and for requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines before being purchased or used in the state. Massachusetts also requires election officials to carry out pre-election logic and accuracy testing on all machines that will be used in an upcoming election.

To improve its overall election security, Massachusetts must require more rigorous post-election audits after every election, not just after presidential elections. The number of ballots included in an audit should be based upon a statistically significant number tied to the margin of victory in one or more ballot contests, while escalation should be required—not discretionary. In making these changes, state officials should look to risk-limiting audits like those in Colorado as a potential model. Massachusetts should work toward partnering with DHS to identify and assess potential threats to its voter registration system, to the extent possible. While recognizing the importance of state autonomy when it comes to elections as well as the fact that Massachusetts is working with a third-party vendor to assess potential vulnerabilities with its system, federal agencies with expertise in cybersecurity and access to classified information on contemporaneous cyberthreats have the personnel and resources necessary to thoroughly probe and analyze complex

election databases, machines, and cybervulnerabilities. Finally, the state should prohibit electronic absentee voting, even by UOCAVA voters, and require that all voted ballots be returned by mail or delivered in person.

Minimum cybersecurity standards for voter registration system: Fair

- The state's voter registration system is estimated to be at least 10 years old.[737]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[738]
- The state's voter registration system has logging capabilities to track modifications to the database.[739]
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[740]
- The state performs regular vulnerability assessments and penetration testing on its voter registration system.[741]
- The state has not enlisted the National Guard or DHS to help assess and identify potential threats to its voter registration system and election infrastructure, but has worked with third-party contractors for similar purposes.[742]
- The state provides basic cybersecurity information to local election officials, including information on how to keep their passwords secure as well as other basic computing best practices.[743]
- State law permits the use of electronic poll books, but they are not yet used in general elections.[744]

Voter-verified paper audit trail: Good

- Elections are carried out using paper ballots and optical scan machines.[745]

Post-election audits: Unsatisfactory

- The state conducts mandatory post-election audits, but only after presidential elections.[746]
- The state's post-election audits are conducted through manual hand count.[747]
- Audits include 3 percent of all precincts.[748] Audits include contested races for president and vice president, representative in Congress, senator in Congress, representative in the General Court and senator in the General Court, and a statewide ballot question if one exists.[749]
- The precincts included in the audit are selected randomly.[750]
- All ballot types—regular, early voting, absentee, provisional, and UOCAVA—are eligible for auditing.[751]
- If preliminary outcomes are found to be incorrect, the secretary of the commonwealth may require escalation to include additional precincts or contested races.[752]

- Audits are open to the public and the results are made public.[753]
- Audits are carried out prior to certification of official election results.[754]
- An audit can reverse or correct the preliminary outcome of an audited contest if an error is detected.[755]

Ballot accounting and reconciliation: Fair

- All ballots are accounted for at the precinct level.[756]
- Precincts are required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[757]
- Municipalities are required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[758]
- The state does not use a tally server. As such, a memory card review process is unnecessary.[759]
- The state requires that all election results and reconciliation procedures be made public.[760]

Paper absentee ballots: Unsatisfactory

- The state permits UOCAVA voters to submit completed ballots electronically, via email or fax.[761]

Voting machine certification requirements: Fair

- Before they may be purchased and used in the state, all voting machines must be certified by the Election Assistance Commission.[762]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[763]

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[764]
- Testing is open to the public.[765]
- Testing occurs at least four days before an election.[766]

Michigan

Michigan adheres to a number of minimum cybersecurity best practices related to voter registration systems and conducts its elections with paper ballots, but its failure to mandate post-election audits that can confirm the accuracy of election outcomes leaves the state vulnerable. After certification, the state conducts a procedural review that evaluates the proper testing of voting machines' programming and the functionality of hardware and software. The current process does not yet compare ballot totals in a meaningful way. Michigan's ballot accounting and reconciliation procedures can also use improvement. The state did earn points for requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines before being purchased or used in the state, and for prohibiting absentee voters from returning voted ballots electronically. In Michigan, all voted ballots must be returned by mail or delivered in person. The state also requires election officials to carry out pre-election logic and accuracy testing on all machines that will be used in an upcoming election.

To improve its overall election security, Michigan should adopt robust post-election audit processes that test the accuracy of election outcomes. Encouragingly, we were told that state officials piloted a ballot tally comparison as part of Michigan's post-election procedures during the November 2017 election. To improve its auditing procedures, the state should look to risk-limiting audits like those in Colorado as a potential model. Given the threat posed by sophisticated nation-states seeking to disrupt U.S. elections, it is imperative that post-election audits test the accuracy of election outcomes and detect any possible manipulation. Michigan should also update some of its requirements for electronic poll books. We were told by Michigan officials that testing electronic poll books prior to an election is not necessary, given that the poll book system is not connected to the state's voter registration system. Instead, prior to Election Day localities download the relevant voter lists onto the electronic poll book laptop. The concern, however, is that malware could be embedded into these downloaded files, which could leave voter lists inaccessible on Election Day. This is one reason why it is important to test all electronic poll books prior to every election. Finally, Michigan can strengthen its ballot accounting and reconciliation procedures by requiring counties to compare and reconcile precinct totals with composite results to confirm that they add up to the correct number.

Minimum cybersecurity standards for voter registration system: Fair

- The state's voter registration system is estimated to be at least 10 years old.[767] However, the system is in the process of being completely rewritten in a new language on a new platform and a new server.[768] The new system is expected to be rolled out in early 2018.[769]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[770]
- The state's voter registration system has logging capabilities to track modifications to the database.[771]
- The voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[772]
- The state performs regular vulnerability assessments and penetration tests on the state's voter registration system.[773]
- The state has enlisted DHS to help assess and identify potential threats to its voter registration system and election infrastructure.[774]
- The state provides initial cybersecurity training to election officials at the state level and to others who have access to the state's voter registration system. The state plans to expand its online cybersecurity module training to election officials at the local level.[775]
- Electronic poll books are used statewide in Michigan.[776] The state's electronic poll book system is not connected to the state's voter registration system. Instead, prior to Election Day localities download the relevant voter lists onto an encrypted electronic poll book laptop. In doing so, they are directed by the state to confirm that all of the proper software updates have been loaded onto the machine. Pre-election testing of electronic poll books is left up to the localities that use them.[777] Paper voter registration lists are available at polling places that use electronic poll books on Election Day.[778]

This year, Michigan will unveil a completely refurbished new voter registration system, rewritten in an updated language on a updated platform and server.[779]

Michigan has received or is expected to receive additional funding for cybersecurity at their election agencies.[780]

Voter-verified paper audit trail: Good

- Elections are carried out using paper ballots and optical scan machines.[781]

Post-election audits: Unsatisfactory

- The state conducts a post-election procedural review after certification and evaluates the proper testing of voting machines' programming and the functionality of hardware and software.[782] The review does not yet compare ballot totals in a meaningful way.[783] However, during the 2017 elections, state officials piloted a new ballot-tally comparison with plans to expand the program to counties this year. According to one state official, the program "will include a ballot count for 1-3 races on the audited precinct ballot. The number

of races counted will depend on the number of races and proposals on the ballot … For larger statewide ballots in even years, we will plan to count up to 3 races (e.g., top of the ticket, county level, local level)." The process includes a manual hand count conducted by two staff persons to verify that the number of ballots matches the number tabulated on Election Day. According to the state officials, "The ballots are then separated into piles based on the vote cast in the counted race; totals are then tallied and reported for each candidate (if applicable); proposal Yes/No (if applicable); write-in votes (if applicable); overvotes; and undervotes. Audit count results are recorded and reported with the rest of the audited tasks, with any anomalies and/or changes from Election Day totals noted."[784]

Ballot accounting and reconciliation: Unsatisfactory

- All ballots are accounted for at the precinct level.[786]
- Precincts are required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[787]
- Counties are not explicitly required to compare and reconcile precinct totals with county-wide results to ensure that they add up to the correct amount.[788]
- As a matter of standard practice on election night, counties confirm that all precinct tally results and memory cards are received and loaded at the county level.[789]
- All election results and reconciliation procedures are made public.[790]

In 2017, state officials piloted a new ballot tally comparison as part of Michigan's post-election procedures with plans to expand the process for counties beginning in 2018.[785]

Paper absentee ballots: Fair

- The state does not permit voters—including UOCAVA voters—to submit completed ballots electronically. All voted ballots must be returned by mail or delivered in person.[791]

Voting machine certification requirements: Fair

- Before they may be purchased and used in the state, all voting machines must be certified by the Election Assistance Commission.[792]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago. However, the state began to replace all optical scanning machines in August 2017.[793] As of November 2017, 49 of 83 counties had converted to new voting systems.[794] All remaining voting machines are scheduled to be updated by August 2018.

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[797]
- Testing is open to the public.[798]
- Testing is carried out at least five days before an election.[799]

Michigan began to replace all optical scanning machines in August 2017. As of November 2017, 49 of 83 counties had converted to new voting systems. All remaining voting machines will be updated by August 2018.

Minnesota

Minnesota adheres to a number of minimum cybersecurity best practices related to voter registration systems and conducts its elections with paper ballots, but its post-election audits lack important criteria. For example, the number of ballots included in the state's post-election audits is currently a fixed number depending on the size of county, rather than a statistically significant number tied to the margin of victory in one or more ballot contests. The state did receive points for prohibiting voters stationed or living overseas from returning voted ballots electronically, a practice that election security experts say is notoriously insecure. In Minnesota, all voted ballots must be returned by mail or delivered in person. The state also exercises best practices by requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines before being purchased or used in the state, and by requiring election officials to carry out pre-election logic and accuracy testing on all voting machines that will be used in an upcoming election.

To improve its overall election security, Minnesota should strengthen its post-election audit requirements by basing the number of ballots included in an audit on a statistically significant number tied to the margin of victory in one or more ballot contests, rather than a fixed number based on the size of a given county. Given the threat posed by sophisticated nation-states seeking to disrupt U.S. elections, it is imperative that post-election audits test the accuracy of election outcomes and detect any possible manipulation. Minnesota should also require election officials to undergo cybersecurity training prior to elections so that they are prepared to identify and respond to threats or phishing attempts. Finally, the state should do away with allowing poll workers to remove excess ballots at random if discrepancies arise between the number of voters who sign into the polling place and voted ballots.

Minimum cybersecurity standards for voter registration system: Fair

- The state's voter registration system is estimated to be at least 10 years old.[800]
- The state's voter registration system provides access control to ensure that only authorized personnel can access the database.[801]

- The state's voter registration system has logging capabilities to track modifications to the database.[802]
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[803]
- The state performs regular vulnerability assessments and penetration testing on its voter registration system.[804]
- In 2016, the secretary of state's office communicated with and made use of information provided by DHS. However, until a law changed in 2017, the secretary of state's office was prohibited from utilizing DHS assessment services and from sharing certain information regarding the secretary of state's office system with DHS. Since the new legislation became effective in 2017, the secretary of state's office has begun working with DHS to utilize the assessment tools available to states.[805]
- The state does not require election officials to undergo cybersecurity training prior to an election.[806]
- Approximately six counties make use of electronic poll books, although many of those are simply testing out the equipment to determine whether they will be used in future elections.[807] The state requires each jurisdiction using electronic poll books to certify at least 30 days before the election that the electronic poll books meet basic security and functionality requirements.[808] Paper voter registration lists are available at polling places that use electronic poll books on Election Day.[809] Because Minnesota's electronic poll books are still in the piloting phase, the state was not graded on e-pollbook best practices.

Minnesota contracted with a third-party vendor to help assess and identify potential threats to its voter registration system during 2016 after a law prohibiting the state from sharing security information with federal officials prevented it from enlisting help from DHS.[810]

Voter-verified paper audit trail: Good

- Elections are carried out using paper ballots and optical scan machines.[812]

Post-election audits: Fair

- The state conducts mandatory post-election audits.[813]
- The state's post-election audits are conducted through manual hand count.[814]
- The number of precincts selected for an audit are based on the county's registered voter population.[815] For example, the county canvassing board of a county with fewer than 50,000 registered voters must conduct an audit on at least two precincts. Counties with between 50,000 and 100,000 registered voters must audit at least three precincts. Counties with more than 100,000 registered voters must audit at least four precincts or 3 percent of the total number of precincts in the county, whichever is greater.[816] State law requires that audits consider votes cast for president or governor, U.S. senator, and U.S. representative, and may include consideration of other ballot contests.[817]
- The precincts included in the audit are selected randomly.[818]

"…I continue to believe the most serious challenge to the integrity of our election system is the threat of outside forces, including foreign governments, who seek to disrupt and undermine our elections."
—Minnesota Secretary of State Steve Simon[811]

- All ballot categories—regular, early voting, absentee, provisional, and UOCAVA—are eligible for auditing.[819]
- If a discrepancy of more than 0.5 percent is found, the audit escalates to include additional precincts.[820] If necessary, the audit can escalate to include all precincts statewide.[821]
- Audits are open to the public and the results are made publicly available.[822]
- Audits are carried out prior to certification of official election results.[823]
- An audit can reverse the preliminary outcome of an audited contest if an error is detected.[824]

Ballot accounting and reconciliation: Unsatisfactory

- All ballots are accounted for at the precinct level.[825]
- Precincts are required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[826] However, as part of the reconciliation process, poll workers can remove excess ballots at random.[827]
- Counties are required to compare and reconcile precinct totals with county-wide results to ensure that they add up to the correct amount.[828]
- There is no statutorily mandated review process to ensure that all voting machine memory cards have been properly loaded onto the tally server at the county level.[829] However, tabulator tapes are compared against tally server totals as a matter of best practice.[830]
- The state requires that election results and ballot reconciliation information be made public.[831]

Paper absentee ballots: Fair

- The state does not permit voters—including UOCAVA voters—to submit completed ballots electronically. All ballots must be returned by mail or delivered in person.[832]

Voting machine certification requirements: Fair

- Before being purchased and used for any election in the state, all voting machines must undergo testing by a federally accredited laboratory.[833]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[834]

In 2017, the state authorized $7 million in grant funds to replace Minnesota's outdated voting equipment by 2020.[835]

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[836]
- Testing is open to the public.[837]
- Testing is carried out 14 days before an election.[838]

Mississippi

Mississippi adheres to recommended minimum cybersecurity best practices related to voter registration systems, but the state allows voting using machines that do not provide a paper record and fails to mandate post-election audits, which does not provide confirmation that ballots are cast as the voter intends and counted as cast. Adding to this is the fact that Mississippi allows voters stationed or living overseas to return voted ballots electronically, a practice that election security experts say is notoriously insecure. Mississippi did earn points for its state's ballot accounting and reconciliation procedures and for requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines. Additionally, Mississippi requires election officials to conduct pre-election logic and accuracy testing on all machines that will be used in an upcoming election.

To improve its overall election security, Mississippi should switch over to a paper ballot voting system and require post-election audits that test the accuracy of election results. The state's reliance on machines that do not provide a paper record and its failure to conduct robust post-election audits even in jurisdictions with a voter-verified paper audit trail leave the state open to undetected hacking and other Election Day problems. In conducting post-election audits, the state should look to risk-limiting audits like those in Colorado as a potential model. Given the threat posed by sophisticated nation-states seeking to disrupt U.S. elections, it is imperative that post-election audits test the accuracy of election outcomes and detect any possible manipulation. Mississippi should also prohibit electronic absentee voting—even by UOCAVA voters, who are currently permitted to return voted ballots by email or fax. All voted ballots should be returned by mail or delivered in person. By making these changes, Mississippi will dramatically improve the security of its elections.

Minimum cybersecurity standards for voter registration system: Fair

- The state's voter registration system is estimated to be at least 10 years old.[839]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[840]

- The state's voter registration system has logging capabilities to track modifications to the database.[841]
- The state performs regular vulnerability assessments on its voter registration system.[842]
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[843]
- The state has carried out DHS recommendations for protecting voter registration systems and election infrastructure.[844]
- The state provides annual cybersecurity training to election officials.[845]
- Electronic poll books are used by only a handful—approximately five to seven—of counties in the state.[846] Pre-election testing of electronic poll books are conducted by the counties.[847] Paper poll books are available at polling places that use electronic poll books on Election Day.[848]

Voter-verified paper audit trail: Unsatisfactory

- Depending on the jurisdiction, some voters in Mississippi cast paper ballots, while others vote using DRE machines.[849] Some DRE machines in the state produce a VVPR, while others are entirely paperless.[850]

Post-election audits: Unsatisfactory

- Mississippi's use of paperless DRE machines prevents it from carrying out audits that can confirm the accuracy of election outcomes. After certification of election results, Mississippi sometimes carries out a hand-to-eye count of absentee envelopes and applications.[851]

Ballot accounting and reconciliation: Fair

- All ballots are accounted for at the precinct level.[852]
- Precincts are required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[853]
- Counties are required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[854]
- There is no statutorily mandated review process to ensure that all voting machine memory cards have been properly loaded onto the tally server at the county level.[855]
- The state requires that all election results and reconciliation procedures are subject to public record requests.[856]

Paper absentee ballots: Unsatisfactory

- The state permits UOCAVA voters to submit completed ballots electronically, via email or fax.[857]

Voting machine certification requirements: Fair

- Before being purchased and used for an election, all voting machines must be shown to meet or exceed federal voting system standards.[858]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[859]

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[860]
- Testing is open to the public.[861]
- Testing is carried out at least two days prior to an election.[862]

Missouri

Missouri uses paper ballots and voting machines that provide a paper record, but the state's post-election audits lack important criteria. For example, the number of ballots included in an audit is based on a fixed percentage rather than a statistically significant number, and there is no explicit requirement that all ballot types—regular, absentee, provisional, and UOCAVA—be included in the audit. The law is also silent on whether an audit must automatically escalate to include more ballots if necessary. Also, Missouri allows voters stationed or living overseas to return voted ballots electronically, a practice that election security experts say is notoriously insecure. The state's ballot accounting and reconciliation procedures also need improvement. Despite numerous attempts to speak to someone in state government about cybersecurity standards for the state's voter registration system, state officials did not follow through on requests for information and comment on our research, and we were unable to locate all of the information independently. Even if Missouri is adhering to all of the minimum cybersecurity best practices for voter registration systems, its overall grade would not increase given the point distribution in the other categories. Missouri did earn points for requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines before being purchased or used in the state, and for requiring election officials to carry out pre-election logic and accuracy testing on all machines that will be used in an upcoming election.

To improve its overall election security, Missouri should adopt more comprehensive procedures for carrying out post-election audits that test the accuracy of election outcomes. Specifically, the number of ballots included in an audit should be tied to the margin of victory in one or more ballot contests, and the audit should automatically escalate if necessary. In revising its audit requirements, the state should look to risk-limiting audits like those in Colorado as a potential model. Given the threat posed by sophisticated nation-states seeking to disrupt U.S. elections, it is imperative that post-election audits test the accuracy of election outcomes and detect any possible manipulation. Missouri should also strengthen its ballot accounting and reconciliation procedures by requiring counties to compare

and reconcile precinct totals with countywide composite results to ensure that they add up to the correct number. Additionally, Missouri should prohibit voters stationed or living overseas from returning voted ballots electronically. All voted ballots should be returned by mail or delivered in person. The state should require all election officials to receive cybersecurity training prior to an election, and it should also require electronic poll books to undergo pre-election testing to ensure that they are in good working order before Election Day. At the same time, backup paper voter registration lists must be made available at polling places that use electronic poll books in case of emergency.

Minimum cybersecurity standards for voter registration system: Incomplete

**State officials did not follow through on our requests for information and comment on cybersecurity requirements for the state's voter registration system. Information gathered for this section derives from independent research and correspondence with a county official.*

- The state's voter registration system is estimated to be at least 10 years old.[863]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[864]
- State officials were unable to provide us with information on whether the state's voter registration system has logging capability to track modifications to the database.
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities[865]
- The state performs regular vulnerability assessments on its voter registration system.[866]
- State officials were unable to provide us with information on whether the state has enlisted the National Guard or DHS to help assess and identify potential threats to its voter registration system.
- The state does not provide cybersecurity training to election officials.[867] However, at least one county—St. Louis County—has started providing cybersecurity training to election personnel in partnership with its IT department.[868]
- Missouri permits the use of electronic poll books.[869] The state does not require that backup paper voter registration lists be made available, nor does it require that all electronic poll books be tested prior to an election.[870] However, at least one county—St. Louis County—tests all of its electronic poll books prior to an election.[871]

Voter-verified paper audit trail: Fair

- Depending on the jurisdiction, some voters in Missouri cast paper ballots, while others vote using DRE machines with VVPR.[872]

Post-election audits: Mixed

- The state conducts mandatory post-election audits.[873]
- The state's post-election audits are conducted through manual hand count.[874]
- The state requires post-election audits on no fewer than 5 percent of precincts.[875] The ballot contests considered in the audit are randomly selected, along with one randomly selected contested from each of the following categories: "(1) Presidential and Vice-Presidential electors, United States senate candidates and state-wide candidates; (2) state-wide ballot issues; (3) United States representative candidates and state general assembly candidates; [and] (4) Partisan circuit and associate circuit judge candidates and all nonpartisan judicial retention candidates." In addition, the audit must include at least one "contested race or ballot issue from all political subdivisions and special districts, including the county, in the selected precinct(s)" as well as "all races in which the margin of victory between the two (2) top candidates is equal to or less than half of 1 percent (0.5 percent) of the number of votes cast for the office or issue."[876]
- The precincts included in the audit are selected randomly.[877]
- While there are no statutory requirements on whether all categories of ballots—regular, absentee, provisional, and UOCAVA—are eligible for auditing, at least one county includes all ballot categories in its post-election audits.[878]
- There are no statutory requirements on whether an audit escalates to include more voting components in the event that preliminary outcomes are found to be incorrect.[879] Instead, if the results of the audit reveal a discrepancy of more than 0.5 percent from the preliminary results, "[T]he manual recount team shall immediately notify the election authority, who shall investigate the causes of any discrepancy and resolve any discrepancies prior to the date of certification."[880]
- Audits are open to the public and the results are made publicly available.[881]
- Audits are carried out before certification of official election results.[882]
- An audit can reverse the preliminary outcome of an audited contest if an error is detected.[883]

Ballot accounting and reconciliation: Unsatisfactory

- All ballots are accounted for at the precinct level.[884]
- Precincts are required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[885]
- Counties are not explicitly required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[886]

- Counties review and account for all voting machine memory cards or flash drives to ensure they have been properly loaded onto the tally server.[887]
- The state requires election results to be made public, but does not require the same for ballot reconciliation information.[888]

Paper absentee ballots: Unsatisfactory

- The state permits some UOCAVA voters to return completed ballots electronically via email, fax, or web portal.[889]

Voting machine certification requirements: Fair

- State law requires that before being purchased and used for any election in the state, all voting machines must undergo testing by a federally accredited laboratory.[890] In practice, all machines are EAC-certified.[891]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[892]

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[893]
- Testing is open to the public.[894]
- Testing is carried out within 14 days before an election.[895]

Montana

Although Montana adheres to a number of minimum cybersecurity best practices related to voter registration systems and conducts its elections with paper ballots, its failure to carry out post-election audits in certain jurisdictions leaves the state open to undetected hacking and other Election Day problems. In Montana, audits are only required in jurisdictions that use ballot tabulators to compile results. Counties that hand count their ballots are not required to conduct a post-election audit. At the same time, the scope of an audit is based on a fixed amount rather than a statistically significant number tied to the margin of victory in one or more ballot contests, and the audit law is silent on whether all categories of ballots—regular, absentee, provisional, and UOCAVA—are included in the audit. Montana allows voters stationed or living overseas to return voted ballots electronically, a practice that election security experts say is notoriously insecure. The state did earn points for its ballot accounting and reconciliation procedures and for requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines before they may be purchased or used in the state. Moreover, Montana requires election officials to carry out pre-election logic and accuracy testing on all machines that will be used in an upcoming election.

To secure its elections against sophisticated nation-states seeking to interfere in U.S. elections, Montana must require post-election audits to be conducted statewide that test the accuracy of election outcomes. Robust post-election audits are a critically important step in protecting the state's elections. In updating its audit requirements, Montana should look to risk-limiting audits like those in Colorado as a potential model. Montana should also partner with DHS to identify and assess potential threats to its voter registration system. While recognizing the importance of state autonomy when it comes to elections, federal agencies with expertise in cybersecurity and access to classified information on contemporaneous cyberthreats have the personnel and resources necessary to thoroughly probe and analyze complex election databases, machines, and cybervulnerabilities. By combining their expertise on cyberthreats and their insight into the unique qualities of localized election infrastructure, state and federal officials can better assess

and deter attempts at electoral disruption. Finally, Montana should prohibit electronic absentee voting, even for UOCAVA voters, who are currently allowed to return voted ballots by email or fax. Because experts have warned that electronic voting is not secure, all voted ballots should be returned by mail or delivered in person to prevent potential manipulation and protect voter privacy.

Minimum cybersecurity standards for voter registration system: Fair

- The state's voter registration system is estimated to be at least 10 years old.[896]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[897]
- The state's voter registration system has logging capabilities to track modifications to the database.[898]
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[899]
- The state performs regular vulnerability assessments and penetration testing on its voter registration system.[900]
- The state has not enlisted the National Guard or DHS to help assess and identify potential threats to its voter registration system.[901]
- The state provides annual cybersecurity training to election officials.[902]
- The state does not use electronic poll books, and therefore was not graded on e-pollbook best practices.[903] However, some counties are currently considering using electronic poll books for future elections.[904]

Some counties in Montana are currently considering using electronic poll books for future elections.[905]

Voter-verified paper audit trail: Good

- Elections are carried out using paper ballots and both optical and digital scan machines.[906]

Post-election audits: Unsatisfactory

- The state conducts mandatory post-election audits for counties that use ballot tabulators to compile results.[907] Jurisdictions that hand count their ballots are not required to carry out post-election audits.[908]
- The state's post-election audits are conducted through manual hand count.[909]
- Audits include at least 5 percent of precincts in each county or a minimum of one precinct in each county, whichever is greater.[910] Audits examine one statewide office race, one federal office race, one legislative office race, and one statewide ballot issue if one exists.[911]
- The precincts and ballot contests included in the audit are selected randomly.[912]
- All categories of ballots—regular, absentee, provisional, and UOCAVA—are eligible for auditing.[913]

- If a discrepancy of five ballots or more than 0.5 percent—whichever is greater—is found, at least three additional precincts within the county must be audited.[914]
- Audits are open to the public and the results are made publicly available.[915]
- Audits must be conducted prior to certification of election results.[916]
- An audit can reverse the preliminary outcome of an audited contest if an error is detected.[917]

Ballot accounting and reconciliation: Fair

- All ballots are accounted for at the precinct level.[918]
- Precincts are required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[919]
- Counties are required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[920]
- There is no statutorily mandated review process to ensure that all voting machine memory cards have been properly loaded onto the tally server at the county level.[921] However, the statewide tally system—Electronic Statewide Election Reporting System (eSERS)—functions in such a way that election officials would be made aware if a precinct's results were missing and the county would be required to reload the results before certifying the election.[922]
- The state requires that all election results and reconciliation procedures be made public.[923]

Paper absentee ballots: Unsatisfactory

- Montana allows UOCAVA voters to submit completed ballots electronically, via email or fax.[924]

Voting machine certification requirements: Fair

- Before being purchased and used for an election, all voting machines must be shown to meet or exceed federal voting system standards.[925]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[926]

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[927]
- Testing is open to the public.[928]
- Testing is carried out within 30 days of an election.[929]

Nebraska

Although Nebraska adheres to a number of minimum cybersecurity best practices related to voter registration systems and conducts its elections with paper ballots, its failure to mandate post-election audits that test the accuracy of election outcomes leaves the state open to potential hacking and other Election Day problems. We are told that post-election audits are carried out in practice. However, given their importance in securing U.S. elections against sophisticated nation-states seeking to interfere, it is important that audits be statutorily mandated. Adding to this is the fact that Nebraska allows voters stationed or living overseas to return voted ballots electronically, a practice that election security experts say is notoriously insecure. The state's ballot accounting and reconciliation procedures can also be improved. Nebraska did earn points for requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines before they may be purchased or used in the state and for requiring election officials to carry out pre-election logic and accuracy testing on all machines that will be used in an upcoming election.

To improve its overall election security, Nebraska should codify post-election audits that test the accuracy of election outcomes. In doing so, the state should look to risk-limiting audits like those in Colorado as a potential model. It is not enough that the state has carried out post-election reviews for the past several years. It is imperative that post-election audits be robust and required by law. Nebraska should also prohibit electronic absentee voting, even for UOCAVA voters who are currently allowed to return voted ballots by email or fax. All voted ballots should be returned by mail or delivered in person. The state can strengthen its ballot accounting and reconciliation procedures by requiring precincts to compare and reconcile the number of ballots with the number of voters who signed in at the polling place and by requiring counties to compare and reconcile precinct totals with composite results to confirm that they add up to the correct number.

Minimum cybersecurity standards for voter registration system: Good

- The state's voter registration system is estimated to be at least 10 years old.[930]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[931]

- The state's voter registration system has logging capabilities to track modifications to the database.[932]
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[933]
- The state performs regular vulnerability assessments on its voter registration system.[934]
- The state has enlisted DHS to help assess and identify potential threats to its voter registration system.[935]
- The state provides cybersecurity training to election officials.[936]
- The state does not use electronic poll books, and therefore was not graded on e-pollbook best practices.[937]

Voter-verified paper audit trail: Good

- Elections are carried out using paper ballots and optical scan machines.[938]

Post-election audits: Unsatisfactory

- The state does not legally require post-election audits. That being said, the Nebraska secretary of state is permitted to conduct an audit by discretion, and we are told that post-election audits have been carried out in the state after general elections since at least 2008.[939] Discretionary audits include 2 percent of randomly selected precincts and a federal, statewide, and local ballot contest.[940] Even though audits are conducted by manual hand count, they are only carried out after certification of election results, cannot escalate in the event that preliminary outcomes are found to be incorrect, and cannot reverse the preliminary outcome of an audited contest if an error is detected.[941]

Ballot accounting and reconciliation: Unsatisfactory

- All ballots are accounted for at the precinct level.[942]
- Precincts are not required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[943]
- Counties are not explicitly required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[944]
- There is no statutorily mandated review process to ensure that all voting machine memory cards have been properly loaded onto the tally server at the county level.[945] According to one state official: "Nebraska law that requires at least 3 independent test[s] to be conducted before counting to verify the accuracy of the counting process which includes the memory cards and tally disks. … These three test[s] are conducted before Election Day. The results of the tests would … verify that the counting programs are successfully installed

in the counting machines, to make sure the results of the test deck ballots are accurate and then saved to a disk which is then uploaded to the States Election Night reporting system during the mock election to make sure the results are properly uploaded and match what the counting machines states."[946] Those tests are more similar in nature to pre-election logic and accuracy testing rather than a review process accounting for all voting machine memory cards or flash drives to ensure they are all properly uploaded.

- The state publicly releases a state "abstract," which includes an accumulation of all local vote totals and any reconciliation procedures performed.[947]

Paper absentee ballots: Unsatisfactory

- **The state allows UOCAVA voters to return completed ballots electronically, via email or fax.[948]**

Voting machine certification requirements: Fair

- **Before they may be purchased and used in the state, all voting machines must be certified by the Election Assistance Commission.[949]**
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[950]

Pre-election logic and accuracy testing: Fair

- **Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[951]**
- Testing is open to the public.[952]
- Testing occurs within two weeks of an election.[953]

Nevada

While it is good that Nevada uses voting machines that provide an auditable paper record, the state's post-election audits are also lacking important criteria. For example, the number of ballots included in an audit is based on a fixed percentage depending on the population size of a given county rather than a statistically significant number tied to the margin of victory in one or more ballot contests. Nevada does not require cybersecurity training for election officials and has not yet partnered with DHS to identify and assess potential threats to its voter registration system, though we are told that Nevada Secretary of State Barbara Cegavske serves as an alternate on the Election Infrastructure Sector Government Coordinating Council, which is comprised of representatives from the Department of Homeland Security (DHS), Election Assistance Commission (EAC), the National Association for Secretaries of State (NASS), as well as state and local election officials. While recognizing the importance of state autonomy when it comes to elections, federal agencies with expertise in cybersecurity and access to classified information on contemporaneous cyberthreats have the personnel and resources necessary to thoroughly probe and analyze complex election databases, machines, and cyber vulnerabilities. Furthermore, Nevada allows voters stationed or living overseas to return voted ballots electronically, a practice that election security experts say is notoriously insecure The state's ballot accounting and reconciliation procedures also need improvement. The state did earn points for requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines before being purchased or used in the state, and for requiring election officials to carry out pre-election logic and accuracy testing on all voting machines that will be used in an upcoming election.

It would be a good idea for Nevada to eventually switch over to a statewide paper ballot voting system. Encouragingly, we were told that some counties are considering switching over to paper ballots and optical scanners for the 2018 elections. Moreover, the scope of a post-election audit should be based on a statistically significant number tied to the margin of victory in one or more ballot contests. Given the threat posed by sophisticated nation-states seeking to disrupt U.S. elections, it

is imperative that post-election audits test the accuracy of election outcomes and detect any possible manipulation. Nevada should also require that electronic poll books undergo pre-election testing prior to Election Day to ensure that they are in good working order. In addition, the state should prohibit voters from returning voted ballots electronically. We are told that Nevada has a UOCAVA ballot return rate of 91.2 percent, due, at least in part, to the state's Effective Absentee System for Elections (EASE) online ballot delivery system. However, under the current threat environment, going forward, all voted ballots should be returned by mail or delivered in person. Finally, Nevada can strengthen its ballot accounting procedures by requiring counties to compare and reconcile precinct totals with composite results to confirm they add up to the correct number.

Minimum cybersecurity standards for voter registration system: Mixed

- The state's voter registration is estimated to be at least 10 years old.[954]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[955]
- The state's voter registration system has logging capabilities at the county level to track modifications to the database.[956]
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[957]
- The state performs regular vulnerability assessments on its voter registration system.[958]
- The state has not enlisted the National Guard or DHS to help assess and identify potential threats to its voter registration system. Nevada Secretary of State Barbara Cegavske serves as an alternate on the Election Infrastructure Sector Government Coordinating Council, which is comprised of representatives from the Department of Homeland Security (DHS), Election Assistance Commission (EAC), the National Association for Secretaries of State (NASS), and state and local election officials from around the country.[959]
- The state does not require cybersecurity training for election officials. Rather, it is left up to the counties whether to provide cybersecurity training to their election personnel.[960]
- Electronic poll books are used by some, but not all, jurisdictions in the state.[961] By 2018, all counties are expected to employ electronic poll books.[962] Paper voter registration lists are available at polling places that use electronic poll books on Election Day.[963] Pre-election testing of electronic poll books is left up to the counties that use them.[964]

On June 2, 2017, Nevada Gov. Brian Sandoval (R) signed Assembly Bill 471, which establishes an Office of Cyber Defense Coordination within the state's Department of Public Safety.[965] The new "cyber defense center" will be responsible for detecting, preventing, and responding to cyberthreats against government and citizen data.[966] More specifically, the office will conduct regular vulnerability assessments on state databases, develop and provide cybersecurity training to state personnel, and launch a cybersecurity response team.[967]

Voter-verified paper audit trail: Fair

- Elections are carried out using DRE machines with VVPR;[968] Carson City will use ballot-marking devices for the 2018 elections.[969]

Some counties in Nevada are considering switching over to paper ballots and optical scanners for the 2018 elections. Carson City will be using ballot marking devices for the 2018 elections.[970]

Post-election audits: Fair

- The state conducts mandatory post-election audits.[971]
- The state's audits are carried out through manual hand count.[972]
- County clerks in counties with populations of at least 100,000 are tasked with selecting 2 percent of all voting machines in the county or at least 20 machines—whichever is greater—for auditing.[973] County clerks in counties with populations of fewer than 100,000 are tasked with selecting 3 percent of all voting machines in the county or at least four machines—whichever is greater—for auditing.[974]
- The voting machines included in the audit are selected randomly.[975]
- All categories of ballots—regular, early voting, absentee, provisional, and UOCAVA—are eligible for auditing.[976]
- An audit escalates in the event that the preliminary outcome is found to be incorrect.[977]
- Audits are open to the public and the results are made public.[978]
- Audits must be completed within seven business days after an election, before certification of election results.[979]
- An audit can reverse the preliminary outcome of an audited contest if an error is detected.[980]

Ballot accounting and reconciliation: Unsatisfactory

- All ballots are accounted for at the precinct level.[981]
- Precincts are required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[982]
- Counties are not explicitly required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[983]
- Counties are required to account for and review to ensure that all voting machine memory cards have been properly loaded onto the tally server.[984]
- While state law requires that election results be made public, it is unclear whether the same is true of information regarding ballot reconciliation processes and results.[985]

Paper absentee ballots: Unsatisfactory

- The state permits UOCAVA voters to submit completed ballots electronically, via email or by fax.[986]

Voting machine certification requirements: Fair

- Before being purchased and used for any election in the state, all voting machines must undergo testing by a federally accredited laboratory.[987]
- All of the state's counties plan on having new machines in place for the 2018 election.[988]

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[991]
- Testing is open to the public.[992]
- Testing occurs no more than two weeks before an election and must be carried out by 5 p.m. on the day before the first day of early voting.[993]

All of Nevada's 17 counties plan on having new voting machines in place for the 2018 election.[989]

The Nevada legislature passed a bill to provide $8 million in grants to counties for the purposes of purchasing new voting equipment, $35,000 of which may be used to purchase electronic poll books.[990]

New Hampshire

New Hampshire conducts its elections with paper ballots, but its failure to require post-election audits leaves the state open to undetected hacking and other Election Day problems. New Hampshire also does not require voting machines to be tested to EAC Voluntary Voting System Guidelines. Unfortunately, state officials—citing legal concerns—refused to provide us with information on cybersecurity protocol for its voter registration system, and we were unable to locate all of the information independently. Even if the state is adhering to all of the minimum cybersecurity best practices under that category, its overall grade would not be raised given the point distribution for the other categories. The state did earn points for its ballot accounting and reconciliation procedures and for prohibiting voters stationed or living overseas from returning voted ballots electronically. In New Hampshire all voted ballots must be returned by mail or delivered in person. The state also exercises good practices by requiring election officials to conduct pre-election logic and accuracy testing on all machines that will be used in an upcoming election.

To improve its overall election security, New Hampshire should immediately establish robust post-election audits that test the accuracy of election outcomes after every election. In doing so, state officials should look to risk-limiting audits like those in Colorado as a potential model. New Hampshire should also explicitly require that all voting machines be tested to EAC Voluntary Voting System Guidelines before being purchased or used in an election. Doing so would ensure that all voting machines meet a basic level of functionality, security, and accessibility, which can prevent machine malfunction and other disruptions on Election Day.

Minimum cybersecurity standards for voter registration system: Incomplete

**State officials—citing legal reasons—refused to share information on cybersecurity requirements for the state's voter registration system.[994] Information gathered for this section derives from independent research.*

- The state's voter registration system has received cybersecurity updates since being put into place at least 10 years ago.[995]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[996]
- State officials were unable to provide us with information on whether the state's voter registration system has logging capabilities to track modifications to the database.
- State officials were unable to provide us with information on whether the state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.
- State officials were unable to provide us with information on whether the state performs regular vulnerability assessments on its voter registration system.
- State officials were unable to provide us with information on whether the state has enlisted the National Guard or DHS to help assess and identify potential threats to its voter registration system.
- The state provides cybersecurity training to election officials.[997]
- While the state does not currently use electronic poll books, the state legislature passed a law in 2017 to establish a pilot program for electronic poll books.[998] However, because New Hampshire does not currently use electronic poll books, the state was not graded on e-pollbook best practices.

Voter-verified paper audit trail: Good

- Elections are carried out using paper ballots and optical scan counting devices.[999]

Post-election audits: Unsatisfactory

- The state does not require post-election audits.[1000]

Ballot accounting and reconciliation: Fair

- All ballots are accounted for at the polling place.[1001]
- Polling places are required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[1002]
- Reporting jurisdictions are required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[1003]
- The state does not use a tally server. As such, a memory card review process is unnecessary.[1004]
- The state requires that all election results and ballot reconciliation information and processes be made public.[1005]

Paper absentee ballots: Fair

- The state does not permit voters—including UOCAVA voters—to submit completed ballots electronically. All ballots must be returned by mail or delivered in person.[1006]

Voting machine certification requirements: Unsatisfactory

- The state does not require voting machines to meet federal requirements before they are purchased and used in elections in the state.[1007]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[1008]

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[1009]
- Testing is open to the public.[1010]
- Testing occurs no later than the Wednesday before an election.[1011]

New Jersey

New Jersey allows voting using machines that do not provide a paper record and fails to mandate post-election audits, which does not provide confirmation that ballots are cast as the voter intends and counted as cast. New Jersey's ballot accounting and reconciliation procedures are also lacking in certain respects. The state did earn points for requiring election officials to carry out pre-election logic and accuracy testing on all machines that will be used in an upcoming election. Also, while the state would not normally receive credit for allowing UOCAVA voters to return voted ballots by email or fax, we award the state a point for requiring that any electronically returned ballot be coupled with a paper copy of the voter's ballot.

Until New Jersey switches to a statewide paper-based voting system and requires post-election audits, its elections will remain vulnerable. New Jersey should immediately require that all future elections be carried out using paper ballots, and put into place robust post-election audits that test the accuracy of election outcomes. In crafting its audit requirements, state officials should look to risk-limiting audits like those in Colorado as a potential model. Given the threat posed by sophisticated nation-states seeking to disrupt U.S. elections, it is imperative that post-election audits test the accuracy of election outcomes and detect any possible manipulation. New Jersey should also strengthen its ballot accounting and reconciliation procedures by requiring precincts to compare and reconcile the number of ballots with the number of voters who signed in at the polling place and by requiring counties to compare and reconcile precinct totals with composite results to confirm they add up to the correct number. Furthermore, state law should explicitly require that all voting machines be tested to EAC Voluntary Voting System Guidelines before being purchased or used in the state. Even though all voting machines currently in use meet or exceed the federal requirements. All future machines must be explicitly required to adhere to baseline functionality, security, and accessibility standards established by the EAC.

Minimum cybersecurity standards for voter registration system: Good

- The state's voter registration system is estimated to be at least 10 years old.[1012]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[1013]
- The state's voter registration system has logging capabilities to track modifications to the database.[1014]
- The state is in the process of developing an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[1015]
- The state performs regular vulnerability assessments on its voter registration database.[1016]
- The state has enlisted DHS to help assess and identify potential threats to its voter registration system.[1017]
- Members of the New Jersey Association of Election Officials attend a training twice a year that includes cybersecurity training.[1018] The state is working with DHS to develop additional training.[1019]
- The state does not use electronic poll books, and therefore was not graded on e-pollbook best practices.[1020]

Voter-verified paper audit trail: Unsatisfactory

- Elections are carried out using paperless DRE machines.[1021]

Legislation introduced in 2018 would require future elections to be carried out exclusively with paper ballots.[1022]

Post-election audits: Unsatisfactory

- The state does not require post-election audits.[1023] The state does have a statutory procedure on the books for conducting public post-election audits on DRE machines with VVPR, if they were used. Such an audit would include at least 2 percent of election districts in each county. The precincts, districts, and machines included in the audit would be randomly selected, and provisional ballots would not be included. In terms of timing, the law specifies that audits must occur within a "reasonable period of time" after the final vote count but before certification. If discrepancies arise that call into question the accuracy of election results, an audit can expand to include additional jurisdictions or machines.[1024]

Ballot accounting and reconciliation: Unsatisfactory

- State law requires that all ballots be accounted for at the precinct level.[1025]
- Precincts are not required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[1026]
- Counties are not explicitly required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[1027]
- Counties review and account for all voting machine memory cards or flash drives to ensure they are properly loaded onto the tally server.[1028]

- State law requires that election results be made public.[1029] Ballot reconciliation takes place at public meetings held by the County Board of Elections, and the meeting minutes are publicly available.[1030]

Paper absentee ballots: Fair

- The state permits UOCAVA voters to return ballots electronically, via email or fax. However, voters who do must also submit a hard copy of the completed ballot through the mail.[1031]

Voting machine certification requirements: Fair

- State law does not require voting machines to meet federal requirements before they are purchased and used in elections in the state. In practice, however, all voting machines undergo testing by a federally accredited laboratory.[1032]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[1033]

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[1034]
- Testing is open to the public.[1035]
- The law does not specify precisely when testing must be carried out, merely requiring that testing be conducted "prior to the start of the count of the ballots."

New Mexico

New Mexico received high scores for its use of paper ballots and adherence to many cybersecurity best practices, though the state would do well to require backup paper copies of voter registration lists at polling places using electronic poll books in case problems arise. And while fairly good overall, New Mexico's post-election audit procedures, which includes counting a set, tiered number of ballots, prevent election officials and the public from knowing with a high degree of certainty whether election outcomes are correct. The tiered workload lead to a weaker overall audit than if the size of the audit were based on the specific margin of victory—rather than a set range—in a given ballot contest, as is common with risk-limiting audits. Adding to this is the fact that the state allows voters stationed or living overseas to return voted ballots electronically, which leaves its elections vulnerable to manipulation and undermines the overall effectiveness of its audits. The state did earn points for its ballot accounting and reconciliation procedures and for requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines. Additionally, New Mexico requires election officials to carry out pre-election logic and accuracy testing on all machines that will be used in an upcoming election.

To improve its overall election security, New Mexico should strengthen its post-election audit procedures to ensure that they are robust enough to correct incorrect election results by basing the number of ballots included in a post-election audit on a statistically significant number tied to the specific margin of victory in a given ballot contest. The state should also require that backup paper voter registration lists be available at polling places that use electronic poll books, in case of emergency. Although the state requires that backup electronic poll books be provided, these electronic backups will do nothing to ensure that eligible voters can cast ballots that count when they show up to the polls if there is widespread system failure or a major cyber breach, which would corrupt the entire electronic database. Finally, New Mexico should prohibit electronic absentee voting, which has been deemed insecure by election security experts. All voted ballots should be return by mail or delivered in person.

Minimum cybersecurity standards for voter registration system: Fair

- The state's voter registration system underwent a complete update in December 2017.[1036]
- The state's voter registration system provides access control to ensure that only authorized personnel can access the database.[1037]
- The state's voter registration system has logging capabilities to track modifications to the database.[1038]
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[1039]
- The state performs regular vulnerability assessments on its voter registration system.[1040]
- The state has enlisted either the National Guard or DHS to help assess and identify potential threats to its voter registration system.[1041]
- The state requires election officials to undergo cybersecurity training as part of the state's "election schools," which are required of all county officials prior to any statewide election.[1042]
- Electronic poll books are used by some, but not all, jurisdictions in the state.[1043] The state does not require polling places using electronic poll books to have backup paper copies of voter registration lists available in case of emergency.[1044] However, backup electronic poll books are available at polling places on Election Day.[1045] Election officials conduct pre-election testing on electronic poll books prior to an election.[1046]

New Mexico's voter registration system underwent a complete update in December 2017.[1047]

Voter-verified paper audit trail: Good

- Elections are carried out using paper ballots and optical scan machines.[1049]

Post-election audits: Fair

- The state conducts mandatory post-election audits.[1050]
- The state's post-election audits are conducted through manual hand count.[1051]
- Audits are "conducted for all federal offices, for governor and for the statewide elective office, other than the office of the governor, for which the winning candidate won by the smallest percentage margin of all candidates for statewide office in New Mexico."[1052] The sample size must ensure with at least 90 percent probability that faulty tabulators would be detected if they had changed the outcome of the election. The precise number of precincts selected depends on the ranged margin of victory between the top two candidates in a race. For example, if the margin of victory between the candidates was greater than 14 but less than or equal to 15, four precincts would be audited. If the margin of victory was 0.5 or less, 165 precincts would be audited.[1053]

New Mexico began offering cybersecurity training to election officials in 2016, largely in response to attempts by hackers to infiltrate voter registration systems in Illinois and Arizona. The hacking attempts were incorporated into a lesson plan and used as case studies. The training included information on the utility of cybersecurity protections and the proper usage of voter registration databases.[1048]

- The precincts included in the audit are selected randomly.[1054]
- Provisional ballots are not included in the post-election audit and are hand counted separately.[1055]
- An audit escalates to include more voting components in the event that preliminary outcomes are found to be incorrect.[1056]
- Audit results are publicly available.[1057]
- Audits are carried out before certification.[1058]
- An audit can reverse the preliminary outcome of an audited contest if an error is detected and a full recount of the contest is ordered by the canvassing board.[1059]

**Although New Mexico's post-election audit procedures are fair, the state's allowance of electronic absentee voting undermines the audits' overall effectiveness.*

Ballot accounting and reconciliation: Fair

- All ballots are accounted for at the precinct level.[1060]
- Precincts are required to reconcile the number of ballots with the number of voters who signed in at the polling place.[1061]
- Counties are required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[1062]
- Although there is no statutorily mandated review process to ensure that all voting machine memory cards have been properly loaded onto the tally server at the county level, this process is conducted in practice.[1063]
- The state requires that vote tallies and ballot reconciliation information be made public.[1064]

Paper absentee ballots: Unsatisfactory

- The state permits UOCAVA voters to submit completed ballots electronically, via email or fax.[1065]

Voting machine certification requirements: Fair

- Before being purchased and used for any election in the state, all voting machines must undergo testing by a federally accredited laboratory.[1066]
- The state's voting machines were replaced statewide in 2014.[1067]

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[1068]
- The law does not specifically require that testing be open to public observance.
- Testing occurs between two weeks and one month before an election.[1069]

New York

New York adheres to recommended minimum cybersecurity best practices related to voter registration systems and conducts its elections with paper ballots, but its post-election audit procedures lack important criteria that leave the state vulnerable to Election Day problems. Currently, post-election audits may be carried out electronically through automated retabulation, which is vulnerable to hacking. Additionally, the number of ballots included in an audit is tied to a fixed percentage, rather than a statistically significant number tied to the margin of victory in one or more ballot contests. Furthermore, the state audit law lacks specifics on whether all ballot categories—including early voting, absentee, and provisional ballots—must be included, and whether audits are open to the public. The state's ballot accounting and reconciliation procedures can also be improved. New York did earn points for prohibiting absentee voters from returning voted ballots electronically, a practice that election security experts say is notoriously insecure. In New York, all voted ballots must be returned by mail or delivered in person. The state also exercises good practices by requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines, and for requiring election officials to carry out pre-election logic and accuracy testing on all machines that will be used in an upcoming election.

To improve its overall election security, New York should look to risk-limiting audits like those in Colorado as a potential model for updating its post-election audit procedures. By making changes in this area, the state could improve both election security and public confidence in election outcomes. Finally, New York should also strengthen its ballot accounting and reconciliation procedures by requiring counties to compare and reconcile precinct totals with composite results to confirm they add up to the correct number.

Minimum cybersecurity standards for voter registration system: Good

**State officials were unable to share information on cybersecurity requirements for the state's voter registration system. Information gathered for this section derives from independent research.*

- The state's voter registration system has been updated within the past 10 years.[1070]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[1071]
- The state's voter registration system has logging capabilities to track modifications to the database.[1072]
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[1073]
- The state performs regular vulnerability assessments on its voter registration system.[1074]
- The state has enlisted DHS to help assess and identify potential threats to its voter registration system.[1075]
- The state provides cybersecurity training to election officials.[1076]
- The state does not use electronic poll books, and therefore was not graded on e-pollbook best practices.[1077]

Voter-verified paper audit trail: Good

- Elections are carried out using paper ballots and optical scan machines.[1080]

Post-election audits: Mixed

- The state conducts mandatory post-election audits.[1081]
- The state's post-election audits may be conducted by manual hand count or electronically through automated retabulation.[1082]
- Audits are conducted on 3 percent of voting machines or systems within the jurisdiction of each local board of elections.[1083]
- The machines or systems included in the audit are selected randomly.[1084]
- There is no statutory requirement dictating whether absentee or provisional ballots must be included in an audit. However, we are told that absentee and provisional ballots are included in post-election audits for jurisdictions that use electronic automated tabulation to count ballots.[1085]
- An audit escalates to include more voting components in the event that discrepancies occur between the initial audit results and the preliminary outcome and can result in a full recount if necessary.[1086]
- The audit is open to the public.[1087]
- Audits are conducted prior to certification.[1088]
- An audit that results in a full recount can reverse the preliminary outcome of an audited contest if an error is detected.[1089]

In December 2017, New York Gov. Andrew Cuomo (D) announced a new election security initiative as part of his 2018 State of the State agenda, including creating a state Election Support Center, developing an Elections Cyber Security Support Toolkit, and providing Cyber Risk Vulnerability Assessments and Support for Local Boards of Elections, among other things.

New York Gov. Andrew Cuomo (D) ordered an in-depth review of the state's cybersecurity practices related to election infrastructure.[1078] The New York State Cyber Security Advisory Board is working alongside state agencies—including the Department of Motor Vehicles and the Office of Information Technology Services—as well as state and county boards of elections to identify possible vulnerabilities and provide recommendations.[1079]

Legislation introduced in 2018 would require the board of elections or a bipartisan committee appointed by such a board to conduct risk-limiting audits.[1090]

Ballot accounting and reconciliation: Fair

- All ballots are accounted for at the precinct level.[1091]
- Precincts are required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[1092]
- Counties are required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[1093]
- Counties review and account for all voting machine memory cards or flash drives to ensure they have been properly loaded onto the tally server, to the extent they are used.[1094]
- State law requires that election results be made public, and the vote canvassing process—where decisions about ballot reconciliation are made—is open to the public.[1095]

Paper absentee ballots: Fair

- The state does not permit voters—including UOCAVA voters—to submit completed ballots electronically. All ballots must be returned by mail or delivered in person.[1096]

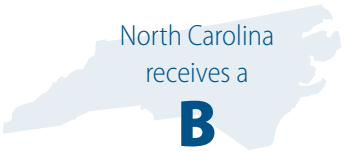
Voting machine certification requirements: Fair

- Before being purchased and used for an election, all voting machines must be shown to meet or exceed federal voting system standards.[1097]
- All voting machines in New York have likely been replaced within the past 10 years.[1098]

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[1099]
- The law does not specifically require that testing be open to public observance.[1100]
- Voting machines are tested annually. Voting machines that will be used in an election must be tested before the start of voting.[1101]

North Carolina



North Carolina adheres to a number of minimum cybersecurity best practices related to voter registration systems and conducts its elections using paper ballots and voting machines that provide a paper record. However, its post-election audits do not currently include provisional ballots. North Carolina allows voters stationed or living overseas to return voted ballots electronically, a practice that election security experts say is notoriously insecure. The state did earn points for requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines before being purchased or used in the state, and for requiring election officials to carry out pre-election logic and accuracy testing on all machines that will be used in an upcoming election.

To protect its elections from potential manipulation, North Carolina should adopt robust post-election audits that adequately test the accuracy of election outcomes. In updating its requirements, the state should look to risk-limiting audits like those in Colorado as a potential model. Given the threat posed by sophisticated nation-states seeking to disrupt U.S. elections, it is imperative that post-election audits test the accuracy of election outcomes and detect any possible manipulation. North Carolina should also make sure that any cybersecurity training that state officials receive includes training specific to election security. The state should also prohibit electronic absentee voting, even by UOCAVA voters who are currently allowed to return voted ballots by email or fax. All voted ballots should be returned by mail or delivered in person.

Minimum cybersecurity standards for voter registration system: Good

- The state's voter registration system is estimated to be at least 10 years old.[1102] However, the North Carolina State Board of Elections maintains an in-house technical staff of approximately 19 employees to maintain and update the state's voter registration system.[1103]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[1104]

- The state's voter registration system has logging capabilities to track modifications to the database.[1105]
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[1106]
- The state partners with DHS for regular security and vulnerability assessments in addition to monitoring through North Carolina's Department of Information Technology and in-house controls.[1107]
- The state has enlisted DHS to help assess and monitor state voter registration systems and identify potential vulnerabilities.[1108]
- Although election officials do not receive training specific to elections, all state employees must receive some basic cybersecurity training.[1109]
- Electronic poll books are used by some, but not all, jurisdictions in North Carolina.[1110] The state conducts pre-election testing on electronic poll books prior to an election.[1111] All polling places that use electronic poll books are required to have paper backups of voter registration lists available on Election Day.[1112]

Voter-verified paper audit trail: Fair

- Depending on the jurisdiction, some voters in North Carolina currently cast paper ballots, while others vote using DRE machines with VVPR.[1114] Roughly three-quarters of North Carolina counties rely exclusively on paper ballots. By 2019, North Carolina will phase out all DRE machines and switch to a statewide paper ballot voting system.[1115]

North Carolina's partnership with the Department of Homeland Security has broadened beyond cybersecurity assessments and includes physical security assessments.[1113]

Post-election audits: Fair

- The state requires post-election audits.[1116]
- The state's post-election audits are conducted through manual hand count.[1117]
- Audits include a statistically significant number—determined in consultation with a statistician—of precincts or ballot groupings derived from absentee or early voting.[1118] Usually two precincts or ballot contests are considered enough to produce a "statistically significant result," as required by state law.[1119] Only one ballot contest is required to be included in an audit. During presidential election years, the contest to be audited must be the presidential contest. Two or more ballot contests are sometimes audited for municipal elections.[1120]
- The precincts or ballot groupings included in the audit are selected randomly.[1121]

- Provisional ballots are not included in manual audits.[1122] North Carolina's extensive post-election audit procedures include examining provisional ballots to determine voter eligibility.[1123]
- An audit escalates in the event that preliminary outcomes are found to be incorrect up to a full recount if necessary.[1124]
- The audits are open to the public.[1125]
- Audits typically occur within 24 hours after an election and are usually completed by the Thursday after Election Day, prior to certification of official election results.[1126]
- An audit can reverse the preliminary outcome of an audited contest if a significant discrepancy is discovered and a full hand count is ordered.[1127]

Ballot accounting and reconciliation: Fair

- All ballots are accounted for at the precinct level.[1128]
- Precincts are required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[1129]
- Counties are required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[1130] Reconciliation is monitored by the state through the election management system.[1131]
- Counties are required to review and ensure that all voting machine memory cards have been properly loaded onto the tally server.[1132]
- State law requires that election results be made public, and while the state does not publish a full report on ballot reconciliation procedures, it is required to furnish public information, including election data, to any requesting party not covered by a very narrow list of exceptions in state law.[1133]

Paper absentee ballots: Unsatisfactory

- The state permits UOCAVA voters to submit completed ballots, via email or fax.[1134]

Voting machine certification requirements: Fair

- Before being purchased and used for any election in the state, all voting machines must undergo testing by a federally accredited laboratory.[1135]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[1136]

Pre-election logic and accuracy testing: Fair

- **Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.**[1137]
- Testing is open to the public.[1138]
- The law does not specify precisely when testing must be carried out.

North Dakota

North Dakota conducts its elections with paper ballots, but its failure to carry out post-election audits that test the accuracy of election outcomes leaves the state open to undetected hacking and other Election Day problems. On election night, the state conducts a test on the voting machines in one precinct in each county. The test involves retabulating a set of test ballots to ensure that the machines are working correctly. This kind of automated retabulation is insufficient for detecting and confirming potential manipulation or errors in election outcomes. State officials—citing security reasons—were unable to provide us with information on some cybersecurity standards for the state's voter registration system and we were unable to locate all of the information independently. Even if the state is adhering to all of the minimum cybersecurity best practices under that category, its overall grade would not be raised given the point distribution for the other categories. North Dakota allows voters stationed or living overseas to return voted ballots electronically, a practice that election security experts say is notoriously insecure. The state did earn points for its ballot accounting and reconciliation procedures and for requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines. North Dakota also exercises best practices by requiring election officials to carry out pre-election logic and accuracy testing on all machines that will be used in an upcoming election.

To improve its overall election security, North Dakota should immediately establish robust post-election audits that test the accuracy of election outcomes. In doing so, the state should look to risk-limiting audits like those in Colorado as a potential model. North Dakota should also require electronic poll books to undergo pre-election testing to ensure that they are in good working order before Election Day and should also require backup paper voter registration lists to be made available in case of emergency. Finally, the state should prohibit voters stationed or living overseas from returning voted ballots electronically. Going forward, all voted ballots should be returned by mail or delivered in person.

Minimum cybersecurity standards for voter registration system: Incomplete

**State officials—citing security concerns—were unable to share information on some cybersecurity requirements for the state's voter registration system, particularly that related to intrusion detection systems.*

- The state's central voter file database has been updated within the past 10 years.[1139]
- The state's central voter file database provides access control to ensure that only authorized personnel have access to the database.[1140]
- The state's central voter file has logging capabilities to track modifications to the database.[1141]
- State officials were unable to provide us with information on whether the state's central voter file database includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities. According to the state's election director, "All of our IT is hosted centrally … [the] security team handles all cybersecurity for our Central Voter File, as well as all other hosted applications."[1142]
- The state conducts regular vulnerability assessments and penetration testing on its central voter file database.[1143]
- The state has enlisted the help of DHS to help assess and identify potential threats to its central voter file database and election infrastructure.[1144]
- The state has begun holding conferences with election officials on cyberthreats to election systems and administration.[1145] The state anticipates continuing these information and training sessions for future elections.[1146]
- Electronic poll books are used by some, but not all, jurisdictions in the state.[1147] Pre-election testing of electronic poll books is left up to the counties that use them.[1148] Backup paper voter registration lists are not required at jurisdictions using electronic poll books.[1149] All jurisdictions are required to have voter registration lists on electronic file and available for printing, if necessary.[1150]

Voter-verified paper audit trail: Good

- Elections are carried out using paper ballots and optical scan machines.[1151]

Post-election audits: Unsatisfactory

- The state does not conduct mandatory post-election audits.[1152] On election night, the state conducts a test of the voting machines in one precinct in each of the state's 53 counties. The test consists of retabulating a set of ballots to ensure that the machines are working correctly.[1153]

Ballot accounting and reconciliation: Fair

- All ballots are accounted for at the precinct level.[1154]
- Precincts are required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[1155]
- Counties are required to compare and reconcile precinct totals with county-wide results to ensure that they add up to the correct amount.[1156]
- Counties are required to review and ensure that all voting machine memory cards have been properly loaded onto the tally server.[1157]
- The state requires that vote tallies and ballot reconciliation information be made public.[1158]

Paper absentee ballots: Unsatisfactory

- The state permits UOCAVA voters to submit completed ballots electronically via fax or web portal.[1159]

Voting machine certification requirements: Fair

- Before being purchased and used for any election in the state, all voting machines must undergo testing by a federally accredited laboratory.[1160]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[1161]

In 2017, North Dakota's legislature rejected funding proposals that would have allowed the state to purchase new voting machines.[1162]

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[1163]
- Testing is open to the public.[1164]
- A public test is conducted one week before an election. Internal nonpublic testing takes place earlier, approximately three weeks before an election.[1165]

Ohio

Ohio uses paper ballots and voting machines that provide a paper record, but its post-election audit requirements are lacking important criteria. For example, the number of ballots included in an audit is based on a fixed percentage rather than a statistically significant number tied to the margin of victory in one or more ballot contests. The state's ballot accounting and reconciliation procedures also need improvement. The state did earn points for requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines and for requiring election officials to carry out pre-election logic and accuracy testing on all machines that will be used in an upcoming election. It also exercises good practices by prohibiting voters stationed or living overseas from returning voted ballots electronically. In Ohio, all voted ballots are returned by mail or delivered in person.

Despite numerous attempts to speak to someone in state government about the cybersecurity standards for the state's voter registration system, state officials did not respond to requests for information and comment on our research, and we were unable to locate all of the information independently. If Ohio is adhering to all of the minimum cybersecurity best practices for voter registration systems, it would receive a "good" score—worth 3 points—for that category, bringing its grade up to a B.

To improve its overall election security, Ohio should immediately update its post-election audit requirements to ensure that they adequately test the accuracy of election outcomes with a high degree of confidence. In doing so, the state should look to codify risk-limiting audits like those in Colorado as a potential model. Given the threat posed by sophisticated nation-states seeking to disrupt U.S. elections, it is imperative that post-election audits test the accuracy of election outcomes and detect any possible manipulation. Ohio should also firm up its ballot accounting and reconciliation procedures. For example, the state should explicitly require that precincts using DRE machines with VVPR compare and reconcile the number of ballots with the number of voters who signed in at the polling place. At the same time, counties should be required to compare and reconcile precinct totals with composite results to confirm they add up to the correct number.

Minimum cybersecurity standards for voter registration system: Incomplete

**State officials did not respond to our requests for information and comment on cybersecurity requirements for the state's voter registration system. Information gathered for this section derives from independent research. If Ohio does require the missing cybersecurity best practices, its grade would be raised from a C to a B.*

- The state's voter registration system is estimated to be at least 10 years old.[1166]
- State officials were unable to provide us with information on whether the state's voter registration system provides access control to ensure that only authorized personnel have access to the database.
- State officials were unable to provide us with information on whether the state's voter registration system has logging capabilities to track modifications to the database.
- State officials were unable to provide us with information on whether the state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.
- State officials were unable to provide us with information on whether the state performs regular vulnerability analysis on its voter registration system.
- The state has enlisted the National Guard and has worked with DHS to help assess and identify potential threats to its voter registration system.[1167]
- State officials were unable to provide us with information on whether the state provides cybersecurity training to election officials.
- Electronic poll books are used by some, but not all, jurisdictions in the state.[1168] The state conducts pre-election testing on electronic poll books prior to an election.[1169] Paper voter registration lists are available at polling places that use electronic poll books on Election Day.[1170]

Voter-verified paper audit trail: Fair

- Depending on the jurisdiction, some voters in Ohio cast paper ballots, while others vote using DRE machines with VVPR.[1171]

Post-election audits: Fair

- The state conducts mandatory post-election audits.[1173] While jurisdictions may use a "simple, percentage-based post-election audit or a risk-limiting audit," the state recommends conducting risk-limiting audits.[1174]
- The state's post-election audits are conducted through manual hand count.[1175]
- It is within the discretion of the county board of elections whether to carry out the audit by precinct, polling place, or by individual voting machine, though "[i]t is preferable to audit the smallest unit available."[1176] The number of units

Legislation introduced in January 2018 would require Ohio to conduct elections exclusively by paper ballot, establish a cybersecurity directory within the Secretary of State's Office, and put into place a cybersecurity advisory council with an eye towards making Ohio elections more secure.[1172]

included in the audit must "equal at least 5% of the total number of votes cast for the county."[1177] If auditing by precinct and the precinct's vote count is greater than or equal to 5 percent, an additional precinct must be audited. The same is true if auditing by polling place.[1178] Audits include at least three ballot contests, including one top-of-the-ticket race, at least one other statewide race, and at least one nonstatewide contest.[1179]

- The election units included in the audit are selected randomly.[1180]
- All categories of ballots—regular, early voting, absentee, provisional, and UOCAVA—are eligible for auditing.[1181]
- Escalation is required if a county audit's "accuracy rate is less than 99.5% in a contest with a certified margin that is at least 1% (calculated as a percentage of ballots cast on which the contest appeared), or less than 99.8% in a contest with a certified margin that is less than 1%. Escalation entails drawing a second random sample of at least 5% of votes cast, selected from units that were not audited in the original sample, and auditing the ballots (using the same procedures) with respect to any such contest. If, after the second round of auditing, the accuracy rate from the two samples is below 99.5%, the county shall investigate the cause of the discrepancy and report its findings to the Secretary of State's Office," at which point the secretary of state may order a full manual recount.[1182]
- Audits are open to the public and the results are made publicly available.[1183]
- Although audits are carried out after certification, an audit can reverse or correct election outcomes if an error is detected.[1184]

Ballot accounting and reconciliation: Unsatisfactory

- All ballots are accounted for at the precinct level.[1185]
- Precincts using paper ballots are required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place,[1186] though it is unclear whether these requirements also apply to jurisdictions using DRE machines.[1187]
- Counties are not explicitly required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[1188]
- There is no statutorily mandated review process to ensure that all voting machine memory cards have been properly loaded onto the tally server at the county level.[1189]
- While state law requires that election results be made public, it is unclear whether the same is true of information regarding ballot reconciliation processes and results.[1190]

Paper absentee ballots: Fair

- The state does not permit voters—including UOCAVA voters—to submit completed ballots electronically. All ballots must be returned by mail or delivered in person.[1191]

Voting machine certification requirements: Fair

- Before they may be purchased and used in the state, all voting machines must be certified by the Election Assistance Commission.[1192]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[1193]

"It is time for the state's leaders to step forward and approve a funding plan to replace Ohio's aging voting technology."
– Ohio Secretary of State Jon Husted[1194]

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[1195]
- Testing is open to the public.[1196]
- The law does not specify precisely when testing must be carried out.

Oklahoma

Oklahoma conducts its elections with paper ballots, but its failure to require post-election audits leaves the state open to undetected hacking and other Election Day problems. Oklahoma also allows voters stationed or living overseas to return voted ballots electronically, a practice that election security experts say is notoriously insecure. Its ballot accounting and reconciliation procedures also need improvement. Oklahoma did earn credit for requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines before being purchased or used in the state and for requiring election officials to carry out pre-election logic and accuracy testing on all machines that will be used in an upcoming election.

Despite numerous attempts to speak to someone in state government about the cybersecurity standards for the state's voter registration system, state officials did not respond to our requests for information and comment, and we were unable to locate all of the information independently. Even if Oklahoma is adhering to all of the minimum cybersecurity best practices for voter registration systems its overall grade would not change, given the point distribution for the other categories.

To improve its overall election security, Oklahoma should immediately adopt robust post-election audits that confirm the accuracy of election outcomes. In doing so, the state should look to risk-limiting audits like those in Colorado as a potential model. Given the threat posed by sophisticated nation-states seeking to disrupt U.S. elections, it is imperative that post-election audits be comprehensive enough to test the accuracy of election outcomes with a high degree of confidence and detect any possible manipulation. Oklahoma should also strengthen its ballot accounting and reconciliation procedures by requiring that all ballots—used, unused, and spoiled—are fully accounted for at the precinct level. Part of this includes comparing and reconciling the number of ballots with the number of voters who signed in at the polling place. Moreover, Oklahoma should require counties to compare and reconcile precinct totals with composite results to ensure that they add up to the correct number. Finally, Oklahoma should prohibit voters stationed or living overseas from returning voted ballots electronically. All voted ballots should be returned by mail or delivered in person.

Minimum cybersecurity standards for voter registration system: Incomplete

**State officials did not respond to our requests for information and comment on cybersecurity requirements for the state's voter registration system. Information gathered for this section derives from independent research.*

- The state's voter registration system is estimated to be at least 10 years old.[1197]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[1198]
- The state's voter registration system has logging capabilities to track modifications to the database.[1199]
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[1200]
- The state performs regular vulnerability assessments on its voter registration system.[1201]
- State officials were unable to provide us with information on whether the state has enlisted the National Guard or DHS to help assess and identify potential threats to its voter registration system.
- State officials were unable to provide information on whether the state provides cybersecurity training to election officials.
- The state does not use electronic poll books, and therefore was not graded on e-pollbook best practices.[1202]

Voter-verified paper audit trail: Good

- Elections are carried out using paper ballots and optical scan machines.[1203]

Post-election audits: Unsatisfactory

- The state does not conduct post-election audits.[1204]

Ballot accounting and reconciliation: Unsatisfactory

- Ballots are not fully accounted for at the precinct level.[1205]
- Precincts are not required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[1206]
- Counties are not explicitly required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[1207]
- Counties are required to review and ensure that all voting machine memory cards have been properly loaded onto the tally server.[1208]
- While state law requires that election results be made public, it is unclear whether the same is true of information regarding ballot reconciliation processes and results.[1209]

Paper absentee ballots: Unsatisfactory

- The state allows UOCAVA voters to submit competed ballots electronically via fax.[1210]

Voting machine certification requirements: Fair

- Before being purchased and used for an election, all voting machines must be shown to meet or exceed federal voting system standards.[1211]
- All voting machines in Oklahoma have likely been replaced within the past 10 years.[1212]

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[1213]
- The law does not require that testing be open to public observance.[1214]
- The law does not specify precisely when testing must be carried out.

Oregon

Oregon adheres to a number of minimum cybersecurity best practices related to voter registration systems and uses paper ballots. However, while fairly good overall, Oregon's post-election audits, which include counting a set, tiered number of ballots, prevent election officials and the public from confirming whether election outcomes are correct. The tiered workload lead to a weaker overall audit than if the size of the audit were based the specific margin of victory—rather than a set range—in a given ballot contest, as is common with risk-limiting audits. Adding to this is the fact that the state allows voters stationed or living overseas to return voted ballots electronically—a practice that election security experts say is notoriously insecure. Oregon's ballot accounting and reconciliation procedures also need improvement. The state did earn points for requiring all voting machines to be EAC certified or tested by a federally accredited laboratory before being purchased or used in the state, and for requiring election officials to carry out pre-election logic and accuracy testing on all machines that will be used in an upcoming election.

To improve its overall election security, Oregon should ensure that its post-election audits are robust enough to correct incorrect election results by basing the number of ballots included in a post-election audit on a statistically significant number tied to the specific margin of victory in a given ballot contest. Oregon should also prohibit voters stationed or living overseas from returning voted ballots electronically. Given widespread consensus that electronic absentee voting is insecure, Oregon should require that all voted ballots be returned by mail or delivered in person. Finally, Oregon can strengthen its ballot accounting and reconciliation procedures by requiring counties to compare and reconcile precinct totals with composite results to ensure that they add up to the correct number.

Minimum cybersecurity standards for voter registration system: Good

- The state's voter registration system is estimated to be at least 10 years old.[1215]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[1216]
- The state's voter registration system has logging capabilities to track modifications to the database.[1217]

- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[1218]
- The state performs regular vulnerability assessments on its voter registration system.[1219]
- The state has enlisted either the National Guard or DHS to help assess and identify potential threats to its voter registration system.[1220]
- The state began providing cybersecurity training to election officials in December 2017 and plans to conduct more training at an in-person conference in February 2018.[1221]
- The state does not use electronic poll books, and therefore was not graded on e-pollbook best practices.[1222]

Oregon has received or is expected to receive additional funding for cybersecurity at their election agencies.[1223]

Voter-verified paper audit trail: Good

- The state is a vote-by-mail state, meaning that most votes are cast using paper ballots.[1224]

Post-election audits: Fair

- The state conducts mandatory post-election audits.[1225]
- The state's post-election audits are conducted through manual hand count.[1226]
- The number of precincts or ballot batches selected for an audit is based on a set, tiered system tied to the margin of victory in a given ballot contest.[1227] For example, if the margin of victory between the two candidates receiving the largest share of votes is less than 1 percent of the total votes cast in that election in the county, the audit includes at least 10 percent of all precincts or at least 10 percent of all batches of ballots for that county.[1228] If the margin of victory is greater than or equal to 1 percent but less than 2 percent, the audit includes at least 5 percent of all precincts or at least 5 percent of all batches of ballots for that county.[1229] If the margin of victory is greater or equal to 2 percent, the county clerk hand counts at least 3 percent of all precincts or at least 3 percent of all batches of ballots for that county.[1230]
- The precincts or ballot batches included in the audit are selected randomly.[1231]
- All categories of ballots—regular, provisional, absentee, and UOCAVA—are eligible for auditing.[1232]
- If a discrepancy of more than 0.5 percent is found between the initial outcome and the audit results, all ballots in that county must be hand counted.[1233]
- Audits are carried out prior to certification.[1234]
- Audits are open to the public and the results are made public.[1235]
- An audit can reverse the preliminary outcome of an audited contest if the discrepancy between the initial tally and the audit count is greater than 0.5 percent.[1236]

Ballot accounting and reconciliation: Unsatisfactory

- Because the state is a vote-by-mail state, it is not necessary that all ballots be accounted for at the precinct level, specifically.[1237] Election officials are required to account for all ballots at the end of Election Day.[1238]
- Because the state is a vote-by-mail state, it is not necessary that the number of ballots be compared to the number of voters at the precinct level, specifically.[1239] Counties compare and reconcile the number of ballots cast with the number of voters on the vote history roster or the number of return identification ballot envelopes.[1240]
- Counties are not explicitly required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[1241]
- There is no statutorily mandated review process to ensure that all voting machine memory cards have been properly loaded onto the tally server at the county level.[1242]
- The state requires that vote tallies and ballot reconciliation information be made public.[1243]

Paper absentee ballots: Unsatisfactory

- The state permits UOCAVA voters to return completed ballots electronically, via email or fax.[1244]

Voting machine certification requirements: Fair

- Before being purchased and used for any election in the state, all voting machines must be EAC certified or undergo testing by a federally accredited laboratory.[1245]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[1246]

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[1247]
- Testing is open to the public.[1248]
- Testing begins at least seven days before an election.[1249]

Pennsylvania

Pennsylvania adheres to a number of minimum cybersecurity best practices related to voter registration systems, but the state allows voting using machines that do not provide a paper record. In addition to being vulnerable to hacking, this prevents the state from carrying out post-election audits that test the accuracy of election outcomes, which does not provide confirmation that ballots are cast as the voter intends and counted as cast. Even in places that do use paper ballots, the state's audit requirements lack important criteria. For example, audits may be conducted electronically through automated retabulation, which is vulnerable to hacking. Also, the number of ballots included in an audit is based on a fixed percentage, rather than one that is statistically significant and tied to the margin of victory in one or more ballot contests. Moreover, the audit law does not specify whether all categories of ballots—regular, absentee, provisional, and UOCAVA—are included in the audit, or if escalation occurs automatically if necessary. Pennsylvania's ballot accounting and reconciliation procedures also need improvement. The state did earn points for prohibiting voters stationed or living overseas from returning voted ballots electronically, a practice that election security experts say is notoriously insecure. In Pennsylvania, all voted ballots are returned by mail or delivered in person. The state exercises good practices by requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines before they are purchased or used in the state, and by requiring election officials to carry out pre-election logic and accuracy testing on all machines that will be used in an upcoming election.

The state's use of paperless DRE machines and insufficient post-election audits leave Pennsylvania open to undetected hacking and other Election Day problems. Pennsylvania should immediately switch to a statewide paper ballot voting system and require robust post-election audits that test the accuracy of election outcomes. Encouragingly, in December 2017, the General Assembly's Advisory Committee on Voting Technology recommended legislative funding to assist counties in obtaining voting machines that produce voter-verifiable paper records. And on February 9, Pennsylvania Gov. Wolf's administration ordered counties looking to replace voting systems to purchase machines with paper records, though counties already using paperless DRE voting systems would still be allowed to repurchase that equipment, at least until they are decertified. In updating its post-election audit requirements, state officials should look to risk-limiting audits like those in Colorado as a potential model.

To further improve its overall election security, Pennsylvania should require pre-election testing for electronic poll books in jurisdictions where they are used to ensure that they are in good working order before Election Day. Finally, Pennsylvania can strengthen its ballot accounting and reconciliation procedures by requiring counties to compare and reconcile precinct totals with composite results to confirm they add up to the correct number.

Minimum cybersecurity standards for voter registration system: Fair

- The state's voter registration system is estimated to be at least 10 years old.[1250]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[1251]
- The state's voter registration system has logging capabilities to track modifications to the database.[1252]
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[1253]
- The state performs regular vulnerability assessments on its voter registration system.[1254]
- The state has enlisted DHS to help assess and identify potential threats to its voter registration system.[1255]
- Commonwealth employees are required to participate in cybersecurity training.[1256]
- Electronic poll books are used by some, but not all, jurisdictions in the state.[1257] Paper voter registration lists are available at polling places that use electronic poll books on Election Day.[1258] Pre-election testing of electronic poll books is left up to the counties that use them.[1259]

Voter-verified paper audit trail: Unsatisfactory

- Depending on the jurisdiction, some voters in Pennsylvania cast paper ballots, while others vote using paperless DRE machines. On February 9, Pennsylvania Gov. Wolf's administration ordered counties looking to replace voting systems to purchase machines with paper backups, though counties already using paperless DRE voting systems would still be allowed to repurchase that equipment, at least until they are decertified.[1263]

Post-election audits: Unsatisfactory

- The state conducts mandatory post-election audits.[1265] However, Pennsylvania's use of paperless DRE machines prevents it from carrying out audits that can confirm the accuracy of election outcomes.
- The state's post-election audits may be conducted by manual hand count or electronically through automated retabulation.[1266] In any case, votes must be audited by a different method from how they were initially tabulated.[1267] For example, if an audited ballot was initially counted by an optical scan machine, in the audit

Pennsylvania conducts routine back-ups of the voter registration system and database.[1260]

While cybersecurity training is ultimately left up to the counties in Pennsylvania, state election officials—in partnership with the counties—are in the process of developing a statewide training program that could include information on how to better protect against cyberthreats, including avoiding and detecting spear-phishing attempts.[1261] The state hopes to have the training program in place and available to counties by the 2018 elections.[1262]

In a December 2017 report by the Advisory Committee on Voting Technology within the General Assembly recommended the Assembly provide funding to assist counties in obtaining voting equipment that produces a voter-verifiable paper record.[1264]

that ballot would have to be counted manually or by some other means.[1268]
- Audits are carried out on at least 2 percent of votes cast or 2,000 votes total, whichever is fewer.[1269]
- The ballots included in the audit are selected randomly.[1270]
- There is no statutory requirement on whether all categories of ballots—regular, absentee, provisional, and UOCAVA—are eligible for auditing.
- There is no statutory requirement on whether an audit escalates to include more ballots in the event that preliminary outcomes are found to be incorrect.
- Audits are open to public observance.[1271]
- Audits are carried out approximately 20 days before certification.[1272]
- We were told that although not explicitly required by law, counties are required during an audit to resolve any discrepancies identified. The resolution of the discrepancies could change election results.[1273]

Ballot accounting and reconciliation: Unsatisfactory

- All ballots are accounted for at the precinct level.[1274]
- Precincts are required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[1275]
- Counties are not explicitly required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[1276]
- There is no statutorily mandated review process to ensure that all voting machine memory cards have been properly loaded onto the tally server.[1277] While state law requires that election results be made public, it is unclear whether the same is true of information regarding ballot reconciliation processes and results.[1278]

Paper absentee ballots: Fair

- The state does not permit voters—including UOCAVA voters—to submit completed ballots electronically. All ballots must be returned by mail or delivered in person.[1279]

Voting machine certification requirements: Fair

- Before they may be purchased and used in the state, all voting machines must be certified by the Election Assistance Commission.[1280]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[1281]

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[1282]
- Testing is open to the public.[1283]
- Testing is carried out at least four days before an election.[1284]

Rhode Island

In many ways, Rhode Island is leading the states in election security, receiving "good" scores for the three most important categories due to its statewide use of paper ballots, its adherence to minimum cybersecurity best practices, and its new risk-limiting audit law. Still, the state's ballot accounting and reconciliation requirements need improvement, and Rhode Island's allowance of voted absentee ballots being returned electronically leaves its elections vulnerable. Although the state's new "risk-limiting" post-election audit law is "good," the fact that the state allows some electronic absentee voting undermines the overall effectiveness of these audits. Voted ballots that are submitted electronically via fax, for example, cannot be properly audited because there is a low degree of confidence in electronically submitted ballots, and they are vulnerable to manipulation. In addition to the top three categories, Rhode Island earned points for requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines before being purchased or used in the state and for requiring election officials to carry out pre-election logic and accuracy testing on all machines that will be used in an upcoming election.

To improve its overall election security, Rhode Island should strengthen its ballot accounting and reconciliation procedures by requiring poll workers to reconcile any discrepancies between the number of ballots cast and number of voters who signed in at the polling place and by requiring counties to compare and reconcile precinct totals with countywide composite results to ensure that they add up to the correct number. Finally, Rhode Island should prohibit voters stationed or living overseas from returning voted ballots electronically. Election security experts and federal entities have warned that submitting voted ballots in this way is insecure and vulnerable to manipulation. Going forward, all voted ballots should be returned by mail or delivered in person.

Minimum cybersecurity standards for voter registration system: Good

- The state's voter registration system is estimated to be at least 10 years old.[1285]
- The state's voter registration system provides access control to ensure that only authorized personnel can access the database.[1286]

- The state's voter registration system has logging capabilities to track modifications to the database.[1287]
- The state's voter registration database is protected by an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[1288]
- The state performs regular vulnerability assessments and penetration testing on its voter registration system.[1289]
- The state has enlisted either the National Guard or DHS to help assess and identify potential threats to its voter registration system.[1290]
- In 2017, Rhode Island Secretary of State Nellie Gorbea brought together state election officials—including more than 100 municipal election officials—for a cybersecurity training and information summit.[1291]
- In 2016, the state developed a new pilot program that allows polling places to make use of electronic poll books, a handful of which were used during the 2016 election.[1292] A total of 57 jurisdictions participate in the electronic poll book pilot program, with the state hoping to expand the program statewide in time for the 2018 elections.[1293] Paper voter registration lists are available at polling places that use electronic poll books on Election Day.[1294] The state conducts pre-election testing on electronic poll books prior to an election.[1295] Because Rhode Island's electronic poll books are still in the piloting phase, the state was not graded on e-pollbook best practices.

Rhode Island has increased its information technology staff by 40 percent in recent years.[1296]

Voter-verified paper audit trail: Good

- Elections are carried out using paper ballots and optical scan machines.[1297]

Post-election audits: Good

- The state does not currently require post-election audits. However, in 2017, the State of Rhode Island General Assembly passed legislation that would require risk-limiting post-election audits to be carried out after every election.[1298] Once enacted, risk-limiting audits will become optional for the 2018 elections and mandatory by 2020.[1299] The ballots included in the audit will be selected randomly through a "statistical method that ensures a large, predetermined chance of requiring a full manual tally" if preliminary vote totals are found incorrect. The audit will be conducted publicly within seven days after an election, and can replace preliminary outcomes if they are found to be incorrect.[1300]

**Although Rhode Island's new post-election audit requirements are good, the state's allowance of electronic absentee voting undermine the audits' overall effectiveness.*

Ballot accounting and reconciliation: Unsatisfactory

- All ballots are accounted for at the precinct level.[1301]
- While poll workers are required to record the number of ballots cast and the number of voters who signed in at the polling place, there is no requirement that these numbers be reconciled if discrepancies arise.[1302]
- Counties are not explicitly required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[1303]
- There is no statutorily mandated review process to ensure that all voting machine memory cards have been properly loaded onto the tally server to the extent that they are used.[1304]
- The state requires that vote tallies and ballot reconciliation information be made public.[1305]

Paper absentee ballots: Unsatisfactory

- The state allows UOCAVA voters to submit completed ballots electronically via fax, but only if the voter's absentee application was sent in the same manner.[1306]

Voting machine certification requirements: Fair

- Before being purchased and used for any election in the state, all voting machines must undergo testing by a federally accredited laboratory.[1307]
- The state replaced all of its voting machines in 2016.[1308]

Pre-election logic and accuracy testing: Fair

- Election officials conducts mandatory logic and accuracy testing on all voting machines prior to an election.[1309]
- Testing is open to the public.[1310]
- Testing occurs "as near to the time of the election as is feasible."[1311]

South Carolina

South Carolina adheres to recommended minimum cybersecurity best practices related to voter registration systems. But the state allows voting using machines that do not provide a paper record, which prevents it from carrying out post-election audits that test the accuracy of election results. South Carolina also allows voters stationed or living overseas to return voted ballots electronically, a practice that election security experts say is notoriously insecure. The state did earn points for its ballot accounting and reconciliation procedures and for requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines. Additionally, South Carolina requires election officials to carry out pre-election logic and accuracy testing on all machines that will be used in an upcoming election.

The state's use of machines that do not provide a paper record and its lack of robust post-election audits leaves South Carolina open to undetected hacking and other Election Day problems. To protect its elections from sophisticated nation-states, South Carolina should switch over to a paper ballot voting system and enact laws requiring robust post-election audits that test the accuracy of election outcomes. In doing so, the state should look to risk-limiting audits like those in Colorado as a potential model. South Carolina should also prohibit voters stationed or living overseas from returning voted ballots electronically. Given the threat posed by those seeking to interfere in U.S. elections, all voted ballots should be returned by mail or delivered in person to protect against manipulation and maintain voter privacy.

Minimum cybersecurity standards for voter registration system: Good

- The state's voter registration system was put into place in 2011.[1312]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[1313]
- The state's voter registration system has logging capabilities to track modifications to the database.[1314]
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[1315]

- The state performs regular vulnerability assessments and penetration testing on its voter registration system.[1316]
- The state has enlisted both the National Guard and DHS to help assess and identify potential threats to its voter registration system.[1317]
- The state provides cybersecurity training to election officials at the state and county level. County election directors attend a mandatory security meeting annually and receive routine security briefings on an ongoing basis.[1318]
- Electronic poll books are used by some, but not all, jurisdictions in the state.[1319] The state conducts pre-election testing on electronic poll books prior to an election.[1320] Paper voter registration lists are available at polling places that use electronic poll books on Election Day.[1321]

In addition to receiving help from the South Carolina National Guard's new Cyberprotection Battalion and DHS, South Carolina also enlists the help of the state's Division of Technology and Division of Information Security and a private cybersecurity vendor to help assess and identify potential threats to its voter registration system.[1322]

Voter-verified paper audit trail: Unsatisfactory

- Elections are carried out using paperless DRE machines.[1323]

Post-election audits: Unsatisfactory

- South Carolina's use of paperless DRE machines prevents it from carrying out audits that can confirm the accuracy of election outcomes. Instead, after an election, South Carolina conducts two separate tests at the county and state level prior to certification that check to ensure that all ballots have been counted as part of the tabulation process. According to the South Carolina's Election Commission website: "The audit process compares the tabulated results of the election with the raw data collected in the electronic audit files by each iVotronic voting machine on a flash card. The State Election Commission has developed a series of computer applications written in the public domain language … that compares the tabulated returns reports with the raw audit data. If the audit application detects an anomaly it lists it in one or more audit report." Provisional and vote by mail "paper ballots are tabulated using an optical scanner, and results are loaded into the results tabulation software using a memory stick or Zip drive."[1324]

"We're taking steps to enhance every aspect of the election infrastructure."—Marci Andino, director, South Carolina State Election Commission[1325]

Ballot accounting and reconciliation: Fair

- Ballots are fully accounted for at the precinct level.[1326]
- Precincts are required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[1327]
- Counties are required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[1328]
- Counties are required to review and ensure that all voting machine memory cards have been properly loaded onto the tally server.[1329]

- The state requires that all election results and ballot reconciliation information be made public.[1330]

Paper absentee ballots: Unsatisfactory

- The state permits UOCAVA voters to submit completed ballots electronically via fax or email.[1331]

Voting machine certification requirements: Fair

- Before being purchased and used for any election in the state, all voting machines must be tested to federal standards and undergo testing by a federally accredited laboratory.[1332]
- It has been reported that jurisdictions in South Carolina still use voting machines that were purchased more than a decade ago.[1333]

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[1334]
- Testing is open to the public.[1335]
- State law requires that testing be carried out at least three days prior to an election. In practice, testing is carried out approximately 60 days in advance.[1336]

South Dakota

South Dakota receives a C*

South Dakota conducts its elections with paper ballots, but its failure to require post-election audits that test the accuracy of election outcomes leaves the state open to undetected hacking and other Election Day problems. The state did earn points for its ballot accounting and reconciliation procedures and for prohibiting voters stationed or living overseas from returning voted ballots electronically, a practice that election security experts say is notoriously insecure. In South Dakota, all voted ballots are returned by mail or delivered in person. South Dakota also exercises good practices by requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines and by requiring election officials to carry out logic and accuracy testing on all machines that will be used in an upcoming election.

Despite numerous attempts to speak to someone in state government about the cybersecurity standards for the state's voter registration system, state officials told us they would not provide us with information or comment on our research, and we were unable to locate all of the information independently. Even if South Dakota is adhering to all of the minimum cybersecurity best practices for voter registration systems, its overall grade would not change, given the point distribution for the other categories.

To protect its elections from sophisticated nation-states seeking to disrupt U.S. elections, South Dakota should adopt robust post-election audits that test the accuracy of election outcomes. In doing so, state officials should look to risk-limiting audits like those in Colorado as a potential model. South Dakota should also require cybersecurity training for election officials and should partner with DHS in identifying and assessing potential threats to its voter registration system, if it's not already doing so. While recognizing the importance of state autonomy when it comes to elections, federal agencies with expertise in cybersecurity and access to classified information on contemporaneous cyberthreats have the personnel and resources necessary to thoroughly probe and analyze complex election databases, machines, and cyber vulnerabilities. By combining their expertise on cyberthreats and their insight into the unique qualities of localized election infrastructure, state and federal officials can better assess and deter attempts at electoral disruption.

Minimum cybersecurity standards for voter registration system: Incomplete

**State officials told us they would not participate in our research and therefore were unable to share information on cybersecurity requirements for the state's voter registration system. Information gathered for this section derives from independent research and correspondence with a county official.*

- The state's voter registration system was put into place in 2012.[1337]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[1338]
- The state's voter registration system has logging capabilities to track modifications to the database.[1339]
- State officials were unable to provide us with information on whether the state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[1340]
- State officials were unable to provide us with information on whether the state performs regular vulnerability assessments on its voter registration system.[1341]
- State officials were unable to provide us with information on whether the state has enlisted the National Guard or DHS to help assess and identify potential threats to its voter registration system.
- The state does not provide cybersecurity training to election officials.[1342] However, county officials do meet "regularly with Secretary of State on security matters."[1343]
- Electronic poll books are used by some, but not all, jurisdictions in the state.[1344] Unfortunately, state officials were unable to provide us with information on whether the state requires electronic poll books to receive pre-election logic and accuracy testing before an election or whether backup paper voter registration lists are required in jurisdictions that use them in case of emergency.

Voter-verified paper audit trail: Good

- Elections are carried out using paper ballots and optical scan machines.[1345]

Post-election audits: Unsatisfactory

- The state does not require post-election audits.[1346]

Ballot accounting and reconciliation: Fair

- All ballots are accounted for at the precinct level, including used, unused, and spoiled.[1347]
- Precincts compare and reconcile the number of ballots with the number of voters who signed into the polling place.[1348]
- Precinct totals are reconciled with countywide results at the state auditor's office on election night and again after the provisional ballots are investigated.[1349]

- There is no statutorily mandated review process to ensure that all voting machine memory cards have been properly loaded onto the tally server to the extent they are used.[1350]
- While state law requires that election results be made public, it is unclear whether the same is true of information regarding ballot reconciliation processes and results.[1351]

Paper absentee ballots: Fair

- The state does not permit voters—including UOCAVA voters—to submit completed ballots electronically. All ballots must be returned by mail or delivered in person.[1352]

Voting machine certification requirements: Fair

- Before they may be purchased and used in the state, all voting machines must be certified by the Election Assistance Commission.[1353]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[1354]

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[1355]
- Testing is open to the public.[1356]
- Testing occurs within 10 days before an election.[1357]

Tennessee

Tennessee uses voting using machines that do not provide a paper record and fails to mandate statewide post-election audits that test the accuracy of election outcomes, which does not provide confirmation that ballots are cast as the voter intends and counted as cast. Currently, only jurisdictions using paper ballots are required to audit their results. The number of ballots included in an audit is based on a fixed amount, rather than a statistically significant number tied to the margin of victory in one or more ballot contests. The initial audit is carried out electronically through automated retabulation and is only carried out manually upon escalation. Provisional ballots are excluded from the audit and it is unclear whether audit results have an impact on election outcomes if an error is found.

Furthermore, despite numerous attempts to speak to someone in state government about the cybersecurity standards for the state's voter registration system, state officials did not respond to our follow up requests for information and comment, and we were unable to locate all of the information independently. If Tennessee is adhering to all of the minimum cybersecurity best practices for voter registration systems, it would receive a "good" score—worth 3 points—for that category, bringing its grade up to a D. And while Tennessee requires pre-election testing be performed on all optical scan machines, testing is only required for a percentage of DRE machines in the state. Tennessee did earn points for prohibiting voters stationed or living overseas from returning voted ballots electronically. In Tennessee, all voted ballots are returned by mail or delivered in person.

Tennessee's use of paperless DRE machines and insufficient post-election audit procedures leave the state open to undetected hacking and other Election Day problems. Tennessee should immediately transition to a statewide paper ballot voting system and update its post-election audit requirements. In doing so, the state should look to risk-limiting audits like those in Colorado as a potential model. Tennessee should also strengthen its ballot accounting and reconciliation procedures by requiring that precincts fully account for all ballots—used, unused, and spoiled—at the end of Election Day, and reconcile any discrepancies

between the number of ballots and the number of voters who entered the polling place. Finally, pre-election logic and accuracy testing should be conducted on all machines that will be used in an upcoming election.

Minimum cybersecurity standards for voter registration system: Incomplete

**State officials did not respond to our follow up requests for information and comment and therefore were unable to share information on cybersecurity requirements for the state's voter registration system. Information gathered for this section derives from independent research. If Tennessee is carrying out the missing cybersecurity best practices, its grade would be raised from an F to a D.*

- The state's voter registration system is estimated to be at least 10 years old.[1358]
- State officials were unable to provide us with information on whether the state's voter registration system provides access control to ensure that only authorized personnel can access the database.
- State officials were unable to provide us with information on whether the state's voter registration system has logging capabilities to track modifications to the database.
- State officials were unable to provide us with information on whether the state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.
- State officials were unable to provide us with information on whether the state performs regular vulnerability assessments on its voter registration system.
- State officials were unable to provide us with information on whether the state has enlisted the National Guard or DHS to help assess and identify potential threats to its voter registration system.
- State officials were unable to provide us with information on whether the state provides cybersecurity training to election officials.
- The state permits the use of electronic poll books.[1359] Unfortunately, state officials were unable to provide us with information on whether the state requires electronic poll books to receive pre-election logic and accuracy testing before an election or whether backup paper voter registration lists are required in jurisdictions that use them in case of emergency.

Voter-verified paper audit trail: Unsatisfactory

- Depending on the jurisdiction, some voters in Tennessee cast paper ballots, while others vote using paperless DRE machines.[1360]

Post-election audits: Unsatisfactory

- Tennessee's use of paperless DRE machines prevents it from carrying out audits that can confirm the accuracy of election outcomes. And although Tennessee conducts post-election reviews, it only does so in jurisdictions that use paper ballots.[1361]
- The initial audit is conducted electronically through automated retabulation, though the ballots selected must be fed through a different optical scanner than was used as part of the original count.[1362] If the review escalates, the expanded audit may be carried out by manual hand count upon discretion.[1363]
- The county election commission is responsible for selecting at least one precinct-based optical scan machine that was used to count ballots cast during early voting.[1364] In addition, for counties with a population of fewer than 300,000, at least one voting precinct in the county must be selected for auditing.[1365] For counties with a population of 300,000 or more, at least five voting precincts are randomly selected for review.[1366] The post-election tests include a review of the top-of-the-ticket contest, either presidential or gubernatorial.[1367]
- The election units included in the audit are selected randomly.[1368]
- Provisional ballots are not included in the post-election review.[1369]
- The review escalates if a discrepancy of at least 1 percent arises.[1370] In that event, the county election commission must review at least 3 percent of voting precincts in the county.
- The post-election review process is open to the public and the results are made public.[1371]
- The reviews are carried out before certification.[1372]
- While it is unclear whether a post-election review can reverse the preliminary outcome of a tested contest if an error is detected, its results can be used as evidence in a legal dispute over election outcomes.[1373]

Ballot accounting and reconciliation: Unsatisfactory

- Ballots are not fully accounted for at the precinct level.[1374] For example, precincts are required to gather and return all materials, but there are no specific requirements for accounting for all ballots, used and unused.[1375]
- While poll workers are required to record the number of voters who entered the polling place, they are not required to reconcile these numbers with the number of ballots.[1376]
- Counties are required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[1377]
- There is no statutorily mandated review process to ensure that all voting machine memory cards have been properly loaded onto the tally server.[1378]

- One state election official indicated that all election results and information regarding ballot reconciliation processes and results are made publicly available, citing Tennessee Code § 2-8-104.[1379] However, it is not enough that "all candidates, their representatives, representatives of the political parties, and representatives of the press" be allowed to be present when the commission "compares the votes from the tally tapes of all appropriate sources to the tabulated election results." It is important that vote tallies and any reconciliation information be posted publicly so that members of the public can review how election outcomes were ultimately reached even if they are unable to attend in person.

Legislation introduced in 2017 would require the creation of uniform polling place procedures related specifically to the handling of ballots and emergency procedures.[1380]

Paper absentee ballots: Fair

- The state does not permit voters—including UOCAVA voters—to submit completed ballots electronically. All ballots must be returned by mail or delivered in person.[1381]

Voting machine certification requirements: Fair

- Before they may be purchased or used in the state, all voting machines must be certified by the Election Assistance Commission.[1382]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[1383]

Pre-election logic and accuracy testing: Unsatisfactory

- Election officials conduct mandatory logic and accuracy testing on all optical scan machines prior to an election.[1384] Jurisdictions using electronic voting machines—such as DREs—are required to "select a number of precincts equal to at least one percent of the number of precincts in the election and have all machines used in such precincts" tested.[1385]
- While state requirements are explicit in requiring that testing of optical scanners is open to the public,[1386] it is unclear whether the same is true of tests performed on DREs.[1387]
- Testing on optical scan machines is carried out at least two days before an election.[1388] The precise timing for testing DRE machines is unclear.[1389]

Texas

Texas allows voting using machines that do not provide a paper record and fails to mandate statewide post-election audits that test the accuracy of election outcomes, which does not provide confirmation that ballots are cast as the voter intends and counted as cast. Currently, state law only requires post-election audits for jurisdictions that use paper ballots. It is within the Texas secretary of state's discretion to audit "any portion of any number of ballots from any precinct in which the electronic voting system was used." In addition, the number of ballots included in an audit is based on a fixed amount, rather than a statistically significant number tied to the margin of victory in one or more ballot contests. Also troublesome is the fact that audits are not binding on election results and cannot reverse the preliminary outcome of an audited contest even if an error is detected. Additionally, Texas allows some voters stationed or living overseas to return voted ballots electronically, a practice that election security experts say is notoriously insecure. The state did earn points for its ballot accounting and reconciliation procedures and for requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines. Additionally, Texas requires election officials to carry out pre-election logic and accuracy testing on all machines that will be used in an upcoming election.

Texas's use of paperless DRE machines and its failure to conduct robust post-election audits that test the accuracy of election outcomes leaves Texas vulnerable to hacking and malfunction. Texas should immediately switch to a statewide paper ballot voting system and update its post-election audit procedures. In doing so, state officials should look to risk-limiting audits like those in Colorado as a potential model. Texas should also require pre-election testing for electronic poll books to ensure that they are in good working order before Election Day. In addition, Texas should prohibit all absentee voters from returning voted ballots electronically. Going forward, all voted ballots should be returned by mail or delivered in person. Although the state does not currently provide cybersecurity training to election officials, we were told that it is considering adding some cybersecurity training in the future. And while state officials did not specifically disclose whether the state has worked with DHS to identify and assess potential threats to its voter registration system, we were told that state officials maintain "a good relationship" with the federal agency.

Minimum cybersecurity standards for voter registration system: Mixed

- The state's voter registration system has been updated within the past 10 years.[1390]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[1391]
- The state's voter registration system has logging capabilities to track modifications to the database.[1392]
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[1393]
- The state performs regular vulnerability assessments on its voter registration system.[1394]
- The state has attended meetings and has "a good relationship" with DHS on election security matters, but it is unclear whether the state has accepted DHS's help in identifying or assessing vulnerabilities in its voter registration system.[1395] At least one county in the state has partnered with DHS to assess and identify potential vulnerabilities.[1396]
- While the state does not currently require its election officials to receive cybersecurity training prior to an election, it is considering adding some cybersecurity training in the future.[1397] At least one county has conducted outreach to educate election officials on phishing attempts and the importance of "clean computing."[1398]
- Electronic poll books are used by some, but not all, jurisdictions in the state.[1399] Pre-election testing of electronic poll books is left up to the counties that use them.[1400] While there is no requirement that jurisdictions using electronic poll books provide back-up paper voter registration lists in case problems arise, "[t]ypically, those counties using epollbooks will provide the epollbook and a backup copy of the list in either in hardcopy or in a different electronic format that can be accessed outside of the epollbook software with different equipment."[1401]

While Texas does not currently require its election officials to receive cybersecurity training prior to an election, it is considering adding some cybersecurity training in the future.[1402]

Voter-verified paper audit trail: Unsatisfactory

- Depending on the jurisdiction, some voters in Texas cast paper ballots, while others vote using paperless DRE machines.[1403]

Post-election audits: Unsatisfactory

- Texas's use of paperless DRE machines prevents it from carrying out audits that can confirm the accuracy of election outcomes. Moreover, state law only requires post-election audits for jurisdictions that use paper ballots.[1404] It is within the Texas secretary of state's discretion to audit "any portion of any number of ballots from any precinct in which the electronic voting system was used."[1405]
- The state's post-election audits are conducted through manual hand count.[1406]

- For counties using paper ballots, county officials are required to audit ballots in at least 1 percent of election precincts or 3 percent of machines, whichever is greater.[1407] In most cases, all ballot items are subject to auditing. However, for certain elections—general elections for state and county officers, primary elections, or any election with proposed state constitutional amendments or statewide ballot measures—an audit includes up to three contested races and three ballot propositions.[1408] Beyond this, the secretary of state may choose to audit additional ballots and precincts."[1409]
- The precincts included in the audit are selected randomly.[1410]
- All categories of ballots—regular, early voting, absentee, provisional, and UOCAVA—are eligible for auditing.[1411]
- An audit can escalate in the event that preliminary outcomes are found to be incorrect.[1412]
- Audits are not open to the public and the results are not made publicly available but written notice of an audit is posted and candidates and their representatives are entitled to be present.[1413] However, at least one county allows members of the public to be present for audits.[1414]
- A manual audit must be completed within 21 days after an election, before certification.[1415]
- An audit cannot reverse the preliminary outcome of an audited contest if an error is detected.[1416]

Ballot accounting and reconciliation: Fair

- In practice, all ballots are accounted for at the precinct level.[1417]
- Poll workers are required to compare and reconcile vote tallies and the number of voters who entered the polling place.[1418]
- Precinct totals are generated at the county level by central counting station personnel who generate precinct returns and develop the unofficial totals from those returns. The central counting station personnel compare the precinct returns to the corresponding tally list.[1419]
- There is no statutorily mandated review process to ensure that all voting machine memory cards have been properly loaded onto the tally server at the county level.[1420]
- The state requires that vote tallies and ballot reconciliation information be made public.[1421]

Paper absentee ballots: Unsatisfactory

- One Texas county has been approved by the Texas secretary of state to receive ballots via email from UOCAVA voters who are eligible for hostile fire or imminent danger pay or who are stationed in a designated combat zone.[1422]

Voting machine certification requirements: Fair

- Before they may be purchased and used in the state, all voting machines must be certified by the Election Assistance Commission.[1423]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[1424]

Pre-election logic and accuracy testing: Fair

- The entity conducting an election conducts logic and accuracy testing of the tabulation equipment for all vote-tabulating machines prior to an election. This includes precinct scanners, central scanners, central accumulator, and DRE machines.[1425]
- Testing is open to the public.[1426]
- Testing occurs at least 48 hours before the machines are to be used in an election.[1427]

Utah

Utah receives a **C**

Utah adheres to a number of minimum cybersecurity best practices related to voter registration systems and conducts its elections using paper ballots and voting machines that provide a paper record, but the state's post-election audits lack important criteria. For example, the number of ballots included in an audit is based on a fixed amount, rather than a statistically significant number tied to the margin of victory in one or more ballot contests. Adding to this is the fact that audits cannot escalate to include more ballots if necessary. If an error is discovered in preliminary outcomes, election officials are required to investigate to determine the cause of the problem and provide a written record. Moreover, Utah allows voters stationed or living overseas to return voted ballots electronically, a practice that election security experts say is notoriously insecure. The state's ballot accounting and reconciliation procedures also need improvement. Utah did earn points for requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines before being purchased or used in the state and for requiring election officials to carry out pre-election logic and accuracy testing on all machines that will be used in an upcoming election.

To improve its overall election security, Utah should adopt more comprehensive audits that test the accuracy of election outcomes. In doing so, the state should look to risk-limiting audits like those in Colorado as a potential model. Given the threat posed by sophisticated nation-states seeking to disrupt U.S. elections, it is imperative that post-election audits be comprehensive enough to test the accuracy of election outcomes with a high degree of confidence and detect any possible manipulation. Utah should also require jurisdictions using electronic poll books to have backup paper voter registration lists available in case of emergency. Moreover, the state can strengthen its ballot accounting and reconciliation procedures. All ballots—used, unused, and spoiled—must be fully accounted for at the precinct level, while counties should be required to compare and reconcile precinct totals with composite results to confirm they add up to the correct number. Finally, Utah should prohibit voters stationed or living overseas from returning voted ballots electronically. All voted ballots should be returned by mail or delivered in person to prevent manipulation and maintain voter privacy.

Minimum cybersecurity standards for voter registration system: Fair

- The state's voter registration system is estimated to be at least 10 years old.[1428]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[1429]
- The state's voter registration system has logging capabilities to track modifications to the database.[1430]
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[1431]
- The state performs regular vulnerability assessments on its voter registration system.[1432]
- The state has enlisted either the National Guard or DHS to help assess and identify potential threats to its voter registration system.[1433]
- The state requires that election officials at the state level receive cybersecurity security awareness training prior to an election.[1434]
- The state's statewide voter registration system functions as an electronic poll book and is used by jurisdictions throughout the state.[1435] The system undergoes testing before elections.[1436] It is up to the counties whether they want to provide backup paper copies of voter registration lists at polling places.[1437]

Currently, Utah's voter registration system tracks and logs all modifications to voter registration information.[1438] The state intends to strengthen the system's logging capabilities by including a tracking feature that logs and time-stamps who downloads voter registration reports.[1439]

Voter-verified paper audit trail: Fair

- Depending on the jurisdiction, some voters in Utah cast paper ballots, while others vote using DRE machines with VVPR.[1440]

Post-election audits: Fair

- The state conducts mandatory post-election audits.[1441]
- The state's post-election audits are conducted through manual hand count.[1442]
- Audits include at least 1 percent of voting machines used in the state.[1443] At least one voting machine from each county must be included in the audit.[1444]
- The voting machines included in the audit are selected randomly.[1445]
- All categories of ballots—regular, early voting, absentee, provisional, and UOCAVA—are eligible for auditing.[1446]
- If an error is discovered in preliminary outcomes, election officials are required to investigate to determine the cause of the problem and provide a written record.[1447] There is no statutory requirement on whether audits escalate.
- Audit results are publicly available.[1448]
- Audits must be conducted prior to certification of election results.[1449]
- An audit can reverse the preliminary outcome of an audited contest if an error is detected.[1450]

Ballot accounting and reconciliation: Unsatisfactory

- Ballots may not always be fully accounted for at the precinct level.[1451] For example, although ballot disposition forms—which ask about the number of used, unused, and spoiled ballots—are distributed, there is no legal requirement that these forms be filled out.[1452] One state official did mention that counties submit formal statements of votes cast to the state every regular election. Statements of votes cast typically only include the total number of votes cast for ballot contests in a given precinct.[1453] This best practice is concerned with whether election officials at individual polling places account for every ballot—including unused and spoiled ballots—not just the number of voted ballots. We are told that several counties reconcile the number of ballots remaining at the end of Election Day with the number of ballots delivered to the polling place.[1454]
- Precincts are required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[1455]
- Counties are not explicitly required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[1456]
- There is no statutorily mandated review process to ensure that all voting machine memory cards have been properly loaded onto the tally server at the county level.[1457]
- While state law requires that election results be made public, it is unclear whether the same is true of information regarding ballot reconciliation processes and results.[1458] In answering this question, one state official pointed us to Utah Code § 20A-4-105, which requires election results to be posted publicly along with the total number of votes cast in the board's jurisdiction, the number of votes for each candidate, the number of votes for and against each ballot proposition, the total number of votes given in the board's jurisdiction to each candidate and for and against each ballot proposition, and the number of ballots that were rejected.[1459] However, nowhere does the law explicitly require that information related to how ballots are reconciled be posted publicly.

Paper absentee ballots: Unsatisfactory

- The state permits UOCAVA voters and voters with disabilities to submit completed ballots electronically, via email or fax.[1460]

Voting machine certification requirements: Fair

- Before being purchased and used for any election in the state, all voting machines must either undergo testing by a federally accredited laboratory or be certified by the Election Assistance Commission.[1461]

Utah is in the process of seeking bids to replace its voting machines.[1463]

- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[1462]

Pre-election logic and accuracy testing: Fair

- **Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.**[1464]
- Testing is open to the public.[1465]
- The law does not specify precisely when testing must be carried out.

Vermont

Vermont adheres to a number of minimum cybersecurity best practices related to voter registration systems and conducts its elections with paper ballots, but its post-election audits are lacking important criteria. For example, audits may be carried out after certification and their results are not binding on election outcomes even if an error is discovered. Moreover, the audit law lacks specifics on the number of ballots that must be included and allows audits to be carried out electronically through automated retabulation, depending on the jurisdiction. State law does not explicitly require voting machines to be tested to EAC Voluntary Voting System Guidelines before being purchased or used in the state. Vermont did earn points for its ballot accounting and reconciliation procedures and for prohibiting voters stationed or living overseas from returning voted ballots electronically. In Vermont, all voted ballots must be returned by mail or delivered in person. The state also exercises good practices by requiring that election officials carry out pre-election logic and accuracy testing on all machines that will be used in an upcoming election. Encouragingly, although Vermont does not currently provide cybersecurity training for election officials, there is some discussion of including cybersecurity training for future elections.

To protect its elections from sophisticated nation-states seeking to interfere in U.S. elections, Vermont should update its post-election audit procedures with requirements that can confirm the accuracy of election outcomes with a high degree of confidence. In doing so, the state should look to risk-limiting audits like those in Colorado as a potential model. Vermont should also explicitly require by law that all voting machines be tested to EAC Voluntary Voting System Guidelines to ensure that voting machines meet baseline requirements for functionality, security, and accessibility.

Minimum cybersecurity standards for voter registration system: Fair

- The state's voter registration system has been updated within the past 10 years.[1466]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[1467]

- The state's voter registration system has logging capabilities to track modifications to the database.[1468]
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[1469]
- The state performs vulnerability assessments on its voter registration system.[1470]
- The state has enlisted the help of either the National Guard or DHS to assess and identify potential threats to its voter registration system and election infrastructure.[1471]
- Although Vermont does not currently provide cybersecurity training for election officials, there is some discussion of including cybersecurity training for future elections.[1472]
- The state does not use electronic poll books, and therefore was not graded on e-pollbook best practices.[1473]

Vermont has received or is expected to receive additional funding for cybersecurity at their election agencies.[1474]

Voter-verified paper audit trail: Good

- Elections are carried out using paper ballots and optical scan machines.[1475]

Post-election audits: Unsatisfactory

- The state conducts mandatory post-election audits.[1476]
- The method by which audits are conducted depends on the polling place. For example, polling places that tabulate ballots by means of an optical scan machine are audited electronically through automated retabulation.[1477] Polling places that hand count ballots are audited through manual hand count.[1478]
- State law requires that the secretary of state "shall conduct a random post-election audit of any polling place election results for a general election."[1479]
- All categories of ballots—regular, early voting, absentee, provisional, and UOCAVA—are eligible for auditing.[1480]
- If preliminary outcomes are found to be incorrect and cannot be resolved, the state will likely seek a court order requiring a do-over of the election.[1481]
- Audits are public and the results are announced publicly as an audit is being conducted.[1482]
- Audits must be carried out within 30 days of an election, which means that they could be conducted after certification of official election results, which in 2016 fell on November 15.[1483]
- Audit results cannot reverse the preliminary outcome of an audited contest if an error is detected, but they can form the basis of a case for fraud.[1484]

Ballot accounting and reconciliation: Fair

- All ballots are accounted for at the precinct level.[1485]
- Precincts are required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[1486]
- Counties are required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[1487]
- The state does not use a tally server. As such, a memory card review process is unnecessary.[1488]
- The state requires that all election results and reconciliation procedures be made public.[1489]

Paper absentee ballots: Fair

- The state does not permit voters—including UOCAVA voters—to submit completed ballots electronically. All ballots must be returned by mail or delivered in person.[1490]

Voting machine certification requirements: Unsatisfactory

- The state does not require voting machines to meet federal requirements before they are purchased and used in elections in the state.[1491] Instead, Vermont's secretary of state is responsible for certifying all election machines. The state is developing standards for state certification.[1492]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[1493]

While Vermont is not currently seeking bids to purchase new optical scan machines, it is replacing its ballot-marking devices, which are used by eligible voters with disabilities.[1494]

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[1495]
- Testing is open to the public.[1496]
- Testing is carried out at least 10 days before an election.[1497]

Virginia

Virginia should be applauded for its decision to switch to a statewide paper ballot voting system before the 2017 gubernatorial election. Noting the risks posed by paperless DRE machines, election officials took swift action in replacing these insecure machines with paper ballots in time for Election Day to help ensure that votes were protected. However, even though Virginia conducts its elections with paper ballots and adheres to a number of minimum cybersecurity best practices related to voter registration systems, its failure to carry out post-election audits that test the accuracy of election outcomes leaves the state open to undetected hacking and other Election Day problems. Although the state will begin conducting what the law calls "risk-limiting" audits in 2018, they are not risk-limiting audits in the true sense because they lack important criteria. For one thing, the audits are designed only to test the accuracy of ballot scanner machines, not the accuracy of election results. In addition, the audits will be conducted after certification and will have no effect on election outcomes. Put another way, the audit will not be able to reverse preliminary outcomes even if an error is found to have occurred. The state's ballot accounting and reconciliation procedures can also use improvement, and its failure to require pre-election logic and accuracy testing for all machines that will be used in an upcoming election leave polling places vulnerable to machine malfunction. Virginia did earn points for prohibiting voters stationed or living overseas from returning voted ballots electronically, a practice that election security experts say is notoriously insecure. In Virginia, all voted ballots are returned by mail or delivered in person. The state also exercises good practices by requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines before being purchased or used in the state.

By switching to a paper ballot voting system, Virginia has made huge strides in improving the security of its elections. These paper ballots, however, must be accompanied by robust post-election audits that test the accuracy of election outcomes. The state's current statute should be updated to ensure that it conforms to the criteria required for true risk-limiting audits like those in Colorado. Virginia should also do away with the practice of discarding random excess ballots if

discrepancies arise between the number of ballots and the number of voters who signed into a polling place and counties should be required to compare and reconcile precinct totals with composite results to confirm they add up to the correct amount. Regarding pre-election logic and accuracy testing, Virginia should make testing mandatory for all machines that will be used in an upcoming election, rather than leaving testing within the discretion of local election officials.

Minimum cybersecurity standards for voter registration system: Fair

- The state's voter registration system is newer than 10 years old.[1498]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[1499]
- The state's voter registration system has logging capabilities to track modifications to the database.[1500]
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[1501]
- The state performs vulnerability assessments on its voter registration system.[1502]
- The state has enlisted the state National Guard to help review and provide training exercises related to election security with respect to the state's election systems.[1503]
- The state requires that local election officials receive annual cybersecurity awareness training, which includes online and in-person courses.[1504]
- Electronic poll books are used by some, but not all, jurisdictions in the state.[1505] Pre-election testing of electronic poll books is left up to the counties that use them.[1506] Paper voter registration lists are available at polling places that use electronic poll books on Election Day.[1507]

Voter-verified paper audit trail: Good

- Elections are carried out using paper ballots and optical scanning machines.[1512]

Post-election audits: Unsatisfactory

- The state does not currently require post-election audits; rather, it is within the discretion of the Virginia State Board of Elections whether to carry them out.[1514] However, beginning this year the state will begin conducting mandatory post-election audits after every election.[1515] Although the law refers to these audits as "risk-limiting," they are not risk-limiting audits in the true sense.[1516] For example, the new audits will be meant only to test the accuracy of ballot scanner machines, not the accuracy of election results.[1517] And even though the new audits will consist of a manual hand count, they will not be able to reverse election outcomes, even if an error is detected.[1518]

Former Virginia Gov. Terry McAuliffe (D) led the charge on cybersecurity in the states, making cybersecurity a priority for his administration.[1508] As chair of the National Governors Association, former Gov. McAuliffe spearheaded the "Meet the Threat" initiative, which encouraged governors to institute cybersecurity governing bodies and standards for their respective states.[1509]

Virginia's Department of Elections has created a new digital security position.[1510]

Virginia has received or is expected to receive additional funding for cybersecurity at their election agencies.[1511]

Virginia decided to scrap its electronic touch-screen voting machines reportedly in response to reports coming out of the 2017 DEF CON, an annual hacker convention, that hackers succeeded in hacking and infiltrating some voting machines in fewer than 90 minutes.[1513]

Ballot accounting and reconciliation: Unsatisfactory

- All ballots are accounted for at the precinct level.[1519]
- Precincts are required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[1520] However, part of the reconciliation process may involve the random removal of excess ballots.[1521]
- Counties are not explicitly required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[1522]
- There is no statutorily mandated review process to ensure that all voting machine memory cards have been properly loaded onto the tally server at the county level.[1523]
- The state requires that election results and ballot reconciliation information be made public.[1524]

Paper absentee ballots: Fair

- The state does not permit voters—including UOCAVA voters—to submit completed ballots electronically. All ballots must be returned by mail or delivered in person.[1525]

Voting machine certification requirements: Fair

- Before being purchased and used for any election in the state, all voting machines must undergo testing by a federally accredited laboratory.[1526]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[1527]

Pre-election logic and accuracy testing: Unsatisfactory

- Pre-election logic and accuracy testing is left within the discretion of the counties, although the state recommends that all voting machines be tested prior to an election.[1528]
- There are no requirements that testing be open to the public.[1529]
- When pre-election testing is conducted, it is typically carried out on absentee ballot-reading machines in August or September during election years, while all other machines are usually tested closer to an election.[1530]

Washington

Washington adheres to recommended minimum cybersecurity best practices related to voter registration systems and conducts its elections with paper ballots, but its failure to require post-election audits on paper ballots leaves the state open to undetected hacking and other Election Day problems. Currently, state law requires post-election audits only for electronic voting machines that produce a paper record—DRE machines with VVPR. Audits on paper ballots are completely voluntary. This is deeply problematic for a vote-by-mail state like Washington, with a particular emphasis on voting by way of paper ballot. The state's ballot accounting and reconciliation procedures also need improvement. And while Washington state requires regular absentee voters who return voted ballots electronically to also submit a paper ballot copy of the voter's ballot, the same is not true of UOCAVA voters. The state did earn points for requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines before being purchased or used in the state, and for requiring election officials to carry out pre-election logic and accuracy testing on all voting machines prior to an election.

To protect its elections against threats, Washington must adopt mandatory statewide post-election audits on all auditable ballots and records. Audits must be comprehensive and must test the accuracy of election outcomes. In updating its audit requirements, the state should look to risk-limiting audits like those in Colorado as a potential model. Given the threat posed by sophisticated nation-states seeking to disrupt U.S. elections, it is imperative that post-election audits be comprehensive enough to test the accuracy of election outcomes with a high degree of confidence and detect any possible manipulation. Washington should also strengthen its ballot accounting and reconciliation procedures by requiring counties to compare and reconcile precinct totals with composite results to confirm they add up to the correct amount and should prohibit UOCAVA voters from returning voted ballots electronically or should require voters to supply paper copies of voted ballots alongside electronic submissions.

Minimum cybersecurity standards for voter registration system: Good

- The state's voter registration system is estimated to be at least 10 years old.[1531]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[1532]
- The state's voter registration system has logging capabilities to track modifications to the database.[1533]
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[1534]
- The state performs vulnerability assessments on its voter registration system.[1535]
- The state has enlisted DHS to help assess and identify potential vulnerabilities, conducting vulnerability assessments and penetration testing on its voter registration system and election infrastructure.[1536]
- Election officials at both the state and county level receive cybersecurity training prior to an election.[1537]
- The state does not use electronic poll books, and therefore was not graded on e-pollbook best practices.[1538]

Voter-verified paper audit trail: Good

- The state is a vote-by-mail state, meaning that most votes are cast using paper ballots,[1540] though several counties have DRE machines with VVPR, which voters are permitted to use if they prefer.[1541]

Washington has received or is expected to receive additional funding for cybersecurity at their election agencies.[1539]

Post-election audits: Unsatisfactory

- State law prescribes a voluntary audit for paper ballots and a mandatory audit for DRE machines with VVPR.
- For mandatory audits conducted on DRE machines with VVPRs, the auditing method is split between manual and electronic retabulation.[1542] Counties that use DRE machines with VVPR are required to audit up to 4 percent of all such machines used or one such machine—whichever is greater—prior to certification.[1543] If testing more than one machine, the results from one-fourth of the machines must be hand counted, while up to three-quarters can be optionally retabulated using an automated tabulation machine.[1544] Three races or ballot issues are randomly selected for the audit.[1545] If preliminary outcomes are found to be incorrect, the canvassing board must "take necessary actions to investigate and resolve the discrepancy."[1546] Audits are open to the public and the results are binding on official election outcomes.[1547]

- The voluntary audit on paper ballots is conducted manually.[1548] These audits are conducted only upon mutual agreement of the political party observers or at the discretion of the county auditor.[1549] These audits include a manual count of up to either three precincts or six batches of ballots, depending on the ballot-counting procedures in place in the county.[1550] Only one race or ballot issue is considered for the audit.[1551] The selection of precincts or ballots is done randomly by the county, as is the selection of race or ballot issue.[1552] All categories of ballots—regular, provisional, absentee, and UOCAVA—are eligible for auditing.[1553] Audits must be completed within 48 hours after an election, before certification.[1554]

Legislation introduced in 2018 would allow jurisdictions to carry out risk-limiting post-election audits.[1555]

Ballot accounting and reconciliation: Unsatisfactory

- Because the state is a vote-by-mail state, it is not necessary that all ballots be accounted for at the precinct level, specifically.[1558] Election officials are required to account for all ballots when the election results are certified.[1559]
- Because the state is a vote-by-mail state, it is not necessary that the number of ballots be compared to the number of voters who signed in at the polling place at the precinct level specifically.[1560] Election officials are required to compare and reconcile the number of ballots cast with the number of voters on the poll roster.[1561]
- Counties are not explicitly required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[1562] However, they are required to examine precinct results for anomalies that may indicate a problem with the tabulation software.[1563]
- There is no statutorily mandated review process to ensure that all voting machine memory cards have been properly loaded onto the tally server at the county level, to the extent they are used.[1564]
- The state requires that vote tallies and ballot reconciliation information be made public.[1565]

Washington state law requires that any discrepancies found between the DRE machine VVPRs and initial vote totals be reported to the voting system vendor.[1556] After being notified of the discrepancy, the vendor must provide a satisfactory explanation for the problem within 30 days.[1557]

Paper absentee ballots: Unsatisfactory

- The state permits absentee voters—including UOCAVA voters—to submit completed ballots electronically, via email or fax.[1566] Regular absentee voters who choose to return voted ballots electronically must also return a hard copy of their voted ballot no later than the day before election results are certified.[1567] The same is not required of UOCAVA voters.

Voting machine certification requirements: Fair

- Before being purchased and used for any election in the state, all voting machines must undergo testing by a federally accredited laboratory.[1568]

- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago, although several counties are currently seeking bids to replace tabulation equipment by 2018 or 2020.[1569] The state is seeking bids for modernizing, by 2019, the election management and voter registration system currently used by all counties and the secretary of state's office.[1570]

Washington is seeking bids for modernizing the election management and voter registration system currently used by all counties and the secretary of state's office by 2019.[1571]

Pre-election logic and accuracy testing: Fair

- **Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.**[1573]
- Testing is open to the public.[1574]
- Although state law requires testing on ballot-tabulating machines to take place at least three days before an election, the law is vague on testing for vote center DRE machines, specifying only that it must take place before an election.[1575]

Legislation introduced in 2018 would require manufacturers of voting system equipment to report certain security breaches on any of their equipment to the secretary of state and attorney general. Specifically, manufacturers would be required to disclose breaches that "compromised the security, confidentiality, or integrity of an election in any state" or if "Personal information of residents in any state was, or is reasonably believed to have been, acquired by an unauthorized person as a result of the breach and the personal information was not secured."[1572]

West Virginia

West Virginia adheres to minimum cybersecurity best practices related to voter registration systems and conducts its elections using paper ballots and voting machines that provide a paper record, but the state's post-election audits lack important criteria. Currently, the number of ballots included in an audit is based on a fixed amount rather than a statistically significant number tied to the margin of victory in one or more ballot contests. Adding to this is the fact that West Virginia allows voters stationed or living overseas to return voted ballots electronically, a practice that election security experts say is notoriously insecure. The state's ballot accounting and reconciliation procedures also need improvement. West Virginia did earn points for requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines before being purchased or used in the state and for requiring election officials to carry out pre-election logic and accuracy testing on all voting machines that will be used in an upcoming election.

To improve its overall election security, West Virginia should update its post-election audit procedures by basing the scope of the audit on a statistically significant number tied to the margin of victory in one or more ballot contests, looking to risk-limiting audits like those in Colorado as a potential model. Given the threat posed by sophisticated nation-states seeking to disrupt U.S. elections, it is imperative that post-election audits be comprehensive enough to test the accuracy of election outcomes with a high degree of confidence and detect any possible manipulation. West Virginia should also strengthen its ballot accounting and reconciliation procedures by requiring precincts to compare and reconcile the number of ballots with the number of voters who signed in at the polling place and by requiring counties to compare and reconcile precinct totals with composite results to confirm they add up to the correct number. Finally, it is also important that West Virginia prohibit voters stationed or living overseas from returning voted ballots electronically. Going forward, all voted ballots should be returned by mail or delivered in person.

Minimum cybersecurity standards for voter registration system: Good

- The state's voter registration system is estimated to be at least 10 years old.[1576]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[1577]
- The state's voter registration system has logging capabilities to track modifications to the database.[1578]
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[1579]
- The state has enlisted the West Virginia Air National Guard to assist with vulnerability probes and assessments of state election systems and databases.[1580]
- County election administrators receive cybersecurity training once every two years, prior to elections.[1581]
- Electronic poll books are used by some, but not all, jurisdictions in the state.[1582] Paper voter registration lists are available at polling places that use electronic poll books on Election Day.[1583] The state conducts pre-election testing on electronic poll books prior to an election.[1584]

The Secretary of State's IT department employs a member of the West Virginia Air National Guard tasked with protecting the state's election system against cyberthreats and attacks.[1585]

Voter-verified paper audit trail: Fair

- Depending on the jurisdiction, some voters in West Virginia cast paper ballots, while others vote using DRE machines with VVPR.[1586]

Post-election audits: Fair

- The state conducts mandatory post-election audits.
- The state's post-election audits are conducted through manual hand count.[1587]
- Post-election audits are conducted on at least 3 percent of precincts in a county.[1588]
- The precincts included in the audit are selected randomly.[1589]
- All categories of ballots—regular, early voting, absentee, provisional, and UOCAVA—are eligible for auditing.[1590]
- If a discrepancy of more than 1 percent arises or if the audit results project a different winner or outcome in a given ballot contest, all ballots must be recounted by hand.[1591]
- Audits are open to the public and the results are made publicly available.[1592]
- Audits are conducted as part of the canvassing process, prior to certification of official election results.[1593]
- An audit can reverse the preliminary outcome of an audited contest if an error is detected.[1594]

Ballot accounting and reconciliation: Unsatisfactory

- All ballots are accounted for at the precinct level.[1595]
- It is unclear whether all precincts compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[1596] Rather, some of that process appears to take place at the county level.[1597]
- There does not appear to be any explicit requirement for comparing and reconciling precinct totals with countywide results to ensure that they add up to the correct amount.[1598]
- There does not appear to be any statutorily mandated review process to ensure that all voting machine memory cards have been properly loaded onto the tally server at the county level.[1599]
- While state law requires that election results be made public, it is unclear whether the same is true of information regarding ballot reconciliation processes and results.[1600]

Paper absentee ballots: Unsatisfactory

- West Virginia permits UOCAVA voters to submit completed ballots electronically, via email or fax.[1601]

Voting machine certification requirements: Fair

- Before they may be purchased and used in the state, all voting machines must be certified by the Election Assistance Commission.[1602]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[1603]

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[1605]
- Testing is open to the public.[1606]
- Testing of automatic tabulating equipment takes place one week before an election, whereas the inspection of vote-recording devices is carried out at least five days before an election.[1607]

One way that voting machine vendors can help improve election security is by alerting any jurisdiction using one of their machines of breaches or widespread malfunctions on similar models that occur anywhere in the country. By doing so, election officials can be on alert for possible Election Day disruptions. In West Virginia, voting system vendors whose machines are used in the state are required by law to submit a biennial report to the West Virginia State Election Commission "that outlines any problem that has been experienced with the equipment by any jurisdiction in the state or in any jurisdiction outside the state that uses the same or a similar version of the equipment that has been certified for use in this state."[1604]

Wisconsin

Wisconsin adheres to minimum cybersecurity best practices related to voter registration systems and conducts its elections using paper ballots and voting machines that provide a paper record. But the state's failure to carry out post-election audits that test the accuracy of election outcomes leaves the state open to undetected hacking and other Election Day problems. Wisconsin's post-election audits are not designed to confirm the accuracy of election outcomes but rather to test the proper functioning of voting machines and other election processes. Audits often occur after certification of official election results, and the results have no bearing on election outcomes even if an error is found to have occurred. Some counties have asked the Wisconsin Elections Commission to allow them to carry out audits prior to certification. While the commission has granted permission, conducting audits prior to certification is still not required. The state's ballot accounting and reconciliation procedures also need improvement. Wisconsin did earn points for prohibiting voters stationed or living overseas from returning voted ballots electronically, a practice that election security experts say is notoriously insecure. In Wisconsin, all voted ballots are returned by mail or delivered in person. The state also exercises good practices by requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines before being purchased or used in the state, and by requiring election officials to carry out pre-election logic and accuracy testing on all voting machines that will be used in an upcoming election.

To protect its elections against potential attack by sophisticated nation-states seeking to interfere in U.S. elections, Wisconsin should adopt robust post-election audits that have binding effect on election results. Audits must be comprehensive enough to confirm—with a high degree of confidence—the accuracy of election outcomes. In making these changes, Wisconsin should look to risk-limiting audits like those in Colorado as a potential model. Wisconsin should also strengthen its ballot accounting and reconciliation procedures by disallowing the practice of discarding randomly selected excess ballots when discrepancies arise.

Minimum cybersecurity standards for voter registration system: Good

- The state's voter registration system was completely revamped and upgraded in 2016.[1608]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[1609]
- The state's voter registration system has logging capabilities to track modifications to the database.[1610]
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[1611]
- The state performs regular vulnerability assessments and penetration testing on its voter registration system.[1612]
- The state has enlisted either the National Guard or DHS to help assess and identify potential threats to its voter registration system.[1613]
- State election officials are required to complete cybersecurity training and are kept informed of any election-specific cybersecurity issues or developments as they arise.[1614] The state will expand cybersecurity training to local election officials as part of the comprehensive election security plan that the state is currently developing for the 2018 elections.[1615]
- Wisconsin permits but does not currently use electronic poll books.[1616] The state is in the process of developing electronic poll book software that will be make them available as an option for municipalities to use prior to the 2018 fall elections.[1617] In the future, when electronic poll books are used, the state plans to make paper copies of voter registration lists available at polling places as a backup in case of system failure or hacking. Because Wisconsin does not yet use electronic poll books, the state was not graded on e-pollbook best practices.[1618]

Wisconsin updated its state voter registration system in January 2016 onto a platform that incorporates additional security features. The state is considering requiring new hardware components for local election officials who operate within the voter registration system. The system is protected, in part, by state agencies that host the system platform and whose staff provides cybersecurity expertise and defenses.[1619]

Voter-verified paper audit trail: Fair

- Depending on the jurisdiction, some voters in Wisconsin cast paper ballots, while others vote using DRE machines with VVPR.[1620]

Post-election audits: Unsatisfactory

- The state conducts mandatory post-election audits, but only for general elections.[1621] The purpose of these audits is to determine whether voting machines functioned properly during voting periods, not to verify the accuracy of election outcomes.[1622]
- The state's post-election audits are conducted through manual hand count.[1623]
- Audits are conducted on a minimum of 100 voting machines across the state. An audit must include at least five machines for each voting system model used in the state. Four ballot contests are audited, including the top-of-the-ticket race, either presidential or gubernatorial. The three other audited races are selected at random after the election.[1624]

- The voting machines included in the audit are selected randomly.[1625]
- All categories of ballots—regular, early voting, absentee, provisional, and UOCAVA ballots—are eligible for auditing.[1626]
- Any discrepancy is resolved by the municipal clerks.[1627] The law is silent on whether an audit escalates in the event that preliminary outcomes are found to be incorrect.
- Audits are open to the public.[1628]
- The state's auditing process has traditionally taken place within two weeks after certification, which typically lands around December 15 in election years.[1629] However, in response to requests by municipal officials, the State Elections Commission has said that it will permit municipalities to begin conducting post-election audits prior to certification.[1630] An estimated 10 percent to 15 percent of all post-election audits in Wisconsin were carried out prior to the state certification deadline after the 2016 election.[1631]
- An audit cannot reverse the preliminary outcome of an audited contest if an error is detected.[1632]

During the 2016 election, approximately 10 percent to 15 percent of all post-election audits in Wisconsin were carried out prior to certification of the official election results.[1633]

Ballot accounting and reconciliation: Unsatisfactory

- All ballots are accounted for at the precinct level.[1634]
- Municipalities are required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[1635] However, part of the reconciliation process may involve randomly removing excess ballots.[1636]
- Counties are required to compare and reconcile municipal totals with county-wide results to ensure that they add up to the correct amount.[1637]
- There is no statutorily mandated review process to ensure that all voting machine memory cards have been properly loaded onto the tally server at the county level.[1638] However, the state's electronic Canvass Reporting System will alert election officials if zero votes appear for any candidates or ballot measures.[1639]
- While state law requires that election results be made public, it is unclear whether the same is true of information regarding ballot reconciliation processes and results.[1640] Reconciliation procedures are outlined in the state published guidance for poll workers, as well as on its website. However, they are not required to be posted publicly.[1641] That said, canvass boards are required to keep minutes, which are public records and are available after the fact to document what specific reconciliation procedures were used and how any discrepancies were resolved.[1642]

Paper absentee ballots: Fair

- The state does not permit voters—including UOCAVA voters—to submit completed ballots electronically. All ballots must be returned by mail or delivered in person.[1643]

Voting machine certification requirements: Fair

- The state removed the statutory requirement that all voting machines must be EAC-certified prior to purchase or use.[1644] In practice, however, all voting machines currently in use are EAC-certified.[1645]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[1646]

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[1647]
- Testing is open to the public.[1648]
- Testing occurs within 10 days before the election.[1649]

Wyoming

Wyoming receives a **C**

Wyoming uses paper ballots and voting machines that provide a paper record, but its failure to carry out post-election audits that test the accuracy of election outcomes leaves the state open to undetected hacking and other Election Day problems. Within 30 days after an election, Wyoming tests 5 percent of automated tabulating equipment to determine whether the machines are in good working order and are likely to have functioned properly during the election. The test involves feeding a random sample of test ballots into an automated ballot tabulator to determine the machine's accuracy. Adding to this is the state's failure to adhere to some important cybersecurity best practices and the fact that its ballot accounting and reconciliation procedures need improvement. Wyoming did earn points for prohibiting voters stationed or living overseas from returning voted ballots electronically, a practice that election security experts say is notoriously insecure. In Wyoming, all voted ballots are returned by mail or delivered in person. The state also exercises good practices by requiring that all voting machines be tested to EAC Voluntary Voting System Guidelines before being purchased and used in the state and by requiring election officials to carry out pre-election logic and accuracy testing on all machines that will be used in an upcoming election.

Given the threat posed by sophisticated nation-states seeking to disrupt U.S. elections, it is imperative that post-election audits be comprehensive enough to test the accuracy of election outcomes with a high degree of confidence and detect any possible manipulation. In updating its post-election audit requirements, state officials should look to risk-limiting audits like those in Colorado as a potential model. Wyoming should also require cybersecurity training for election officials, while pre-election testing should be required for electronic poll books in jurisdictions where they are used to ensure that they are in good working order before Election Day. Backup paper voter registration lists should be available at all polling places that use electronic poll books in case of emergency. In addition to making changes in these areas, Wyoming can strengthen its ballot accounting and reconciliation procedures by requiring counties to compare and reconcile precinct totals with countywide composite results to ensure that they add up to the correct amount.

Minimum cybersecurity standards for voter registration system: Fair

- The state's voter registration system has been updated within the past 10 years.[1650]
- The state's voter registration system provides access control to ensure that only authorized personnel have access to the database.[1651]
- The state's voter registration system has logging capabilities to track modifications to the database.[1652]
- The state's voter registration system includes an intrusion detection system that monitors incoming and outgoing traffic for irregularities.[1653]
- The state performs regular vulnerability assessments on its voter registration system.[1654]
- The Wyoming secretary of state's office has entered into an agreement with DHS to help assess and identify potential threats to the state's statewide voter registration system.[1655]
- The state does not provide cybersecurity training to election officials.[1656]
- Electronic poll books are used by some, but not all, jurisdictions in the state.[1657] Pre-election testing of electronic poll books is left up to the counties that use them.[1658] Paper voter registration lists are available at polling places that use electronic poll books.[1659]

Beginning in 2018, a state certification process will be required of all electronic poll book vendors prior to selling in Wyoming.[1660]

Wyoming counties may only access the statewide voter registration system from approved locations. State regulations warn that "any connection from a source that is not approved is a violation of the user access documents signed by all users of the system and could jeopardize the security of the [Help America Vote Act]-compliant statewide voter registration system." Approved locations are typically limited to county clerks' offices. In some instances, the system may be accessed by remote location, but only if the connection between the remote site and the county clerk's office is a secure virtual private network (VPN) connection.[1661]

Voter-verified paper audit trail: Fair

- Depending on the jurisdiction, some voters in Wyoming cast paper ballots, while others vote using DRE machines with VVPR.[1662]

Post-election audits: Unsatisfactory

- The state does not conduct mandatory post-election audits that confirm the accuracy of election results. Within 30 days after an election, Wyoming tests 5 percent of automated tabulating equipment to determine whether the machines are in good working order and are likely to have functioned properly during the election. The test involves feeding the machines a random sample of test ballots—not actual voted ballots—to determine the machines' accuracy.[1663]

Ballot accounting and reconciliation: Unsatisfactory

- All ballots are accounted for at the precinct level.[1664]
- Precincts are required to compare and reconcile the number of ballots with the number of voters who signed in at the polling place.[1665]
- Counties are not explicitly required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount.[1666]
- The state does not use a tally server. As such, a memory card review process is unnecessary.[1667]
- The state requires that vote tallies and ballot reconciliation information be made public.[1668]

Paper absentee ballots: Fair

- The state does not permit voters—including UOCAVA voters—to submit completed ballots electronically. All ballots must be returned by mail or delivered in person.[1669]

Voting machine certification requirements: Fair

- Before they may be purchased and used in the state, all voting machines must be certified by the Election Assistance Commission.[1670]
- Some jurisdictions in the state likely still use voting machines that were purchased more than a decade ago.[1671]

While Wyoming is not currently seeking bids for new voting machines, the counties plan to work with the Wyoming secretary of state's office to seek legislative appropriation for new equipment purchases in time for the 2020 elections.[1672]

Pre-election logic and accuracy testing: Fair

- Election officials conduct mandatory logic and accuracy testing on all voting machines prior to an election.[1673]
- Testing is open to the public.[1674]
- Testing occurs up to two weeks before an election.[1675]

Conclusion

It is critical that the public have confidence in the security of our electoral process and the accuracy of election outcomes to ensure the proper functioning of our democracy. But to maintain confidence in our democratic institutions and elected leaders, Americans must be assured that all votes are cast as the voter intends and counted as they were cast. Our democracy depends on the core faith that election outcomes are accurate and have not been manipulated or inaccurately tabulated through machine error or hacking. Particularly in the current threat environment, urgent action is needed to strengthen the security of America's election infrastructure.

All states have taken steps—of one kind or another—to protect their elections from outside influence or system failure that undermines the security of our elections. Still, there is much room for improvement. Most importantly, all states should operate on a paper-based voting system. In addition, after every election states must carry out robust post-election audits which provide strong evidence that election outcomes are correct. The practice of returning voted ballots electronically—via email, fax, or web portal—should also be prohibited, given widespread consensus that electronic absentee voting is not secure. Finally, voter registration systems must be equipped with strong cybersecurity protections to thwart any effort to infiltrate and alter voter information by sophisticated nation-states. Any voter registration upgrade should be coupled with mandatory cybersecurity training for election officials who use and manage the system. These officials must be trained on cybersecurity best practices so that they are prepared to recognize and respond to suspicious activity and spear-phishing attempts.

Importantly, in recognizing the threat, a number of states are already taking steps to protect their election infrastructure, switching over to paper ballot voting systems, passing laws requiring mandatory risk-limiting audits, and requiring cyber security training for election officials.

By enhancing practices in these areas and others, states can improve their overall election security and bolster public confidence in electoral processes. Of course, state and local election officials should not be expected to meet the mounting threat of election interference on their own. Federal funding is needed to carry out important and necessary election security best practices. Indeed, securing our elections against future hacking attempts and other Election Day disruptions is dependent upon strong partnerships between officials at all levels of government. Congress must step up and provide federal funding and support to the states for the purposes of securing their elections. We can meet this challenge, but we must do it together and we must do it now.

Acknowledgements

The authors specifically wish to thank the many state and local election officials who contributed to this report and the data undergirding its conclusions. We appreciate the time state and local officials spent in conversation over state policies and practices related to election security. Election officials at the state and local level work tirelessly to protect the security of our elections and are now at the forefront of fortifying election infrastructure against foreign adversaries.

There are many organizations and professionals who have been sounding the alarm and offering real solutions to address vulnerabilities in America's election infrastructure for many years, specifically, but not limited to, Brennan Center for Justice, Common Cause, Rutgers School of Law, Verified Voting Foundation, Philip B. Stark, Alex J. Halderman, and others. "Election Security in All 50 States – Defending America's Elections" would not have possible without their foundational research, analysis, and expertise. CAP commends these organizations and individuals for their past and continuing leadership on the issue of election security.

In addition, the authors would like to thank the following people for their contributions:

- Susannah Goodman
- Lawrence Norden
- Richard A. Clarke
- Mark Lindeman
- John McCarthy
- Patrick Barry
- Moira Whelan
- Gwen Calais-Haase
- Adele Hayer

We also wish to thank the following people for their research assistance on this report: Umair Mamsa, Jill Goatcher, H. Elenore Wade, and Komal Shah.

Finally, the authors would like to thank CAP's Editorial team—particularly Lauren Vicary, Chester Hawkins, Will Beaudouin, Alex Kapitan, and Alexis Evangelos.

Endnotes

1 Associated Press, "Federal Government Tells 21 States Election Systems Targeted by Hackers," September 22, 2017, available at https://www.nbcnews.com/storyline/hacking-of-america/federal-government-tells-21-states-election-systems-targeted-hackers-n804031.

2 Callum Borchers, "What we know about the 21 states targeted by Russian hackers," *The Washington Post*, September 23, 2017, available at https://www.washingtonpost.com/news/the-fix/wp/2017/09/23/what-we-know-about-the-21-states-targeted-by-russian-hackers/?utm_term=.b032a821004b.

3 Scott Bauer, "Homeland Security now says Wisconsin elections not targeted," Associated Press, September 27, 2017, available at https://www.apnews.com/10a0080e8fcb4908ae4a852e8c03194d; David Shepardson, "California, Wisconsin deny election systems targeted by Russian hackers," Reuters, September 28, 2017, available at http://www.reuters.com/article/us-usa-election/california-wisconsin-deny-election-systems-targeted-by-russian-hackers-idUSKCN1C32SQ?utm_source=applenews; ABC News, "Texas says DHS Wrong, hacker didn't target state," September 28, 2017, available at http://abcnews.go.com/amp/Technology/wireStory/latest-texas-dhs-wrong-hacker-target-state-50168406; Cynthia McFadden and others, "Russians penetrated U.S. voter systems, top U.S. official says," NBC, February 8, 2018, available at https://www.nbcnews.com/politics/elections/russians-penetrated-u-s-voter-systems-says-top-u-s-n845721.

4 Justin Volz and Jim Finkle, "Voter Registration Databases in Arizona and Illinois Were Breached, FBI Says," Time, August 26, 2016, available at http://time.com/4471042/fbi-voter-database-breach-arizona-illinois/; Associated Press, "Federal Government Tells 21 States Election Systems Targeted by Hackers"; Callum Borchers, "What we know about the 21 states targeted by Russian hackers."

5 Associated Press, "Federal Government Tells 21 States Election Systems Targeted by Hackers."

6 Peter Baker and David E. Sanger, "Trump-Comey Feud Eclipses a Warning on Russia: 'They Will Be Back,'" *The New York Times*, June 10, 2017, available at https://www.nytimes.com/2017/06/10/us/politics/trump-comey-russia-fbi.html.

7 Joe Uchill, "Hackers breach dozens of voting machines brought to conference," *The Hill*, July 29, 2017, available at http://thehill.com/policy/cybersecurity/344488-hackers-break-into-voting-machines-in-minutes-at-hacking-competition.

8 Peter Reuell, "Voting-roll vulnerability," *Harvard Gazette*, September 6, 2017, available at https://news.harvard.edu/gazette/story/2017/09/study-points-to-potential-vulnerability-in-online-voter-registration-systems/.

9 Massimo Calabresi, "Inside Russia's Social Media War on America," *Time*, May 18, 2017, available at http://time.com/4783932/inside-russia-social-media-war-america/.

10 The race was tied between Shelly Simonds (D) and Delegate David Yancey (R). Laura Vozzella, "A rare, random drawing helped Republicans win a tied Virginia election but it may not end there," *The Washington Post*, January 4, 2016, available athttps://www.washingtonpost.com/local/virginia-politics/republican-yancey-picked-in-random-lottery-declared-winner-of-pivotal-va-house-race/2018/01/04/9c9caa5a-f0a1-11e7-b390-a36dc3fa2842_story.html?utm_term=.f49a8842bcae.

11 Associated Press, "Court rules Virginia House of Delegates race a tie," December 20, 2017, available at https://www.washingtonpost.com/lifestyle/kidspost/virginia-democrat-wins-house-of-delegates-seat-by-one-vote-according-to-recount/2017/12/20/eb856c20-e5ab-11e7-ab50-621fe0588340_story.html?utm_term=.8094d78d6da7.

12 *The New York Times*, "Full Transcript and Video: James Comey's Testimony on Capitol Hill," June 8, 2017, available at https://www.nytimes.com/2017/06/08/us/politics/senate-hearing-transcript.html.

13 During an interview with PBS News House, Sens. Amy Klobuchar (D-MN) and James Lankford (R-OK) expressed concern over the state election preparedness and timing of the 2018 elections but noted the potential for widespread vulnerability screenings for election systems and valuable information sharing between states and the federal government. PBS News Hour, "'42 states haven't upgraded their election equipment in over a decade and Russia knows it,'" January 10, 2018, available at https://www.pbs.org/newshour/show/42-states-havent-upgraded-their-election-equipment-in-over-a-decade-and-russia-knows-it; Martin Matishak, "The time to hack-proof the 2018 election is expiring — and Congress is way behind," *Politico*, November 26, 2017, available at https://www.politico.com/story/2017/11/26/election-cybersecurity-hackers-midterms-259472.

14 *The New York Times*, "Full Transcript and Video: James Comey's Testimony on Capitol Hill."

15 Danielle Root and Liz Kennedy, "9 Solutions to Secure America's Elections" (Washington: Center for American Progress, 2017), available at https://www.americanprogress.org/issues/democracy/reports/2017/08/16/437390/9-solutions-secure-americas-elections/.

16 Open Source Election Technology Institute, "Critical Democracy Infrastructure: Protecting American Elections in the Digital Age," September 2017, available at https://trustthevote.org/wp-content/uploads/2017/09/2017_oset-cdi_briefing1.pdf.

17 The topic of cyber security concerns related to online voter registration systems has been written on extensively in recent months and does not need repeating here. Latanya Sweeney, Ji Su Yoo, and Jinyan Zang, "Voter Identity Theft: Submitting Changes to Voter Registrations Online to Disrupt Elections," Technology Science, September 06, 2017, available at https://techscience.org/a/2017090601.

18 U.S. Const. art. I, sec. 4, cl. 1, available at http://press-pubs.uchicago.edu/founders/tocs/a1_4_1.html.

19 Cory Bennett and others, "Cash-strapped states brace for Russian hacking fight," Politico, September 3, 2017, available at https://www.politico.com/story/2017/09/03/election-hackers-russia-cyberattack-voting-242266.

20 "Five are open to it if the money comes with no strings attached, three oppose it, and two say Congress should supply the remaining $395 million it has yet to provide from a pot of money it authorized in 2002." Bennett and others, "Cash-strapped states brace for Russian hacking fight."

21 National Conference of State Legislatures, "Paper Ballots and Direct-Recording Electronic Voting Machines," July 15, 2015, available at http://www.ncsl.org/research/elections-and-campaigns/voting-equipment.aspx.

22 National Conference of State Legislatures, "Paper Ballots and Direct-Recording Electronic Voting Machines."

23 National Conference of State Legislatures, "Paper Ballots and Direct-Recording Electronic Voting Machines."

24 National Conference of State Legislatures, "Paper Ballots and Direct-Recording Electronic Voting Machines."

25 National Conference of State Legislatures, "Paper Ballots and Direct-Recording Electronic Voting Machines."

26 U.S. Election Assistance Commission, "Chapter 13: Canvassing and Certifying an Election," August 26, 2010, available at https://www.eac.gov/assets/1/6/EMG_chapt_13_august_26_2010.pdf; Ballotpedia, "Election Results Certification Dates, 2016," available at https://ballotpedia.org/Election_results_certification_dates,_2016 (last accessed September 2017).

27 Thompson Reuters and West Law, "Certification of Election Results—General Elections (Statutes)" (2009), available at http://www.uniformlaws.org/shared/docs/military%20and%20overseas%20voters/overseasvoters_timetable%20chart.pdf.

28 National Conference of State Legislatures, "Electronic Poll Books: E-Poll Books," March 22, 2017, available at http://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx.

29 Erin Ferns Lee and Marissa Liebling, "How Electronic Poll Books Improve Elections," Project Vote, November 23, 2015, available at http://www.projectvote.org/blog/how-electronic-poll-books-improve-elections/.

30 National Conference of State Legislatures, "Post-Election Audits," August 8, 2017, available at http://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx.

31 Jay Bagga, Joe Losco, and Raymond H. Scheele, "Pre-Election Logic and Accuracy Testing and Post-Election Audit Initiative" (Indianapolis: The Indiana Election Division and the Bowen Center for Public Affairs at Ball State University, 2013), available at https://www.eac.gov/assets/1/28/EAC%20Ball%20State%20Indiana%20Final%20Report.pdf; U.S. Election Assistance Commission, "Voluntary Voting System Guidelines Volume 1-Version 1.1" (2015), available at https://www.eac.gov/assets/1/28/VVSG.1.1.VOL.1.FINAL1.pdf.

32 Bagga, Losco, and Scheele, "Pre-Election Logic and Accuracy Testing and Post-Election Audit Initiative."

33 Bagga, Losco, and Scheele, "Pre-Election Logic and Accuracy Testing and Post-Election Audit Initiative."

34 See generally, Jennie Bretschneider and others, "Risk-Limiting Post-Election Audits: Why and How," Risk-Limiting Audits Working Group, October 2012, available at https://www.stat.berkeley.edu/~stark/Preprints/RLAwhitepaper12.pdf.

35 Bretschneider and others, "Risk-Limiting Post-Election Audits: Why and How."

36 Mark Lindeman and Philip B. Stark, "A Gentle Introduction to Risk-limiting Audits," IEEE Security and Privacy, Special issue on electronic voting, March 16, 2012, available at https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf.

37 U.S. Department of Justice, "The Uniform and Overseas Citizens Absentee Voting Act," available at https://www.justice.gov/crt/uniformed-and-overseas-citizens-absentee-voting-act (last accessed September 2017).

38 U.S. Department of Justice, "The Uniform and Overseas Citizens Absentee Voting Act"; U.S. Department of Justice, "Fact Sheet: Move Act," October 27, 2010, available at https://www.justice.gov/opa/pr/fact-sheet-move-act.

39 U.S. Election Assistance Commission, "About the U.S. EAC," available at https://www.eac.gov/about-the-useac/ (last accessed January 2018).

40 U.S. Election Assistance Commission, "Voluntary Voting System Guidelines," available at https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines/ (last accessed September 2017).

41 U.S. Election Assistance Commission, "System Certification Process," available at https://www.eac.gov/voting-equipment/system-certification-process/ (last accessed September 2017); See generally, U.S. Election Assistance Commission, "Checklist for securing voter registration data," available at https://www.eac.gov/documents/2017/10/23/checklist-for-securing-voter-registration-data/ (last accessed January 17, 2018).

42 U.S. Election Assistance Commission, "Testing & Certification Program Manual: Version 2.0" (2015), available at https://www.eac.gov/assets/1/28/Cert.Manual.4.1.15.FINAL.pdf; U.S. Election Assistance Commission, "Factsheet: The U.S. Election Assistance Commission's Voting System Testing and Certification Program," March 7, 2017, available at https://www.eac.gov/news/2017/03/07/fact-sheet-the-us-election-assistance-commissions-voting-system-testing-and-certification-program-voting-systems-certification-communications-fact-sheet/.

43 A total of 60 systems have applied for certification. U.S. Election Assistance Commission, "Factsheet."

44 U.S. Election Assistance Commission, "Quick Guide: Voting System Certification" (2007), available at https://www.eac.gov/assets/1/1/Quick%20Start%20Guide%20-%20Voting%20System%20Certification.pdf; U.S. Election Assistance Commission, "Certified Voting Systems: About the Testing and Certification Program," available at https://www.eac.gov/voting-equipment/certified-voting-systems/ (last accessed September 2017).

45 U.S. Election Assistance Commission, "System Certification Process."

46 Prior to the establishment of the EAC Voluntary Voting System Guidelines, the Federal Elections Commission was responsible for setting standards for voting equipment, and the National Association of State Election Directors was responsible for ensuring that voting systems abided by them. Federal Elections Commission, "Performance and Test Standards for Punchcard, Marksense, and Direct Recording Electronic Voting Systems" (1990), available at https://www.eac.gov/assets/1/28/FEC_1990_Voting_System_Standards1.pdf; U.S. Election Assistance Commission, "Voluntary Voting System Guidelines"; U.S. Election Assistance Commission, "Quick Guide."

47 U.S. Election Assistance Commission, "Voluntary Voting System Guidelines"; U.S. Election Assistance Commission, "Voluntary Voting System Guidelines Volume 1-Version 1.1,"; U.S. Election Assistance Commission, "Voluntary Voting System Guidelines Volume 1-Version 1.0" (2005), available at https://www.eac.gov/assets/1/28/VVSG.1.0_Volume_1.PDF; Federal Election Commission, "Voluntary Voting System Standards Volume 1: Performance Standards" (2002), available at https://www.eac.gov/assets/1/28/Voting_System_Standards_Volume_I.pdf.

48 The EAC estimates that at least 47 states "use EAC's Testing and Certification program in some way when deciding which voting system to procure." U.S. Election Assistance Commission, "EAC Standards Board Unanimously Approves the 17 Core Voting System Principles," Press release, May 1, 2017, available at https://www.eac.gov/news/2017/05/01/eac-standards-board-unanimously-approves-the-17-core-voting-system-principles/.

49 Brennan Center Task Force on Voting System Security, "The Machinery of Democracy: Protecting Elections in an Electronic World (2006), available at https://www.brennancenter.org/sites/default/files/publications/Machinery%20of%20Democracy.pdf.

50 Ryan Macias, EAC Certification Program Specialist, interview with author, November 27, 2017; U.S. Election Assistance Commission, "Committee Approves Next Generation of Voting System Guidelines," Press release, September 12, 2017, available at https://www.eac.gov/news/2017/09/12/committee-approves-next-generation-of-voting-system-guidelines/; U.S. Election Assistance Commission, "Voluntary Voting System Guidelines"; U.S. Election Assistance Commission, "Voluntary Voting System Guidelines 2.0," available at https://www.eac.gov/assets/1/6/TGDC_Recommended_VVSG2.0_P_Gs.pdf (last accessed January 2018).

51 U.S. Election Assistance Commission, "Chapter 13."

52 National Conference of State Legislatures, "Vote Centers," available at http://www.ncsl.org/research/elections-and-campaigns/vote-centers.aspx (last accessed September 2017).

53 National Conference of State Legislatures, "Vote Centers."

54 National Conference of State Legislatures, "Vote Centers."

55 Jennie Bretschneider and others, "Risk-Limiting Post-Election Audits: Why and How."

56 Verified Voting, "Voting Equipment in the United States," available at https://www.verifiedvoting.org/resources/voting-equipment/ (last accessed September 2017).

57 Verified Voting, "Voting Equipment in the United States."

58 U.S. Election Assistance Commission, "Voting System Laboratories," available at https://www.eac.gov/voting-equipment/voting-system-test-laboratories-vstl/ (last accessed September 2017).

59 U.S. Election Assistance Commission, "Voting System Laboratories."

60 There are currently only two EAC accredited voting system test laboratories: Pro V&V and SLI Compliance. U.S. Election Assistance Commission, "Voting System Laboratories."

61 Lawrence Norden and Ian Vandewalker, "Securing Elections From Foreign Interference" (Washington: Brennan Center for Justice, 2017), available at https://www.brennancenter.org/publication/securing-elections-foreign-interference.

62 A Republican data firm and GOP contractors reportedly leaked personal information belonging to nearly 200 million people in June 2017. See Selena Larson, "Data of Almost 200 Million Voters Leaked Online by GOP Analytics Firm," CNN, June 19, 2017, available at http://money.cnn.com/2017/06/19/technology/voter-data-leaked-online-gop/index.html; Wesley Bruer and Evan Perez, "Officials: Hackers Breach Election Systems in Illinois, Arizona," CNN, August 30, 2016, available at http://www.cnn.com/2016/08/29/politics/hackers-breach-illinois-arizona-election-systems/index.html.

63 Transcript of "Senate Select Intelligence Committee Holds Hearing on Russian Interference in the 2016 Elections, Panel 2."

64 A used election poll book sold on eBay, for example, was recently found to still contain the personal information of 650,000 Tennessee voters after election officials failed to erase sensitive voter data. See Kevin Collier, "Personal Info of 650,000 Voters Discovered on Poll Machine Sold on Ebay," Gizmodo, August 1, 2017, available at http://gizmodo.com/personal-info-of-650-000-voters-discovered-on-poll-mach-1797438462; Lee and Liebling, "How Electronic Poll Books Improve Elections."

65 U.S. Election Assistance Commission, "Checklist for Securing Voter Registration Data," available at https://www.eac.gov/assets/1/28/Checklist_Securing_VR_Data_FINAL_5.19.16.pdf (last accessed September 2017).

66 U.S. Election Assistance Commission, "Checklist for Securing Voter Registration Data."

67 U.S. Election Assistance Commission, "Checklist for Securing Voter Registration Data."

68 U.S. Election Assistance Commission, "Checklist for Securing Voter Registration Data."

69 Margaret Rouse, "HIDS/NIDS (Host Intrusion Detection Systems and Network Intrusion Detection Systems)," available at http://searchsecurity.techtarget.com/definition/HIDS-NIDS (last accessed September 2017).

70 Researchers at RAND Corporation have estimated that there are more than 100,000 reservists with "some degree of cyber competence, including thousands with deep or mid-level cyber expertise." Researchers see the National Guard as an untapped cyber resource that has the potential to attract the very best in cyber industry and offer a valuable resource to states in protecting critical infrastructure. Isaac Porche and Brian Wisniewski, "Reservists and the National Guard offer uptapped resources for cybersecurity," Tech Crunch, April 18, 2017, available at https://techcrunch.com/2017/04/18/reservists-and-the-national-guard-offer-untapped-resources-for-cybersecurity/.

71 Isaac Porche, "Reservists and the National Guard offer untapped resources for cybersecurity," Tech Crunch, April 18, 2017, available at https://techcrunch.com/2017/04/18/reservists-and-the-national-guard-offer-untapped-resources-for-cybersecurity/.

72 Department of Homeland Security, "Statement by Secretary Johnson Concerning the Cybersecurity of the Nation's Election Systems," Press release, September 16, 2016, available at https://www.dhs.gov/news/2016/09/16/statement-secretary-johnson-concerning-cybersecurity-nation%E2%80%99s-election-systems.

73 There is a reported nine-month waiting list for some DHS state services related to election security. However, the National Defense Authorization Act (NDAA) for Fiscal Year 2018 authorizes the federal government to carry out a "Cyber Guard Exercise" on state election systems upon approval by the state. H.R.2810, available at https://www.congress.gov/bill/115th-congress/house-bill/2810/text?q=%7B%22search%22%3A%5B%22national+defense+authorization+act%22%5D%7D&r=2#toc-H4AF0D6197A6B40608955124A85C212CE; U.S. Department of Defense, "Allies, Partners Observe Cyber Guard Exercise," July 5, 2017, available at https://www.defense.gov/News/Article/Article/1238082/allies-partners-observe-cyber-guard-exercise/; Morgan Chalfant, "33 states accepted DHS aid to secure elections," The Hill, August 2, 2017, available at http://thehill.com/policy/cybersecurity/344981-33-states-accepted-dhs-aid-to-secure-elections.

74 Likhitha Butchireddygari, "Many County Election Officials Still Lack Cybersecurity Training," NBC News, August 23, 2017, available at https://www.nbcnews.com/politics/national-security/voting-prep-n790256.

75 *Additional, nongraded information is indicated by gray font throughout the report.*

76 Norden and Vandewalker, "Securing Elections From Foreign Interference."

77 Norden and Vandewalker, "Securing Elections From Foreign Interference."

78 Lawrence Norden, "We Need Election Integrity—Just Not the Way Trump Is Going About It," *Slate*, July 7, 2017, available at http://www.slate.com/articles/technology/future_tense/2017/07/the_real_way_to_fix_the_actual_election_tampering_crisis_in_the_u_s.html; Brian Barrett, "If You Still Use Windows XP, Prepare for the Worst," Wired, May 14, 2017, available at https://www.wired.com/2017/05/still-use-windows-xp-prepare-worst/.

79 Philip B. Stark and Poorvi L. Vora, "Maryland Voting Audit Falls Short," *The Baltimore Sun*, October 28, 2016, available at http://www.baltimoresun.com/news/opinion/oped/bs-ed-voting-audit-20161028-story.html.

80 UCRJames, "How Many Absentee and Provisional Ballots are Left in FL and PA?," Daily Kos, November 14, 2016, available at https://www.dailykos.com/stories/2016/11/14/1599238/-How-Many-Absentee-and-Provisional-Ballots-are-Left-in-FL-and-PA.

81 Pamela Smith and others, "Counting Votes 2012: A State by State Look at Voting Technology Preparedness" (Washington and New Brunswick: Verified Voting, Common Cause, and Rutgers School of Law, 2012), available at http://countingvotes.org/sites/default/files/CountingVotes2012_Final_August2012.pdf.

82 Smith and others, "Counting Votes 2012."

83 See Sari Horwitz, "More Than 30 States Offer Online Voting, But Experts Warn It Isn't Secure," *The Washington Post*, May 17, 2016, available at https://www.washingtonpost.com/news/post-nation/wp/2016/05/17/more-than-30-states-offer-online-voting-but-experts-warn-it-isnt-secure; National Conference of State Legislatures, "Electronic Transmission of Ballots," January 16, 2017, available at http://www.ncsl.org/research/elections-and-campaigns/internet-voting.aspx.

84 Horwitz, "More Than 30 States Offer Online Voting, But Experts Warn It Isn't Secure."

85 National Institute of Standards and Technology, "NIST Activities on UOCAVA Voting," available at https://www.nist.gov/itl/voting/nist-activities-uocava-voting (last accessed September 2017).

86 In states that allow electronic absentee voting, UOCAVA ballots went unreturned 45 percent of the time, on average. However, in states that prohibit electronic absentee ballots, UOCAVA ballots went unreturned only 40 percent of the time, on average. The Pew Charitable Trusts, "Elections Performance Index," August 9, 2016, available at http://www.pewtrusts.org/en/multimedia/data-visualizations/2014/elections-performance-index#state-CT.

87 In 2012, states with only mail-in returns had an average of 75 percent ballots returned while states with the electronic option had 73 percent of ballots returned. In 2014, states with only mail-in returns had an average of 62% ballots returned while states with the electronic option had 54 percent of ballots returned. The Pew Charitable Trusts, "Elections Performance Index," August 9, 2016, available at http://www.pewtrusts. org/en/multimedia/data-visualizations/2014/elections-performance-index#state-CT.

88 Indeed, If we base projections on EAC data for the 2012 general election, which examined the total number of UOCAVA ballots returned and submitted for counting that year (578,706), and compared that to the list of states that allow internet voting, we could expect more than 240,000 (243,5331 to be exact) UOCAVA ballots to be returned via internet in the 2020 election. Of course, that number assumes that all UOCAVA voters in those states would return their ballots via internet, which is not likely the case. Some may opt to return their voted ballots by mail. Moreover, the EAC has not yet come out with their 2016 numbers and UOCAVA reliance on internet voting may have changed since 2012. However, the EAC data offers a rough estimate of how many ballots could be at risk in future elections. U.S. Election Assistance Commission, "Uniformed and Overseas Citizens Absentee Voting Act" (Washington: EAC, 2013), available at https://www.eac.gov/assets/1/28/508compliant_Main_91_p.pdf.

89 We did not consider whether a state's voting machines are connected to the internet. Today, most voting machines are not directly connected to the internet. It is important to note that machines can be hacked even if they aren't connected to the internet. Pam Fessler, "If Voting Machines Were Hacked, Would Anyone Know?", NPR, June 14, 2017, available at http://www.npr.org/2017/06/14/532824432/if-voting-machines-were-hacked-would-anyone-know; Jessica Schulberg, "Good News for Russia: 15 States Use Easily Hackable Voting Machines," The Huffington Post, July 17, 2017, available at https://www.huffingtonpost.com/entry/electronic-voting-machines-hack-russia_us_5967e1c2e4b03389bb162c96.

90 Ryan Macias, EAC Certification Program Specialist, interview with author, November 27, 2017; U.S. Election Assistance Commission, "Committee Approves Next Generation of Voting System Guidelines," Press release, September 12, 2017, available at https://www.eac.gov/news/2017/09/12/committee-approves-next-generation-of-voting-system-guidelines/; U.S. Election Assistance Commission, "Voluntary Voting System Guidelines"; U.S. Election Assistance Commission, "Voluntary Voting System Guidelines 2.0," available at https://www.eac.gov/assets/1/6/TGDC_Recommended_VVSG2.0_P_Gs.pdf (last accessed January 2018).

91 Ben Berliner, "Some States Look to Feds for Help Replacing Old Voting Equipment," FCW, October 26, 2017, available at https://fcw.com/articles/2017/10/26/aging-voting-machines-berliner.aspx.

92 *Additional, non-graded information is indicated by gray font throughout the report.*

93 Brennan Center for Justice, "Voting System Security and Reliability Risks" (2016), available at https://www.brennancenter.org/analysis/fact-sheet-voting-system-security-and-reliability-risks; Norden and Vandewalker, "Securing Elections From Foreign Interference"; Haley Sweetland Edwards, "'Vote Flipping' Happens, but It Doesn't Mean the Election Is Rigged," *Time*, October 27, 2016, available at http://time.com/4547594/vote-flipping-election-rigged/.

94 Lawrence Norden and Christopher Famighetti, "America's Voting Machines at Risk" (Washington: Brennan Center for Justice, 2015), available at https://www.brennancenter.org/publication/americas-voting-machines-risk.

95 J. Alex Halderman, Testimony before the U.S. Senate Select Committee on Intelligence, "Russian interference in the 2016 U.S. elections," June 21, 2017, available at https://www.intelligence.senate.gov/sites/default/files/documents/os-ahalderman-062117.pdf.

96 Open Source Election Technology Institute, "Critical Democracy Infrastructure."

97 See, generally, Bagga, Losco, and Scheele, "Pre-Election Logic and Accuracy Testing and Post-Election Audit Initiative."

98 *Additional, non-graded information is indicated by gray font throughout the report.*

99 Norden and Vandewalker, "Securing Elections From Foreign Interference."

100 Clay Helms, Assistant Director of Elections and Supervisor of Voter Registration, interview with author, October 11, 2017.

101 Clay Helms, interview with author, October 11, 2017.

102 State of Alabama Information Technology, "Policy 672-00: Vulnerability Scanning," available at http://cybersecurity.alabama.gov/documents/Policy_672_Vulnerability_Scanning.pdf (last accessed January 2018).

103 State of Alabama Information Technology, "Policy 672-00."

104 The Alabama secretary of state's office told Yellowhammer that they are working with federal authorities and the state's election system vendor to ensure security. Cliff Sims, "Alabama Moves to Protect Election Systems After FBI Discovers Hacks in Other States," Yellowhammer, August 30, 2016, available at http://yellowhammernews.com/politics-2/alabama-moves-to-protect-election-system-after-fbi-discovers-hacks-in-arizone-illinois/.

105 Clay Helms, interview with author, November 14, 2017.

106 Clay Helms, interview with author, October 11, 2017.

107 The Alabama secretary of state must certify an electronic poll book before it can be used in the state. Any electronic poll book used by the state must "be secure" and "include a failsafe data recovery procedure for information included in the electronic poll book. Ala. Code § 17-4-2.1 (2016), available at http://codes.findlaw.com/al/title-17-elections/al-code-sect-17-4-2-1.html.

108 Megan Brantley, "Select Alabama Polling Places Using Electronic Poll Books in November Election," WHNT, October 18, 2016, available at http://whnt.com/2016/10/18/select-alabama-polling-places-using-electronic-poll-books-in-november-election/.

109 State of Alabama Office of the Secretary of State, "Request for Proposal #2017—003: Electronic Poll Book System or Systems for Two (2) Years in the State of Alabama," May 15, 2017, available at http://sos.alabama.gov/sites/default/files/rfp/RFP-2017-003.pdf.

110 Clay Helms, interview with author, October 11, 2017.

111 Verified Voting, "The Verifier—Polling Place Equipment—November 2016," available at https://thevotingnews.com/verifier/ (last accessed September 2017); Ala. Code § 17-2-4 (2016), available at http://law.justia.com/codes/alabama/2016/title-17/chapter-2/section-17-2-4/.

112 Verified Voting, "State Audit Laws – Alabama," available at https://www.verifiedvoting.org/state-audit-laws/alabama/ (last accessed September 2017).

113 Clay Helms, interview with author, November 14, 2017.

114 Clay Helms, interview with author, November 14, 2017.

115 Clay Helms, interview with author, November 14, 2017; Personal correspondence from Brian Neesby, February 10, 2018.

116 Smith and others, "Counting Votes 2012."

117 Smith and others, "Counting Votes 2012."

118 Alabama is the first state to put into place a fully electronic voting system for armed service members stationed overseas. Ala. Code § 17-11-45 (2016), available at http://codes.findlaw.com/al/title-17-elections/al-code-sect-17-11-45.html; National Conference of State Legislatures, "Electronic Transmission of Ballots."; Jennifer Edwards, "Online Voting for Military Members From Alabama Serving Overseas," ABC, January 27, 2016, available at http://abc3340.com/news/local/online-voting-for-military-members-from-alabama-serving-overseas.

119 Ala. Code § 17-7-23 (2016), available at http://law.justia.com/codes/alabama/2016/title-17/chapter-7/section-17-7-23/; U.S. Election Assistance Commission, "State Requirements and the Federal Voting System Testing and Certification Program," available at https://www.eac.gov/assets/1/1/State%20Requirements%20and%20the%20Federal%20Voting%20System%20Testing%20and%20Certification%20Program.pdf (last accessed September 2017).

120 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

121 Alabama Electronic Voting Committee Administrative Code, "Chapter 307-X-1: Procedures for Electronic Vote Counting Systems" (2002), 307-X-1-.04, available at http://www.alabamaadministrativecode.state.al.us/docs/evc/307-X-1.pdf.

122 Alabama Electronic Voting Committee Administrative Code, "Chapter 307-X-1," 307-X-1-.04.

123 Alabama Electronic Voting Committee Administrative Code, "Chapter 307-X-1," 307-X-1-.04, 307-X-1-.05.

124 Personal communication from Josie Bahnke, Director of Elections, October 26, 2017.

125 "Alaska's Election Security FAQ Sheet" introduced more robust access control to the state's voter registration and election management database. Alaska Division of Elections, "Alaska's Election Security FAQ Sheet," available at http://www.elections.alaska.gov/Headlines/170616%20DOE%20Security%20Update.pdf (last accessed September 2017); Survey response from Josie Bahnke.

126 Survey response from Josie Bahnke.

127 The Alaska Division of Elections says that it has also introduced intrusion detection processes and practices. Alaska Division of Elections, "Alaska's Election Security FAQ Sheet"; Survey response from Josie Bahnke.

128 Alaska Division of Elections, "Alaska's Election Security FAQ Sheet"; Survey response from Josie Bahnke.

129 Alaska Division of Elections, "Alaska's Election Security FAQ Sheet"; Survey response from Josie Bahnke.

130 University of Alaska Anchorage, "Alaska Election Security Report: Phase 2" (2008), available at https://scholarworks.alaska.edu/bitstream/handle/11122/4431/electsec_ph2_final.pdf?sequence=1; Survey response from Josie Bahnke.

131 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books," March 29, 2017, available at http://www.pewtrusts.org/en/multimedia/data-visualizations/2017/a-look-at-how-and-how-many-states-adopt-electronic-poll-books.

132 Personal communication from Josie Bahnke, October 26, 2017.

133 Personal communication from Josie Bahnke, October 26, 2017.

134 Personal communication from Josie Bahnke, October 26, 2017.

135 Personal communication from Josie Bahnke, October 26, 2017. ; Alaska Stat. § 15.15.420 (2016), available at http://law.justia.com/codes/alaska/2016/title-15/chapter-15.15/section-15.15.420/; Alaska Stat. § 15.15.430 (2016), available at http://law.justia.com/codes/alaska/2016/title-15/chapter-15.15/section-15.15.430/; Alaska Stat. § 15.15.440 (2016), available at http://law.justia.com/codes/alaska/2016/title-15/chapter-15.15/section-15.15.440/.

136 Ibid.

137 Survey response from Josie Bahnke.

138 Alaska Stat. § 15.15.430.

139 Alaska Stat. § 15.15.430.

140 Alaska Stat. § 15.15.440.

141 Survey response from Josie Bahnke; Alaska Stat. § 15.15.450 (2016), available at http://law.justia.com/codes/alaska/2016/title-15/chapter-15.15/section-15.15.450/.

142 Local election officials are required to record and certify the number of ballots received by the polling places, the number of ballots voted, the number of spoiled ballots, and the number of unused ballots. The number of voters who signed into the polling place is also recorded. The results are sent to state election officials. Smith and others, "Counting Votes 2012."

143 Smith and others, "Counting Votes 2012."

144 Personal communication from Josie Bahnke, October 26, 2017.

145 Smith and others, "Counting Votes 2012."

146 Smith and others, "Counting Votes 2012."

147 Survey response from Josie Bahnke.

148 Personal communication from Josie Bahnke, December 4, 2017.

149 Personal communication from Josie Bahnke, December 4, 2017.

150 Alaska Stat. § 15.20.910 (2016), available at http://law.justia.com/codes/alaska/2016/title-15/chapter-15.20/article-05/section-15.20.910/.

151 Survey response from Josie Bahnke.

152 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

153 Alaska Stat. § 15.20.900 (2016), available at http://law.justia.com/codes/alaska/2016/title-15/chapter-15.20/article-05/section-15.20.900/; Alaska Legal Resource Center, "6 AAC 25.045. Accu-Vote Tests and Security," available at http://www.touchngo.com/lglcntr/akstats/aac/title06/chapter025/section045.htm (last accessed January 2018); survey response from Josie Bahnke.

154 Survey response from Josie Bahnke.

155 Norden and Vandewalker, "Securing Elections From Foreign Interference."

156 The "State of Arizona Election Procedures Manual" says the statewide voter registration system includes PowerLock, an interface where administrators may determine security and permission levels for users to access the database. Survey response from Reynaldo Valenzuela Jr., Director of Elections, Maricopa County; Arizona Secretary of State, "Secretary Reagan Sounds Alarm on Voter Data Security," September 9, 2016, available at https://www.azsos.gov/about-office/media-center/video-gallery/1077; Arizona Secretary of State, "State of Arizona Elections Procedures Manual" (2017), available at https://www.azsos.gov/sites/azsos.gov/files/2017-2018_arizona_election_procedures_manual_chapter_1_public_draft.pdf.

157 Survey response from Reynaldo Valenzuela Jr..

158 Survey response from Reynaldo Valenzuela Jr..

159 Survey response from Reynaldo Valenzuela Jr.; Arizona Secretary of State, "State of Arizona Elections Procedures Manual."

160 Survey response from Reynaldo Valenzuela Jr.; Arizona Secretary of State, "Arizona Secretary of State Michele Reagan Talks Cybersecurity With CBS Evening News," October 13, 2016, available at https://www.azsos.gov/about-office/media-center/video-gallery/1115.

161 Bennett and others, "Cash-strapped states brace for Russian hacking fight."

162 Pew, "A Look at How—and How Many—States Adopt Electronic Poll Books";Ariz. Rev. Stat. § 16-511 (2016), available at http://law.justia.com/codes/arizona/2016/title-16/section-16-511/; Ariz. Rev. Stat. § 16-571 (2016), available at http://law.justia.com/codes/arizona/2016/title-16/section-16-571/.

163 Ariz. Rev. Stat. §§ 16-511, 16-571; Arizona Secretary of State, "State of Arizona Elections Procedures Manual.".

164 Survey response from Reynaldo Valenzuela Jr.

165 Survey response from Reynaldo Valenzuela Jr.

166 Letter from Eric Spencer, State Election Director, October 13, 2017 (on file with author).

167 Survey response from Reynaldo Valenzuela Jr.

168 Letter from Eric Spencer, State Election Director, October 13, 2017 (on file with author).

169 Survey response from Reynaldo Valenzuela Jr.

170 Verified Voting, "State Audit Laws – Arizona," March 2017, available at https://www.verifiedvoting.org/state-audit-laws/arizona/.

171 Ariz. Rev. Stat. § 16-602 (2016), available at http://law.justia.com/codes/arizona/2016/title-16/section-16-602/.

172 Ariz. Rev. Stat. § 16-602.

173 Ariz. Rev. Stat. § 16-602.

174 Survey response from Reynaldo Valenzuela Jr.; Ariz. Rev. Stat. § 16-602.

175 From a survey response from Reynaldo Valenzuela Jr.: "Yes, if the randomly selected races result in a difference in any race that is equal to or greater than the designated margin when compared to the electronic tabulation of those same ballots, a second hand count of those same ballots and races shall be performed. If the second hand count results in a difference in any race that is equal to or greater than the designated margin when compared to the electronic tabulation for those same ballots, the hand count shall be expanded to include the entire jurisdiction. The 'designated margin' is set by a committee prior to every federal election and the current margins established [are] set at five votes or two percent, whichever is greater for early ballot and three votes or one percent, whichever is greater for regular ballots cast at the polls." See also Ariz. Rev. Stat. § 16-602.

176 Ariz. Rev. Stat. § 16-602.

177 Survey response from Reynaldo Valenzuela Jr.

178 Audits begin within 24 hours of the polls closing and must be completed before the official vote canvass. Ariz. Rev. Stat. § 16-602.

179 Survey response from Reynaldo Valenzuela Jr.; Ariz. Rev. Stat. § 16-602.

180 Once polls close, local officials are responsible for tallying all valid votes and identifying invalid ballots. Results from each voting machine and ballots cast provisionally are tallied before results are certified and delivered to county election officials. Smith and others, "Counting Votes 2012."

181 Smith and others, "Counting Votes 2012."

182 State law requires that precinct totals be reviewed as part of the state canvassing process. If discrepancies arise, precinct officials are called upon to explain the discrepancy and the votes are retallied. If discrepancies persist, the machine is inspected and the vote total may be changed to reflect the results. Smith and others, "Counting Votes 2012."

183 Smith and others, "Counting Votes 2012."

184 Smith and others, "Counting Votes 2012."

185 Smith and others, "Counting Votes 2012."

186 Survey response from Reynaldo Valenzuela Jr.; Letter from Eric Spencer, State Election Director, October 13, 2017 (on file with author); Arizona Secretary of State, "Military and Overseas Voters," available at https://www.azsos.gov/elections/voting-election/military-and-overseas-voters (last accessed September 2017); Federal Voting Assistance Program, "Arizona" (2017), available at https://www.fvap.gov/uploads/FVAP/States/arizona.pdf; National Conference of State Legislatures, "Electronic Transmission of Ballots."

187 Reynaldo Valenzuela Jr.; Ariz. Rev. Stat. § 16-442 (through 2nd reg. sess. 50th Leg. 2012), available at http://law.justia.com/codes/arizona/2012/title16/section16-442.

188 At least one county—Maricopa County—has plans to replace its machines sometime over the next few years. While Maricopa County has not entered into the bid process yet, it plans to begin a request for information (RFI) process in 2018 to collect information to then ready Maricopa County for an official request for proposal (RFP) request to vendors in late 2019. Survey response from Reynaldo Valenzuela Jr.; Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

189 Letter from Eric Spencer, State Election Director, October 13, 2017 (on file with author).

190 From a letter from Eric Spencer, State Election Director, October 13, 2017 (on file with author): "The Secretary of State's Office then conducts logic and accuracy testing in all 15 counties using a random sample of each county's equipment"; Ariz. Rev. Stat. § 16-449 (2016), available at http://law.justia.com/codes/arizona/2016/title-16/section-16-449/.

191 In Maricopa County, notice is usually provided approximately seven days before testing. Survey response from Reynaldo Valenzuela Jr.; Ariz. Rev. Stat. § 16-449.

192 Letter from Eric Spencer, State Election Director, October 13, 2017 (on file with author); Ariz. Rev. Stat. § 16-449.

193 Norden and Vandewalker, "Securing Elections From Foreign Interference."

194 Ark. Code § 7-5-107 (2016), available at http://law.justia.com/codes/arkansas/2016/title-7/chapter-5/subchapter-1/section-7-5-107/; Ark. Code § 7-5-109 (2016), available at http://law.justia.com/codes/arkansas/2016/title-7/chapter-5/subchapter-1/section-7-5-109/.

195 Verified Voting, "The Verifier—Polling Place Equipment—November 2016"; Arkansas Secretary of State, "Arkansas's Voting Machines," available at https://www.sos.arkansas.gov/elections/voter-information/arkansass-voting-machines (last accessed January 2018).

196 Ark. Code § 7-5-301 (2016), available at http://law.justia.com/codes/arkansas/2016/title-7/chapter-5/subchapter-3/section-7-5-301/; Ark. Code § 7-5-532 (2016), available at http://law.justia.com/codes/arkansas/2016/title-7/chapter-5/subchapter-5/section-7-5-532/; Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

197 National Conference of State Legislatures, "Post-election Audits."

198 At the end of the day on Election Day, state law requires poll workers in jurisdictions using optical scan machines to tally the votes counted by the scanners. Write-in ballots are also counted. Overvotes are also examined and may be counted if the voter's intent is able to be discerned. Smith and others, "Counting Votes 2012."

199 Smith and others, "Counting Votes 2012."

200 Smith and others, "Counting Votes 2012.

201 Smith and others, "Counting Votes 2012."

202 Smith and others, "Counting Votes 2012."

203 Smith and others, "Counting Votes 2012."

204 Smith and others, "Counting Votes 2012."

205 National Conference of State Legislatures, "Electronic Transmission of Ballots."

206 Ark. Code § 7-5-504 (2016), available at http://law.justia.com/codes/arkansas/2016/title-7/chapter-5/subchapter-5/section-7-5-504.

207 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

208 Bennett and others, "Cash-strapped states brace for Russian hacking fight."

209 Ark. Code § 7-5-611 (2016), available at http://law.justia.com/codes/arkansas/2016/title-7/chapter-5/subchapter-6/section-7-5-611/; Ark. Code § 7-5-515 (2016), available at http://law.justia.com/codes/arkansas/2016/title-7/chapter-5/subchapter-5/section-7-5-515/.

210 Ark. Code § 7-5-515.

211 Ark. Code §§ 7-5-611, 7-5-515.

212 Voting System Assessment Project, "Voting Reimagined," available at http://vsap.lavote.net/ (last accessed October 2017).

213 Norden and Vandewalker, "Securing Elections From Foreign Interference."

214 Susan Lapsley, Deputy Secretary of State, Help America Vote Act, Activities and Counsel, interview with author, September 26, 2017.

215 Susan Lapsley, interview with author, September 26, 2017.

216 Interview with Susan Lapsley, interview with author, September 26, 2017.

217 Interview with Susan Lapsley, interview with author, September 26, 2017.

218 Interview with Susan Lapsley, interview with author, September 26, 2017.

219 Interview with Susan Lapsley, interview with author, September 26, 2017.

220 Calif. Senate Bill No. 439 (2015), available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201520160SB439.

221 Legislation was introduced that would require polling places that use electronic poll books to have paper copies of voter registration lists available on Election Day. Susan Lapsley, interview with author, September 26, 2017; The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

222 Before "utilization of an electronic poll book for any election, the elections official shall verify and document the readiness of each electronic poll book prior to its use." Personal communication from Susan Lapsley, November 8, 2017; Calif. Code of Regs. § 20165, available at http://admin.cdn.sos.ca.gov/regulations/proposed/elections/poll-book/text-proposed-regulations.pdf; The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

223 Billy Kobin, "Rapid response: What they're saying about Jerry Brown's California budget," *Sacramento Bee*, January 10, 2018, available at http://www.sacbee.com/news/politics-government/capitol-alert/article193991034.html.

224 California Secretary of State's Office, "Secretary of State Padilla Appointed to the Department of Homeland Security's Election Infrastructure Cybersecurity Working Group," Press release, September 1, 2016, available at http://www.sos.ca.gov/administration/news-releases-and-advisories/2016-news-releases-and-advisories/secretary-state-padilla-appointed-department-homeland-securitys-election-infrastructure-cybersecurity-working-group/.

225 There are 58 counties that rely on paper ballots exclusively. Susan Lapsley, interview with author, September 26, 2017; Verified Voting, "The Verifier—Polling Place Equipment—November 2016"; Calif. Elec. Code § 19101 (2016), available at http://law.justia.com/codes/california/2016/code-elec/division-19/chapter-2/section-19101/; Calif. Elec. Code § 19273 (2016), available at http://law.justia.com/codes/california/2016/code-elec/division-19/chapter-3/article-6/section-19273/.

226 Calif. Elec. Code § 336.5 (2016), available at http://law.justia.com/codes/california/2016/code-elec/division-0.5/chapter-4/section-336.5/; Calif. Elec. Code § 15360 (2016), available at http://law.justia.com/codes/california/2016/code-elec/division-15/chapter-4/article-5/section-15360/.

227 Verified Voting, "State Audit Laws – California," March 2017, available at https://www.verifiedvoting.org/state-audit-laws/california/.

228 Calif. Elec. Code §§ 336.5, 15360.

229 Ibid.

230 Calif. Assembly Bill No. 840 (2017), available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB840.

231 Calif. Elec. Code § 15360.

232 Calif. Elec. Code § 15360.

233 Calif. Elec. Code § 15360.

234 Calif. Elec. Code § 15360(e) (2016), available at http://law.justia.com/codes/california/2016/code-elec/division-15/chapter-4/article-5/section-15360/.

235 Calif. Assembly Bill No. 840; Kammi Foote, Kim Alexander, and Barbara Simons, "Letter: Gov. Brown, Don't Make It Easier to Meddle in Our Elections," *The Sacramento Bee*, October 1, 2017, available at http://www.sacbee.com/opinion/letters-to-the-editor/article176432006.html; The Editorial Board, "Here's How Jerry Brown Can Help Protect Vulnerable People, Voting Integrity and Local Control," *The Sacramento Bee*, September 28, 2017, available at http://www.sacbee.com/opinion/editorials/article176017476.html.

236 Once polls close, local election officials are tasked with accounting for all ballots. This involves identifying and discarding unused ballots and separating voted and write-in ballots from void or spoiled ballots by placing them in separate containers. Poll workers must check to make sure that the number of regular and provisional ballots that were cast—as well as the number of spoiled and unused ballots—match the total number of ballots delivered to the precinct. All votes cast—including mail-in absentee ballots—are tallied at the precinct level. Afterward, all ballots are sent to the receiving centers or central tabulating location. Smith and others, "Counting Votes 2012."

237 Smith and others, "Counting Votes 2012."

238 Smith and others, "Counting Votes 2012."

239 Smith and others, "Counting Votes 2012."

240 Smith and others, "Counting Votes 2012."

241 Susan Lapsley, interview with author, September 26, 2017; National Conference of State Legislatures, "Electronic Transmission of Ballots."

242 Susan Lapsley, interview with author, September 26, 2017; Calif. Elec. Code § 19101.

243 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

244 Voting System Assessment Project, "Voting Reimagined," available at http://vsap.lavote.net/ (last accessed October 2017).

245 Voting System Assessment Project, "Process," available at http://vsap.lavote.net/ (last accessed October 2017); Diana Budds, "Voting Needs a Serious Overhaul and L.A. Might Have the Solution," CO. Design, July 13, 2015, available at https://www.fastcodesign.com/3049203/voting-needs-a-serious-overhaul-and-la-might-have-the-solution.

246 Budds, "Voting Needs a Serious Overhaul and L.A. Might Have the Solution."

247 Calif. Elec. Code § 15000 (2016), available at http://law.justia.com/codes/california/2016/code-elec/division-15/chapter-1/section-15000/.

248 Susan Lapsley, interview with author, September 26, 2017.

249 Calif. Elec. Code § 15000.

250 Election vendors are required to notify the Colorado secretary of state within 72 hours of any software incident with its equipment. Norden and Vandewalker, "Securing Elections From Foreign Interference"; Colorado Secretary of State, "Election Rules [8 CCR 1505-1]: Rule 11. Voting Systems," 11.8, available at https://www.sos.state.co.us/pubs/rule_making/CurrentRules/8CCR1505-1/Rule11.pdf.

251 Judd Choate, State Election Director, interview with author, November 14, 2017.

252 Judd Choate, interview with author, November 14, 2017.

253 Judd Choate, interview with author, November 14, 2017.

254 Judd Choate, interview with author, November 14, 2017.

255 Survey response from Judd Choate.

256 Survey response from Judd Choate.

257 Judd Choate, interview with author, September 18, 2017; Colo. Rev. Stat. § 1-5-302 (2016), available at http://law.justia.com/codes/colorado/2016/title-1/general-primary-recall-and-congressional-vacancy-elections/article-5/part-3/section-1-5-302; The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

258 Survey response from Judd Choate; The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books,"

259 Judd Choate, interview with author, November 14, 2017; Judd Choate, interview with author, February 8, 2018.

260 Judd Choate, interview with author, November 14, 2017.

261 In 2014, 95 percent of votes cast in Colorado were paper ballots returned by mail or at a drop-off location. Verified Voting, "The Verifier—Polling Place Equipment—November 2016"; Nathanial Minor, "It Would Be Really Hard To 'Rig' Colorado's Election System. Here's Why," Colorado Public Radio, October 20, 2016, available at http://www.cpr.org/news/story/it-would-be-really-hard-to-rig-colorados-election-system-heres-why.

262 Judd Choate, interview with author, November 14, 2017; Colo. Rev. Stat. § 1-5-615 (2016), available at http://law.justia.com/codes/colorado/2016/title-1/general-primary-recall-and-congressional-vacancy-elections/article-5/part-6/section-1-5-615/; Colol. Rev. Stat. § 1-5-801 (2016), available at http://law.justia.com/codes/colorado/2016/title-1/general-primary-recall-and-congressional-vacancy-elections/article-5/part-8/section-1-5-801/.

263 Survey response from Judd Choate; Colo. Rev. Stat. § 1-7-515 (2016), available at http://law.justia.com/codes/colorado/2016/title-1/general-primary-recall-and-congressional-vacancy-elections/article-7/part-5/section-1-7-515/; Colorado Secretary of State, "Election Rules [8 CCR 1505-1]: Rule 11. Voting Systems," 11.9.4; Eric Geller, "Colorado to Require Advanced Post-Election Audits," Politico, July 17, 2017, available at http://www.politico.com/story/2017/07/17/colorado-post-election-audits-cybersecurity-240631.

264 Verified Voting, "State Audit Laws – Colorado," March 2017, available at https://www.verifiedvoting.org/state-audit-laws/colorado/.

265 Colo. Rev. Stat. § 1-7-515; Colorado Secretary of State, "Election Rules [8 CCR 1505-1]: Rule 11. Voting Systems," 11.9.4; Geller, "Colorado to Require Advanced Post-Election Audits."

266 Survey response from Judd Choate.

267 Ibid.

268 Survey response from Judd Choate.

269 Judd Choate, interview with author, September 18, 2017

270 Judd Choate, interview with author, September 18, 2017.

271 Judd Choate, interview with author, November 14, 2017.

272 Survey response from Judd Choate.

273 Judd Choate, interview with author, September 18, 2017.

274 Judd Choate, interview with author, November 14, 2017.

275 Judd Choate, interview with author, November 14, 2017.

276 Judd Choate, interview with author, November 14, 2017.

277 Judd Choate, interview with author, November 14, 2017.

278 Judd Choate, interview with author, November 14, 2017.

279 Colorado secure ballot return for electronically voted ballots allows voters to drop their ballots on an FTP site or online file deck. Instead of sending a voted ballot across the internet, eligible voters stationed or living overseas can upload their voted ballots onto the FTP site, which is protected by username and password. Through this, voted ballots are made inaccessible to malicious actors who may otherwise try to manipulate voted ballots sent across the internet. Afterward, county officials log into the file deck to retrieve the ballots. Judd Choate, interview with author; Colorado Secretary of State, "Uniformed and Overseas Electors FAQs and Additional Resources," available at https://www.sos.state.co.us/pubs/elections/FAQs/UOCAVA.html (last accessed September 2017); National Conference of State Legislatures, "Electronic Transmission of Ballots."

280 Colo. Rev. Stat. § 1-5-608.5 (2016), available at http://law.justia.com/codes/colorado/2016/title-1/general-primary-recall-and-congressional-vacancy-elections/article-5/part-6/section-1-5-608.5/.

281 Judd Choate, interview with author, November 14, 2017.

282 Colorado Secretary of State, "Election Rules [8 CCR 1505-1]: Rule 11. Voting Systems," § 11.8.2.

283 Colo. Rev. Stat. § 1-7-509 (2016), available at http://law.justia.com/codes/colorado/2016/title-1/general-primary-recall-and-congressional-vacancy-elections/article-7/part-5/section-1-7-509/; Colorado Secretary of State, "Election Rules [8 CCR 1505-1]: Rule 11. Voting Systems," 11.3.2.

284 Colo. Rev. Stat. § 1-7-509.

285 Colorado Secretary of State, "Election Rules [8 CCR 1505-1]: Rule 11. Voting Systems," 11.3.2.

286 The state's voter registration system must meet cybersecurity standards developed by experts at the University of Connecticut's VoTeR Center. Norden and Vandewalker, "Securing Elections From Foreign Interference"; Peggy Reeves, Director of Elections, and Shannon Wegele, Chief of Staff, interview with author, September 8, 2017.

287 Melody A. Currey and Mark Raymond, "Cybersecurity Study: Pursuant to Special Act 15-13," January 1, 2017, available at http://das.ct.gov/images/1090/2017%20DASCybersecurityReport%20SA%2015-13.pdf.

288 Currey and Raymond, "Cybersecurity Study."

289 Peggy Reeves, interview with author, October 13, 2017.

290 Peggy Reeves, interview with author, October 13, 2017.

291 Peggy Reeves and Shannon Wegele, interview with author, September 8, 2017.

292 Peggy Reeves and Shannon Wegele, interview with author, September 8, 2017.

293 Personal correspondence from Peggy Reeves, October 25, 2017. Conn. Gen. Stat. § 9-261c, available at http://codes.findlaw.com/ct/title-9-elections/ct-gen-st-sect-9-261c.html.

294 Peggy Reeves and Shannon Wegele, interview with author, September 8, 2017; Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

295 The state enlists the help of the University of Connecticut's VoTeR Center to carry out post-election audits. Peggy Reeves and Shannon Wegele, interview with author, September 8, 2017.

296 Public Act No. 15-224 (2015), available at https://www.cga.ct.gov/2015/ACT/PA/2015PA-00224-R00SB-01051-PA.htm.

297 The state used to require that a minimum of 10 percent of voting districts be audited. Peggy Reeves and Shannon Wegele, interview with author, September 8, 2017; Conn. Gen. Stat. § 9-320f, available at https://www.cga.ct.gov/current/pub/chap_148.htm#sec_9-320f.

298 Conn. Gen. Stat. § 9-320f.

299 Conn. Gen. Stat. § 9-320f.

300 Ibid.

301 Personal correspondence from Peggy Reeves, October 25, 2017.

302 The Connecticut secretary of state can order a discrepancy re-canvass, statewide if necessary, if the margin of victory in the race for such office is less than the amount of the discrepancy multiplied by the total number of districts where the race appeared. In addition, the secretary of state can conduct further investigation of a tabulator malfunction to determine if it needs to be decertified. Conn. Gen. Stat. § 9-320f.

303 Conn. Gen. Stat. § 9-320f; Personal correspondence from Peggy Reeves, September 25, 2017.

304 Conn. Gen. Stat. § 9-320f; Personal correspondence from Peggy Reeves, October 25, 2017.

305 Peggy Reeves, interview with author, October 13, 2017.

306 Peggy Reeves, interview with author, October 13, 2017.

307 After polls close, municipal officials tally the number of votes cast for each candidate and ballot issue. The total number of voted, spoiled, and unused ballots, as well as the total number of ballots received, are also counted at the municipal level. Smith and others, "Counting Votes 2012."

308 Peggy Reeves, interview with author, October 13, 2017.

309 Personal correspondence from Peggy Reeves, October 25, 2017.

310 Peggy Reeves, interview with author, October 13, 2017.

311 Smith and others, "Counting Votes 2012."

312 Conn. Gen. Stat. § 9-140b, available at http://codes.findlaw.com/ct/title-9-elections/ct-gen-st-sect-9-140b.html; National Conference of State Legislatures, "Electronic Transmission of Ballots."

313 The state maintains a close partnership with the VoTeR Center, which provides the state testing and IT support for election machines and equipment. All machine testing is carried out by the VoTeR Center. The state has found this partnership valuable for several reasons, including the fact that university staffers who conduct the testing are intimately familiar with Connecticut's election process, which allows them to make practical assessments of equipment usage. The state also believes that testing voting equipment through the university rather than through a vender eliminates bias, because the university staff and students are not paid by the state to conduct the testing and therefore have no incentive to potentially skew results or impart a biased determination of the security or functionality of a particular piece of equipment. Conn. Gen. Stat. § 9-242, available at http://codes.findlaw.com/ct/title-9-elections/ct-gen-st-sect-9-242.html; Peggy Reeves and Shannon Wegele, interview with author, September 8, 2017.

314 While the state does not have any plans to replace its voting machines any time soon, it did replace some individual machine components in 2016, upgrading to memory cards without batteries. Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference"; Peggy Reeves and Shannon Wegele, interview with author, September 8, 2017.

315 University of Connecticut, "Center for Voting Technology and Research (VoTeR Center)," available at https://voter.engr.uconn.edu/voter/ (last accessed September 2017).

316 "The pre-election audit has three primary goals: (i) determine whether or not the memory cards are properly programmed for the specific district and specific election, (ii) determine whether or not proper pre-election procedures are followed by the election officials, and (iii) determine whether or not any technical failures occurred."

"The post-election audit focuses on the memory cards that were used in the election. The audits have three primary goals: (i) determine whether or not the memory cards are still properly programmed after the election is closed for the specific district and specific election, (ii) determine whether or not proper pre-election procedures are followed by the election officials, and whether the usage of the cards is consistent with the proper conduct of the election, and (iii) determine whether or not any technical failures occurred. The post-election audit employs a procedure similar to the pre-election audit." Alexander Shvartsman and others, "Pre-Election Audit of Memory Cards for the November 5, 2013 Connecticut Elections" (Storrs, CT: UConn Center for Voting Technology Research, 2014), available athttps://voter.engr.uconn.edu/voter/wp-content/uploads/VC-audit-pre-2013-11.pdf; Personal correspondence from Peggy Reeves, October 25, 2017.

317 Notice must be given to the chairs of the town committees and candidates at least one day before the testing. Peggy Reeves and Shannon Wegele, interview with author, September 8, 2017.

318 Peggy Reeves and Shannon Wegele, interview with author, September 8, 2017.

319 Peggy Reeves and Shannon Wegele, interview with author, September 8, 2017.

320 Norden and Vandewalker, "Securing Elections From Foreign Interference."

321 Personal correspondence from Elaine Manlove, State Election Commissioner, November 14, 2017.

322 Ibid.

323 Personal correspondence from Elaine Manlove, State Election Commissioner, January 2, 2018.

324 Ibid.

325 Elaine Manlove, interview with author, September 19, 2017.

326 Butchireddygari, "Many County Election Officials Still Lack Cybersecurity Training."

327 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

328 Michael Wines, "Wary of Hackers, States Move to Upgrade Voting Systems," *The New York Times*, October 14, 2017, available at https://www.nytimes.com/2017/10/14/us/voting-russians-hacking-states-.html?_r=0.

329 Elaine Manlove, interview with author, September 19, 2017; Verified Voting, "The Verifier—Polling Place Equipment—November 2016"; State of Delaware, "Electronic Voting Machines," available at https://elections.delaware.gov/technology/electronicmachine.shtml (last accessed September 2017).

330 While Delaware has an election statute that refers to an "audit," this law pertains to the number of voters who participated in the election and is a reconciliation of the voter logs, not an audit of machines used or votes cast. 15 Del. Code § 7558, available at http://delcode.delaware.gov/title15/c075/sc04/index.shtml; Elaine Manlove, interview with author, September 19, 2017.

331 Elaine Manlove, interview with author, September 19, 2017.

332 Elaine Manlove, interview with author, September 19, 2017.

333 Elaine Manlove, interview with author, September 19, 2017.

334 Smith and others, "Counting Votes 2012."

335 Smith and others, "Counting Votes 2012."

336 Smith and others, "Counting Votes 2012."

337 Smith and others, "Counting Votes 2012."

338 Personal correspondence from Elaine Manlove, November 14, 2017.

339 Personal correspondence from Elaine Manlove, November 14, 2017.

340 15 Del. Code § 5001 (2016), available at http://law.justia.com/codes/delaware/2016/title-15/chapter-50/section-5001/.

341 Lawrence and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference"; Elaine Manlove, interview with author, September 19, 2017.

342 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference"; Elaine Manlove, interview with author, September 19, 2017.

343 Elaine Manlove, interview with author, September 19, 2017.

344 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference"; Elaine Manlove, interview with author, September 19, 2017.

345 Elaine Manlove, interview with author, September 19, 2017.

346 Personal correspondence from Elaine Manlove, November 14, 2017.

347 15 Del. Code § 5008a (2016), available at http://codes.findlaw.com/de/title-15-elections/de-code-sect-15-5008a.html.

348 Elaine Manlove, interview with author, September 19, 2017.

349 15 Del. Code § 5008a.

350 Washington D.C.'s voter registration system is 20 years old. Alice Miller, Executive Director of the Board of Elections, and Antoine Fagan, Chief Technology Officer, interview with author, October 5, 2017.

351 Alice Miller and Antoine Fagan, interview with author, October 5, 2017.

352 Alice Miller and Antoine Fagan, interview with author, October 5, 2017.

353 Alice Miller and Antoine Fagan, interview with author, October 5, 2017.

354 Alice Miller and Antoine Fagan, interview with author, October 5, 2017.

355 Alice Miller and Antoine Fagan, interview with author, October 5, 2017.

356 Alice Miller and Antoine Fagan, interview with author, October 5, 2017.

357 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books"; National Conference of State Legislatures, "Electronic Poll Books."

358 Alice Miller and Antoine Fagan, interview with author, October 5, 2017.

359 Alice Miller and Antoine Fagan, interview with author, October 5, 2017.

360 Verified Voting, "The Verifier—Polling Place Equipment—November 2016"; Drew Desilver, "On Election Day, Most Voters Use Electronic or Optical-Scan Ballots" (Washington: The Pew Charitable Trusts, 2016), available at http://www.pewresearch.org/fact-tank/2016/11/08/on-election-day-most-voters-use-electronic-or-optical-scan-ballots/.

361 Verified Voting, "State Audit Laws – District of Columbia," March 2017, available at https://www.verifiedvoting.org/state-audit-laws/district%20of%20columbia/.

362 D.C. Code Ann. §1–1001.09a, available at https://beta.code.dccouncil.us/dc/council/code/sections/1-1001.09a.html.

363 D.C. Code Ann. § 1–1001.09a.

364 D.C. Code Ann. § 1–1001.09a.

365 D.C. Code Ann. § 1–1001.09a.

366 D.C. Code Ann. §1-1001.09(c)(1)(B), available at https://beta.code.dccouncil.us/dc/council/code/sections/1-1001.09a.html.

367 D.C. Code Ann. § 1–1001.09a.

368 D.C. Code Ann. § 1–1001.09a.

369 D.C. Code Ann. § 1–1001.09a.

370 D.C. Code Ann. § 1–1001.09a.

371 D.C. Code Ann. § 1–1001.09a.

372 D.C. Code Ann. § 1–1001.09a.

373 After the polls close, poll workers are required to scan and tabulate all votes cast and record the totals. All ballots—including those voted, spoiled, and unused—are accounted for at the polling place. Vote totals, as well as all voting materials, are securely transferred to the central counting location. Smith and others, "Counting Votes 2012."

374 Smith and others, "Counting Votes 2012."

375 Smith and others, "Counting Votes 2012."

376 Smith and others, "Counting Votes 2012."

377 Alice Miller and Antoine Fagan, interview with author, October 5, 2017 ; Smith and others, "Counting Votes 2012."

378 Smith and others, "Counting Votes 2012."

379 D.C. Rule 3-718, available at http://www.dcregs.dc.gov/Gateway/RuleHome.aspx?RuleID=3801738; National Conference of State Legislatures, "Electronic Transmission of Ballots."

380 62 D.C. Code § 14744, available at http://dcregs.dc.gov/Gateway/FinalAdoptionHome.aspx?RuleVersionID=4504115; U.S. Election Assistance Commission, "State Requirements and the Federal Voting System Testing and Certification Program."

381 Brian Barrett, "America's Electronic Voting Machines Are Scarily Easy Targets," Wired, August 2, 2017, available at https://www.wired.com/2016/08/americas-voting-machines-arent-ready-election/.

382 Barrett, "America's Electronic Voting Machines Are Scarily Easy Targets."

383 D.C. Rule § 3-801, available at http://www.dcregs.dc.gov/Gateway/RuleHome.aspx?RuleNumber=3-801.

384 D.C. Rule § 3-801.4, available at http://www.dcregs.dc.gov/Gateway/RuleHome.aspx?RuleNumber=3-801.

385 Norden and Vandewalker, "Securing Elections From Foreign Interference."

386 Florida Department of State, Division of Election, "A Compilation of the Election Laws of the State of Florida" (2016), 98.035, available at http://dos.myflorida.com/media/693802/election-laws.pdf.

387 Florida Department of State, Division of Election, "A Compilation of the Election Laws of the State of Florida," 97.0525.

388 Ali Breland, "State Declines DHS Security for Voting Machines," The Hill, August 26, 2016, available at http://thehill.com/policy/technology/293522-two-swing-states-decline-dhs-security-for-voting-machines.

389 Fla. Stat. § 98.461 (2016), available at http://www.leg.state.fl.us/Statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0000-0099/0098/Sections/0098.461.html; The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

390 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

391 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

392 Gary Fineout, "Florida May Counter "Growing Threat" To Election Security," Sun Sentinel, November 19, 2017, available at http://www.sun-sentinel.com/news/florida/fl-reg-florida-election-security-20171119-story.html.

393 Ibid; "Governor Rick Scott's 2018-2019 budget: Cyber security for counties," http://www.fightingforfloridasfuturebudget.com/web%20forms/Budget/BudgetIssueDetail.aspx?ndx=13&si=45100200&pc=16010000000&icd=36010C0&icnt=21&title=CYBER%20SECURITY%20FOR%20COUNTIES (Last visited January 3, 2018).

394 Gary Fineout, "Florida May Counter "Growing Threat" To Election Security."

395 Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

396 Fla. Stat. § 101.591.

397 Fla. Stat. § 101.591.

398 Fla. Stat. § 101.591.

399 Fla. Stat. § 101.591.

400 Fla. Stat. § 101.591.

401 Fla. Stat. § 101.591.

402 Fla. Stat. § 101.591.

403 Fla. Stat. § 101.591.

404 Fla. Stat. § 101.591.

405 Verified Voting, "State Audit Laws – Florida," March 2017, available at https://www.verifiedvoting.org/state-audit-laws/florida/.

406 Smith and others, "Counting Votes 2012."

407 Smith and others, "Counting Votes 2012."

408 Smith and others, "Counting Votes 2012."

409 Smith and others, "Counting Votes 2012."

410 Smith and others, "Counting Votes 2012."

411 National Conference of State Legislatures, "Electronic Transmission of Ballots."

412 Fla. Stat. § 101.015 (2016), available at http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0100-0199/0101/Sections/0101.015.html; U.S. Election Assistance Commission, "State Requirements and the Federal Voting System Testing and Certification Program."

413 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

414 Fla. Stat. § 101.5612 (2016), available at http://www.leg.state.fl.us/statutes/index.cfm?App_Mode=Display_Statute&Search_String=&URL=Ch0101/Sec5612.htm&StatuteYear=2006.

415 Fla. Stat. § 101.5612.

416 Fla. Stat. § 101.5612; Bagga, Losco, and Scheele, "Pre-Election Logic and Accuracy Testing and Post-Election Audit Initiative."

417 Personal correspondence from Chris Harvey, Elections Director, October 31, 2017.

418 Personal correspondence from Chris Harvey, October 31, 2017.

419 Personal correspondence from Chris Harvey, October 31, 2017.

420 Personal correspondence from Chris Harvey, October 31, 2017.

421 Personal correspondence from Chris Harvey, October 31, 2017.

422 Eric Geller, "Elections Security: Federal Help or Power Grab?", *Politico*, August 28, 2016, available at http://www.politico.com/story/2016/08/election-cyber-security-georgia-227475.

423 Butchireddygari, "Many County Election Officials Still Lack Cybersecurity Training."

424 Ga. Admin. Law § 183-1-12-.07, available at http://rules.sos.state.ga.us/gac/183-1-12.

425 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

426 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books.".

427 Personal correspondence from Chris Harvey, October 31, 2017.

428 Personal correspondence from Chris Harvey, October 31, 2017.

429 Verified Voting, "The Verifier—Polling Place Equipment—November 2016"; Ga. Admin. Law § 183-1-12-.02, available at http://rules.sos.state.ga.us/gac/183-1-12.

430 H.B 680, available at http://www.legis.ga.gov/Legislation/20172018/171077.pdf (last accessed January 2018).; Georgia General Assembly, "2017-2018 Regular Session - HB 680, Elections; direct recording electronic voting systems shall not be used in primaries or elections in this state after January 1, 2019; provisions," available athttp://www.legis.ga.gov/Legislation/en-US/display/20172018/HB/680 (last accessed January 2018); Georgians for Verified Voting, "Paper Ballot Legislation to Replace Georgia Paperless DRE Voting System," YouTube, November 6, 2017, available at https://www.youtube.com/watch?v=j7LAOCUd-dI&feature=youtu.be.

431 Johnny Kauffman, "Paper Ballot Push Gets Boost With Support Of Georgia Lt. Governor," WABE, January 24, 2018, available at https://www.wabe.org/georgia-lt-governor-joins-calls-rapid-switch-paper-ballot-voting-system/.

432 Ga. Code § 21-2-379.11 (2016), available at http://law.justia.com/codes/georgia/2016/title-21/chapter-2/article-9/part-5/section-21-2-379.11/; Smith and others, "Counting Votes 2012."

433 Ga. Code § 21-2-379.11; Ga. Admin. Law § 183-1-12-.02, available at http://rules.sos.state.ga.us/gac/183-1-12; Smith and others, "Counting Votes 2012."

434 Personal correspondence from Chris Harvey, October 31, 2017.

435 Smith and others, "Counting Votes 2012."

436 Personal correspondence from Chris Harvey, October 31, 2017.

437 Personal correspondence from Chris Harvey, October 31, 2017. Ga. Code § 21-2-379 (2016), available at https://law.justia.com/codes/georgia/2016/title-21/chapter-2/article-9/part-4/section-21-2-379/; Ga. Code § 21-2-440 (2016), available at http://law.justia.com/codes/georgia/2016/title-21/chapter-2/article-11/part-2/section-21-2-440/; Ga. Admin. Law § 183-1-12-.02 5(a)(6), available at http://rules.sos.state.ga.us/gac/183-1-12.

438 National Conference of State Legislatures, "Electronic Transmission of Ballots."

439 Ga. Admin. Law § 590-8-1-.01, available at http://rules.sos.ga.gov/gac/590-8-1-.01%20; U.S. Election Assistance Commission, "State Requirements and the Federal Voting System Testing and Certification Program."

440 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

441 GA Admin. Law § 183-1-12-.02(3)(b), available at http://rules.sos.ga.gov/gac/183-1-12-.02.

442 GA Admin. Law § 183-1-12-.02(3)(b).

443 GA Admin. Law § 183-1-12-.02(3)(b).

444 Personal correspondence from Aulii Tenn, Statewide Counting Center Manager, October 30, 2017.

445 According to state best practices for government database protection and maintenance. State of Hawaii, Information Privacy and Security Council, "Breach Best Practices," August 28, 2009, available at http://ipsc.hawaii.gov/wp-content/uploads/2013/10/IPSC-Breach-Best-Practices.pdf.

446 Scott Nago, Chief Election Officer, and Aulii Tenn, Statewide Counting Center Manager, interview with author, September 18, 2017.

447 Personal correspondence from Aulii Tenn, October 30, 2017.

448 Verified Voting, "The Verifier—Polling Place Equipment—November 2016"; Hawaii Rev. Stat. § 16-21 (2016), available at http://law.justia.com/codes/hawaii/2016/title-2/chapter-16/section-16-21/; Hawaii Rev. Stat. § 16-41 (2016), available at http://law.justia.com/codes/hawaii/2016/title-2/chapter-16/section-16-41/; Hawaii Rev. Stat. § 16-42 (2016), available at http://law.justia.com/codes/hawaii/2016/title-2/chapter-16/section-16-42/.

449 Hawaii Rev. Stat. § 16-42; Hawaii Admin. Law § 3-172-102, available at http://elections.hawaii.gov/wp-content/uploads/2015/03/HAR-Office-of-Elections.pdf.

450 Verified Voting, "State Audit Laws – Hawaii," March 2017, available at https://www.verifiedvoting.org/state-audit-laws/hawaii/.

451 Hawaii Rev. Stat. § 16-42; Scott Nago and Aulii Tenn, interview with author, September 18, 2017.

452 Ibid.

453 Scott Nago and Aulii Tenn, interview with author, September 18, 2017.

454 Hawaii Rev. Stat. § 16-42; Hawaii Admin. Law § 3-172-102.

455 Scott Nago and Aulii Tenn, interview with author, September 18, 2017.

456 Hawaii Rev. Stat. § 16-42; Hawaii Admin. Law § 3-172-102.

457 Personal correspondence from Aulii Tenn, September 21, 2017.

458 Hawaii Rev. Stat. § 11-154 (2016), available at http://law.justia.com/codes/hawaii/2016/title-2/chapter-11/section-11-154/; Hawaii Rev. Stat. § 11-152 (2016), available at http://law.justia.com/codes/hawaii/2016/title-2/chapter-11/section-11-152/; Smith and others, "Counting Votes 2012."

459 Smith and others, "Counting Votes 2012."

460 Smith and others, "Counting Votes 2012."

461 Smith and others, "Counting Votes 2012."

462 Hawaii Rev. Stat. § 11-153 (2016), available at http://law.justia.com/codes/hawaii/2016/title-2/chapter-11/section-11-153/; Hawaii Rev. Stat. § 11-155 (2016), available at http://law.justia.com/codes/hawaii/2016/title-2/chapter-11/section-11-155/; Smith and others, "Counting Votes 2012."

463 Hawaii House Bill 1654 (2016), available at http://www.capitol.hawaii.gov/session2016/bills/HB1654_SD2_.htm; National Conference of State Legislatures, "Electronic Transmission of Ballots."

464 Scott Nago and Aulii Tenn, interview with author, September 18, 2017.

465 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

466 Hawaii Rev. Stat. § 16-42; Scott Nago and Aulii Tenn, interview with author, September 18, 2017.

467 Scott Nago and Aulii Tenn, interview with author, September 18, 2017.

468 Personal correspondence from Aulii Tenn, September 21, 2017.

469 Scott Nago and Aulii Tenn, interview with author, September 18, 2017.

470 Norden and Vandewalker, "Securing Elections From Foreign Interference."

471 Survey response from Tim Hurst, Chief Deputy Secretary of State.

472 Survey response from Tim Hurst, Chief Deputy Secretary of State.

473 Idaho Technology Authority, "Enterprise Policy"; State of Idaho, Office of the Governor, Executive Order no. 2017-02, 2017, available at https://adminrules.idaho.gov/rules/current/ExOs/2017-02_ExOr_17-2.pdf; Center for Internet Security, "CIS Controls," available at https://www.cisecurity.org/controls/ (last accessed September 2017); Center for Internet Security, "Critical Security Controls for Effective Cyber Defense: Version 6.0" (2015), available at https://cybersecurity.idaho.gov/wp-content/uploads/sites/23/2016/10/CSCmaster.pdf; National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," February 12, 2014, available athttps://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

474 State of Idaho, Office of the Governor, Executive Order No. 2017-02; National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity"; Center for Internet Security, "CIS Controls"; Center for Internet Security, "Critical Security Controls for Effective Cyber Defense"; The Nelson A. Rockefeller Center at Dartmouth College, "Data Security in New Hampshire: Identifying Targets, Vulnerabilities, and Best Practices" (2017), available at https://rockefeller.dartmouth.edu/sites/rockefeller.drupalmulti-prod.dartmouth.edu/files/prs_data_security_final_1617-12_july_11_2017.pdf.

475 Survey response from Tim Hurst.

476 Survey response from Tim Hurst.

477 Survey response from Tim Hurst; Idaho Code § 34-1106A (2016), available at http://law.justia.com/codes/idaho/2016/title-34/chapter-11/section-34-1106a/; The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

478 Survey response from Tim Hurst; Idaho Code § 34-1106A.

479 Survey response from Tim Hurst.

480 Survey response from Tim Hurst.

481 Idaho Code § 34-1202 (2016), available at https://legislature.idaho.gov/statutesrules/idstat/Title34/T34CH12/SECT34-1202/; Idaho Code § 34-1008 (2016), available at https://legislature.idaho.gov/statutesrules/idstat/Title34/T34CH10/SECT34-1008/; Idaho Code § 34-1201 (2016), available at https://legislature.idaho.gov/statutesrules/idstat/Title34/T34CH12/SECT34-1201/; Idaho Code § 34-1007 (2016), available at https://legislature.idaho.gov/statutesrules/idstat/Title34/T34CH10/SECT34-1007/; Idaho Code § 34-1203 (2016), available at https://legislature.idaho.gov/statutesrules/idstat/Title34/T34CH12/SECT34-1203/; Idaho Code § 34-1204 (2016), available at https://legislature.idaho.gov/statutesrules/idstat/Title34/T34CH12/SECT34-1204/; Smith and others, "Counting Votes 2012."

482 Idaho Code § 34-1202; Smith and others, "Counting Votes 2012."

483 This requirement is made by the Idaho secretary of state. Smith and others, "Counting Votes 2012."

484 Smith and others, "Counting Votes 2012."

485 Idaho Code § 34-1203; Smith and others, "Counting Votes 2012."

486 Specifically, citizens directly affected by "a national or local emergency". Survey response from Tim Hurst; National Conference of State Legislatures, "Electronic Transmission of Ballots."

487 Survey response from Tim Hurst; Idaho Code § 34-2409.

488 According to Verified Voting, as of 2016, some jurisdictions in Idaho were still using 10-year old devices, like the AutoMark voting machine. Verified Voting, "The Verifier—Polling Place Equipment— November 2016"; Associated Press, "Idaho county will use new voting machines in November," KSL, April 1, 2016, available at https://www.ksl.com/?sid=39135493.

489 Idaho Code § 34-2416 (2016), available at https://legislature.idaho.gov/statutesrules/idstat/Title34/T34CH24/SECT34-2416/.

490 Idaho Code § 34-2416; Survey response from Tim Hurst.

491 Survey response from Tim Hurst.

492 Norden and Vandewalker, "Securing Elections From Foreign Interference."

493 Kyle Thomas, Director, Voting and Registration Systems, Illinois State Board of Elections, and Kevin Turner, Director of the Division of Information Technology, interview with author, September 11, 2017.

494 Kyle Thomas and Kevin Turner, interview with author, October 12, 2017.

495 Kyle Thomas and Kevin Turner, interview with author, October 12, 2017.

496 Kyle Thomas and Kevin Turner, interview with author, October 12, 2017.

497 Kyle Thomas and Kevin Turner, interview with author, October 12, 2017.

498 Rick Pearson, "Illinois Election Officials Say Hack Yielded Information on 200,000 Voters," *Chicago Tribune*, August 29, 2016, available at http://www.chicagotribune.com/news/local/politics/ct-illinois-state-board-of-elections-hack-update-met-0830-20160829-story.html.

499 Kyle Thomas and Kevin Turner, interview with author, September 11, 2017.

500 Kyle Thomas and Kevin Turner, interview with author, September 11, 2017.

501 An estimated 25 percent of Illinois election jurisdictions use electronic poll books to check-in eligible voters during early voting and on Election Day, representing about 50 percent of the state's total eligible voting population. Kyle Thomas and Kevin Turner, interview with author, September 11, 2017; The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

502 Kyle Thomas and Kevin Turner, interview with author, September 11, 2017; The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

503 Kyle Thomas and Kevin Turner, interview with author, September 11, 2017; The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

504 Personal correspondence from Kyle Thomas, October 31, 2017.

505 Bennett and others, "Cash-strapped states brace for Russian hacking fight".

506 10 Ill. Stat. § 5/24C-1, available at http://ilga.gov/legislation/ilcs/documents/001000050K24C-1.htm; Verified Voting, "The Verifier—Polling Place Equipment— November 2016."

507 Noah Praetz, "2020 Vision: Election Security in the Age of Committee Foreign Threats" (Cook County Clerk David Orr; Chicago, December 2017), available at https://www.defcon.org/images/defcon-25/Election%20Security%20White%20Paper_Praetz_12062017.pdf.

508 Verified Voting, "State Audit Laws – Illinois," March 2017, available at https://www.verifiedvoting.org/state-audit-laws/illinois/.

509 10 Ill. Stat. § 5/24A-15, available at http://codes.findlaw.com/il/chapter-10-elections/il-st-sect-10-5-24a-15.html; 10 Ill. Stat. § 5/24C-15, available at http://www.ilga.gov/legislation/ilcs/fulltext.asp?DocName=001000050K24C-15.

510 10 Ill. Stat. §§ 5/24A-15, 5/24C-15.

511 Kyle Thomas and Kevin Turner, interview with author, September 11, 2017.

512 Kyle Thomas and Kevin Turner, interview with author, September 11, 2017; 10 Ill. Stat. § 5/24A-15.

513 Kyle Thomas and Kevin Turner, interview with author, September 11, 2017; 10 Ill. Stat. § 5/24C-15.

514 Kyle Thomas and Kevin Turner, interview with author, September 11, 2017.

515 Kyle Thomas and Kevin Turner, interview with author, September 11, 2017.

516 Kyle Thomas and Kevin Turner, interview with author, September 11, 2017; 10 Ill. Stat. § 5/22-9.1, available at http://law.onecle.com/illinois/10ilcs5/22-9.1.html.

517 10 Ill. Stat. § 5/17-18, available at http://www.ilga.gov/legislation/ilcs/ilcs4.asp?DocName=001000050HArt%2E+17&ActID=170&ChapterID=3&SeqStart=59600000&SeqEnd=63500000; 10 Ill. Stat. § 5/17-16, available at http://www.ilga.gov/legislation/ilcs/ilcs4.asp?DocName=001000050HArt%2E+17&ActID=170&ChapterID=3&SeqStart=59600000&SeqEnd=63500000; 10 Ill. Stat. § 5/24B-10, available at http://www.ilga.gov/legislation/ilcs/ilcs4.asp?DocName=001000050HArt%2E+24B&ActID=170&ChapterID=3&SeqStart=85700000&SeqEnd=88600000; 10 Ill. Stat. § 5/24B-10.1, available at http://www.ilga.gov/legislation/ilcs/ilcs4.asp?DocName=001000050HArt%2E+24B&ActID=170&ChapterID=3&SeqStart=85700000&SeqEnd=88600000; 10 Ill. Stat. § 5/24B-15, available at http://www.ilga.gov/legislation/ilcs/ilcs4.asp?DocName=001000050HArt%2E+24B&ActID=170&ChapterID=3&SeqStart=85700000&SeqEnd=88600000; 10 Ill. Stat. § 5/24C-12, available at http://www.ilga.gov/legislation/ilcs/ilcs4.asp?DocName=001000050HArt%2E+24C&ActID=170&ChapterID=3&SeqStart=88600000&SeqEnd=91300000; 10 Ill. Stat. § 5/24C-15; Smith and others, "Counting Votes 2012."

518 10 Ill. Stat. § 5/17-18; Smith and others, "Counting Votes 2012."

519 Personal correspondence from Kyle Thomas, October 31, 2017; 10 Ill. Stat. §§ 5/17-18, 5/24B-10; Smith and others, "Counting Votes 2012."

520 Smith and others, "Counting Votes 2012."

521 Smith and others, "Counting Votes 2012."

522 10 Ill. Stat. §§ 5/24B-10.1, 5/24C-12; 10 Ill. Stat. § 5/17-20, available at http://www.ilga.gov/legislation/ilcs/ilcs4.asp?DocName=001000050HArt%2E+17&ActID=170&ChapterID=3&SeqStart=59600000&SeqEnd=63500000; Smith and others, "Counting Votes 2012."

523 Kyle Thomas and Kevin Turner, interview with author, September 11, 2017; National Conference of State Legislatures, "Electronic Transmission of Ballots."

524 10 Ill. Stat. § 5/24C-16, available at http://www.ilga.gov/legislation/ilcs/documents/001000050K24C-16.htm; Kyle Thomas and Kevin Turner, interview with author, September 11, 2017.

525 New voting machines are purchased at the county level; some jurisdictions purchased new voting machines as recently as last year. Kyle Thomas and Kevin Turner, interview with author, September 11, 2017; Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

526 10 Ill. Stat. § 5/24C-9, available at http://www.ilga.gov/legislation/ilcs/fulltext.asp?DocName=001000050K24C-9; 10 Ill. Stat. § 5/24A-9, available at http://www.ilga.gov/legislation/ilcs/documents/001000050K24A-9.htm.

527 10 Ill. Stat. §§ 5/24C-9, 5/24A-9.

528 10 Ill. Stat. §§ 5/24C-9, 5/24A-9.

529 Kyle Thomas and Kevin Turner, interview with author, September 11, 2017.

530 Personal correspondence from Valerie Warycha, Deputy Chief of Staff and Communications Director for the Indiana Secretary of State, October 31, 2017.

531 Norden and Vandewalker, "Securing Elections From Foreign Interference."

532 Enterprise Information Technology, "Indiana Election Division Statewide Voter Registration System: Security Policy Guideline," available at https://www.in.gov/sos/elections/files/43attl.pdf (last accessed September 2017).

533 Enterprise Information Technology, "Indiana Election Division Statewide Voter Registration System"; Mark Anderson, "Voter Registration Websites for 35 States Are Vulnerable to Voter ID Theft," IEEE Spectrum, September 14, 2017, available at https://spectrum.ieee.org/tech-talk/telecom/security/new-report-suggests-its-surprisingly-easy-to-tamper-with-online-voter-registration-rolls.

534 Enterprise Information Technology, "Indiana Election Division Statewide Voter Registration System."

535 Enterprise Information Technology, "Indiana Election Division Statewide Voter Registration System."

536 Personal correspondence from Angie Nussmeyer, Co-Director, Indiana Election Division November 13, 2017.

537 Personal correspondence from Angie Nussmeyer, November 13, 2017.

538 Ind. Code § 3-11-18.1-12 (2016), available at http://codes.findlaw.com/in/title-3-elections/in-code-sect-3-11-18-1-12.html; Ind. Code § 3-11-8-10.3, available at http://codes.findlaw.com/in/title-3-elections/in-code-sect-3-11-8-10-3.html; The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

539 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

540 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

541 Personal correspondence from Angie Nussmeyer, October 31, 2017.

542 Personal correspondence from Angie Nussmeyer, November 13, 2017.

543 Personal correspondence from Angie Nussmeyer, November 13, 2017.

544 Bennett and others, "Cash-strapped states brace for Russian hacking fight."

545 Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

546 IN H 1269, available at https://custom.statenet.com/public/resources.cgi?id=ID:bill:IN2018000H1269&ciq=ncsl15&client_md=2246cb37aaca3e6a446d2719e58c6b13&mode=current_text (last accessed January 2018).

547 Ind. Code § 3-11-13-38, available at http://iga.in.gov/legislative/laws/2017/ic/titles/003#3-11-13-38.

548 Ind. Code § 3-11-13-38.

549 Ind. Code § 3-11-13-38.

550 Ind. Code § 3-12-3.5-8, available at http://codes.findlaw.com/in/title-3-elections/in-code-sect-3-12-3-5-8.html.

551 Ind. Code § 3-12-3.5-8.

552 Personal correspondence from Valerie Warycha, , October 31, 2017.

553 Personal correspondence from Valerie Warycha, October 31, 2017.

554 Smith and others, "Counting Votes 2012."

555 Smith and others, "Counting Votes 2012."

556 Smith and others, "Counting Votes 2012."

557 Smith and others, "Counting Votes 2012."

558 Ind. Code § 3-12-4-21, available at http://codes.findlaw.com/in/title-3-elections/in-code-sect-3-12-4-21.html; personal correspondence from Angie Nussmeyer, November 13, 2017.

559 Personal correspondence from Angie Nussmeyer, November 13, 2017.

560 Smith and others, "Counting Votes 2012."

561 National Conference of State Legislatures, "Electronic Transmission of Ballots"; Ind. Code §§ 3-11-4-5.7, 3-11-10-26.

562 Ind. Code § 3-11-15-13.3, available at http://codes.findlaw.com/in/title-3-elections/in-code-sect-3-11-15-13-3.html.

563 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

564 Personal correspondence from Valerie Warycha, October 31, 2017.

565 Ind. Code § 3-11-14.5-1, available at http://codes.findlaw.com/in/title-3-elections/in-code-sect-3-11-14-5-1.html; Bagga, Losco, and Scheele, "Pre-Election Logic and Accuracy Testing and Post-Election Audit Initiative."

566 Ind. Code § 3-11-13-22, available at http://codes.findlaw.com/in/title-3-elections/in-code-sect-3-11-13-22.html; Personal correspondence from Angie Nussmeyer, November 13, 2017.

567 Ind. Code § 3-11-13-22.

568 Ind. Code § 3-11-13-22; personal correspondence from Valerie Warycha, October 31, 2017.

569 Norden and Vandewalker, "Securing Elections From Foreign Interference."

570 Office of the Chief Information Officer, Information Security Office, "ISO Catalogue of Services," available at https://secureonline.iowa.gov/about-iso/2016-03-10/iso-catalog-services (last accessed September 2017).

571 See generally, State of Iowa, "Cyber Security Strategy" (2016), available at https://ocio.iowa.gov/sites/default/files/documents/2016/08/2016_cybersec_document_web_version_2_final_0.pdf; Office of the Chief Information Officer, Information Security Office, "ISO Catalogue of Services."

572 Iowa Code § 49.77.1, available at https://www.legis.iowa.gov/docs/code/2017/49.pdf; The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

573 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

574 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

575 Iowa Code § 52.2, available at https://www.legis.iowa.gov/docs/code/2017/52.pdf; Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

576 Iowa House File 516 (2017), available at https://www.legis.iowa.gov/docs/publications/LGE/87/HF516.pdf; Brianne Pfannenstiel, "Iowa House Approves Voter ID Bill Following 12 Hours of Debate," *Des Moise Registrar*, March 9, 2017, available at http://www.desmoinesregister.com/story/news/politics/2017/03/09/iowa-house-approves-voter-id-bill-following-12-hours-debate/98950160/.

577 Iowa House File 516.

578 Iowa House File 516.

579 Smith and others, "Counting Votes 2012."

580 Smith and others, "Counting Votes 2012."

581 Smith and others, "Counting Votes 2012."

582 Smith and others, "Counting Votes 2012."

583 Smith and others, "Counting Votes 2012."

584 Specifically, those located in an area designated as "imminent danger pay area" by the U.S. Department of Defense. Iowa Secretary of State, "Other Available Absentee Voting Alternatives," available at https://sos.iowa.gov/elections/voterinformation/uocava/alternatives.html (last accessed September 2017).

585 Iowa Code § 721-22.2(52), available at https://www.legis.iowa.gov/docs/iac/rule/10-05-2011.721.22.2.pdf.

586 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

587 Iowa Code § 52.35, available at https://www.legis.iowa.gov/docs/code/2016/52.35.pdf.

588 Iowa Code § 52.35.

589 Iowa Code § 52.35.

590 Norden and Vandewalker, "Securing Elections From Foreign Interference."

591 See generally, Kansas Office of the Governor, Office of Information Technology Services, "Information Security Policies, Procedures and Baselines," Policy memorandum, December 1, 2014, available at http://oits.ks.gov/docs/default-source/policydocument-slibrary/p9209-oits-information-security-policy.pdf?sfvrsn=2.

592 Stephen Koranda, "Kobach Confident in Security of Kansas Voter Registration Data," KMUW, September 6, 2016, available at http://kmuw.org/post/kobach-confident-security-kansas-voter-registration-data.

593 Kansas Office of the Governor, Office of Information Technology Services, "Information Security Policies, Procedures and Baselines."

594 Kansas Office of the Governor, Office of Information Technology Services, "Information Security Policies, Procedures and Baselines."

595 Bryan Lowry, "Kansas Partners With Federal Agencies to Keep Voter Data Secure," *Wichita Eagle*, August 30, 2016, available at http://www.kansas.com/news/politics-government/election/article98851622.html.

596 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

597 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

598 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

599 Kan. Stat § 25-4401 (2016), available at http://law.justia.com/codes/kansas/2016/chapter-25/article-44/section-25-4401; Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

600 Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

601 National Conference of State Legislatures, "Post-Election Audits."

602 KS H 2251, available at https://custom.statenet.com/public/resources.cgi?id=ID:bill:KS2017000H2251&ciq=ncsl15&client_md=0e071691ede443d4d88b512d6e52f7ca&mode=current_text (last accessed January 2018).

603 Smith and others, "Counting Votes 2012."

604 Smith and others, "Counting Votes 2012."

605 Smith and others, "Counting Votes 2012."

606 Smith and others, "Counting Votes 2012."

607 Smith and others, "Counting Votes 2012."

608 National Conference of State Legislatures, ", "Electronic transmission of ballots.."

609 Kan. Stat. § 25-4406, available at http://www.ksrevisor.org/statutes/chapters/ch25/025_044_0006.html; Office of the Secretary of State, "Election Standards—Chapter VI: Voting Systems" (Revised 2014), available at http://www.kssos.org/elections/elections_reform_standards.html.

610 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

611 Kan. Stat. § 25-4411, available at http://law.justia.com/codes/kansas/2016/chapter-25/article-44/section-25-4411; Office of the Secretary of State, "Election Standards—Chapter II: Election Administration.".

612 Kan. Stat. § 25-4411; Office of the Secretary of State, "Election Standards—Chapter II."

613 Kan. Stat. § 25-4411; Office of the Secretary of State, "Election Standards—Chapter II."

614 Norden and Vandewalker, "Securing Elections From Foreign Interference."

615 Lindsay Hughes Thurston, Assistant Secretary of State, and Bradford Queen, Director of Communications, interview with author, October 5, 2017.

616 Lindsay Hughes Thurston and Bradford Queen, interview with author, October 5, 2017.

617 Lindsay Hughes Thurston and Bradford Queen, interview with author, October 5, 2017; "Kentucky Information Technology Standards (KITS)," available at https://cgp.ky.gov/sites/COTPUBDOCS/Standards/KITS_Report.pdf (last accessed September 2017).

618 "Kentucky Information Technology Standards (KITS)."

619 Personal correspondence from Bradford Queen, October 31, 2017.

620 Personal correspondence from Bradford Queen, October 31, 2017.

621 Lindsay Hughes Thurston and Bradford Queen, interview with author, October 5, 2017; Brennan Center for Justice, "VRM in the States: Electronic Poll Books," February 6, 2017, available at https://www.brennancenter.org/analysis/vrm-states-electronic-poll-books; National Conference of State Legislatures, "Electronic Poll Books."

622 Personal correspondence from Bradford Queen, October 31, 2017.

623 Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

624 Ky. Rev. Stat. § 117.383, available at http://www.lrc.ky.gov/statutes/statute.aspx?id=27447; Ky. Rev. Stat. § 15.243(3), available at http://codes.findlaw.com/ky/title-iii-executive-branch/ky-rev-st-sect-15-243.html; Ky. Rev. Stat. § 117.275(9), available at http://www.lrc.ky.gov/Statutes/statute.aspx?id=27418; Ky. Rev. Stat § 117.305(1), available at http://www.lrc.ky.gov/statutes/statute.aspx?id=27424; personal correspondence from Bradford Queen, October 31, 2017.

625 Verified Voting, "State Audit Laws – Kentucky," March 2017, available at https://www.verifiedvoting.org/state-audit-laws/kentucky/.

626 Ky. Rev. Stat. § 117.383(8), available at http://www.lrc.ky.gov/statutes/statute.aspx?id=27447.

627 Ky. Rev. Stat. § 15.243(3).

628 Ky. Rev. Stat. § 117.383.

629 Ky. Rev. Stat. §§ 117.275(9), 117.305(1).

630 Ky. Rev. Stat. § 117.383.

631 Ky. Rev. Stat. §§ 117.383(8), 117.305(1); Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

632 Smith and others, "Counting Votes 2012."

633 Smith and others, "Counting Votes 2012."

634 Smith and others, "Counting Votes 2012."

635 Smith and others, "Counting Votes 2012."

636 Smith and others, "Counting Votes 2012."

637 National Conference of State Legislatures, "Post-Election Audits."

638 Ky. Rev. Stat. § 117.381, available at http://www.lrc.ky.gov/statutes/statute.aspx?id=27446; Ky. Rev. Stat. § 117.379, available at http://codes.findlaw.com/ky/title-x-elections/ky-rev-st-sect-117-379.html.

639 Lindsay Hughes Thurston and Bradford Queen, interview with author, October 5, 2017.

640 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

641 Lindsay Hughes Thurston and Bradford Queen, interview with author, October 5, 2017.

642 Lindsay Hughes Thurston and Bradford Queen, interview with author, October 5, 2017.

643 Ky. Admin. Reg. § 2:020, available at http://www.lrc.state.ky.us/kar/031/002/020.htm.

644 Bagga, Losco, and Scheele, "Pre-Election Logic and Accuracy Testing and Post-Election Audit Initiative."

645 Ky. Rev. Stat. § 117.389, available at http://www.lrc.ky.gov/Statutes/statute.aspx?id=27450.

646 Ky. Rev. Stat. § 117.165; personal correspondence from Bradford Queen, October 31, 2017.

647 Norden and Vandewalker, "Securing Elections From Foreign Interference."

648 Personal correspondence from Meg Casper Sunstrom, Press Secretary for Louisiana Secretary of State Tom Schedler, October 27, 2017.

649 Personal correspondence from Meg Casper Sunstrom, October 27, 2017.

650 Personal correspondence from Meg Casper Sunstrom, October 27, 2017; Anderson, "Voter Registration Websites for 35 States Are Vulnerable to Voter ID Theft"; Sweeney, Yoo, and Zang, "Voter Identity Theft."

651 Personal correspondence from Meg Casper Sunstrom, October 27, 2017.

652 Personal correspondence from Meg Casper Sunstrom, October 27, 2017.

653 Personal correspondence from Meg Casper Sunstrom, October 27, 2017.

654 Personal correspondence from Meg Casper Sunstrom, January 26, 2018.

655 Personal correspondence from Meg Casper Sunstrom, October 27, 2017; Butchireddygari, "Many County Election Officials Still Lack Cybersecurity Training."

656 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

657 Personal correspondence from Meg Casper Sunstrom, October 27, 2017.

658 Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

659 Personal correspondence from Meg Casper Sunstrom, October 27, 2017.

660 Personal correspondence from Meg Casper Sunstrom, October 27, 2017.

661 From a personal correspondence from Meg Casper Sunstrom: "While Louisiana law does not currently require post-election audits, the Secretary of State does (through processes/procedures) perform post-election audits using printed machine tapes, electronic machines counts and voter signatures on precinct registers to verify the accuracy of all results before final promulgation.Additionally, Louisiana tests and seals every voting machine in a public meeting before AND after every election in order to demonstrate that every machine is performing properly before votes are cast and after an election has been completed.These processes and procedures provide a trusted audit of voting machine activity that has been submitted as evidence in courts of laws to overcome challenges of Louisiana's machine results.To date, Louisiana's machine results have never been overturned by a court of law." National Conference of State Legislatures, "Post-Election Audits"; Verified Voting, "State Audit Laws – Louisiana," available at https://www.verifiedvoting.org/state-audit-laws/louisiana/ (last accessed September 2017).

662 Smith and others, "Counting Votes 2012."

663 Personal correspondence from Meg Casper Sunstrom, October 27, 2017.

664 Personal correspondence from Meg Casper Sunstrom, October 27, 2017.

665 Personal correspondence from Meg Casper Sunstrom, October 27, 2017.

666 Smith and others, "Counting Votes 2012."

667 Personal correspondence from Meg Casper Sunstrom, October 27, 2017.

668 Personal correspondence from Meg Casper Sunstrom, October 27, 2017; Smith and others, "Counting Votes 2012."

669 National Conference of State Legislatures, "Electronic Transmission of Ballots."

670 La. Rev. Stat. § 18-1361 (2016), available at http://legis.la.gov/legis/Law.aspx?d=81377.

671 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

672 Personal correspondence from Meg Casper Sunstrom, October 27, 2017.

673 La. Rev. Stat. § 18-1373 (2016), available at http://law.justia.com/codes/louisiana/2011/rs/title18/rs18-1373/; Bagga, Losco, and Scheele, "Pre-Election Logic and Accuracy Testing and Post-Election Audit Initiative."

674 La. Rev. Stat. § 18-1373.

675 La. Rev. Stat. § 18-1373.

676 Norden and Vandewalker, "Securing Elections From Foreign Interference.".

677 Survey response from Julie Flynn, Deputy Secretary of State.

678 Personal correspondence from Julie Flynn, October 31, 2017.

679 Survey response from Julie Flynn.

680 Survey response from Julie Flynn.

681 Personal correspondence from Julie Flynn, January 29, 2018.

682 Survey response from Julie Flynn.

683 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books";Survey response from Julie Flynn.

684 Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

685 National Conference of State Legislatures, "Post-Election Audits"; survey response from Julie Flynn.

686 Smith and others, "Counting Votes 2012."

687 Personal correspondence from Julie Flynn, October 31, 2017.

688 Smith and others, "Counting Votes 2012."

689 Julie Flynn, Deputy Secretary of State, interview with author, October 30, 2017.

690 Smith and others, "Counting Votes 2012."

691 Julie Flynn, Deputy Secretary of State, interview with author, October 30, 2017.

692 21-A Maine Rev. Stat. § 809-A (2016), available at http://law.justia.com/codes/maine/2016/title-21-a/chapter-9/subchapter-6/section-809-a/; National Conference of State Legislatures, "Electronic Transmission of Ballots."

693 21-A Maine Rev. Stat. § 809 (2016), available at http://legislature.maine.gov/statutes/21-A/title21-Asec809.html; U.S. Election Assistance Commission, "State Requirements and the Federal Voting System Testing and Certification Program."

694 Survey response from Julie Flynn.

695 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

696 21-A Maine Rev. Stat. § 817-A (2016), available at http://law.justia.com/codes/maine/2016/title-21-a/chapter-9/subchapter-6/article-5-1/section-817-a/; 21-A Maine Rev. Stat. § 854 (2016), available at http://law.justia.com/codes/maine/2016/title-21-a/chapter-9/subchapter-6/article-5-2/section-854/.

697 21-A Maine Rev. Stat. § 854.

698 Survey response from Julie Flynn.

699 Norden and Vandewalker, "Securing Elections From Foreign Interference."

700 Personal correspondence from Nikki Charlson, Deputy State Administrator, October 27, 2017.

701 Personal correspondence from Nikki Charlson, October 27, 2017.

702 Personal correspondence from Linda H. Lamone, Administrator of Elections, September 27, 2017; State of Maryland, "Maryland's Voter Registration Systems – Security Features and Practices," available at http://www.elections.maryland.gov/press_room/Voter%20Registration%20Security%20Talking%20Points.pdf (last accessed September 2017).

703 Personal correspondence from Linda H. Lamone, September 27, 2017; State of Maryland, "Maryland's Voter Registration Systems – Security Features and Practices."

704 Personal correspondence from Linda H. Lamone, September 27, 2017.

705 Personal correspondence from Linda H. Lamone, September 27, 2017; State of Maryland, "Maryland's Voter Registration Systems – Security Features and Practices."

706 Personal correspondence from Nikki Charlson, November 7, 2017.

707 Linda H. Lamone and Nikki Charlson, interview with author, September 15, 2017; "Maryland's Voter Registration Systems – Security Features and Practices."

708 Linda H. Lamone and Nikki Charlson, interview with author, September 15, 2017.

709 Md. Code § 33.17.04.03, available at http://mdrules.elaws.us/comar/33.17.04.03; The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

710 Linda H. Lamone and Nikki Charlson, interview with author, September 15, 2017.

711 Linda H. Lamone and Nikki Charlson, interview with author, September 15, 2017.

712 Md. Elec. Code § 9-201 (2016), available at http://law.justia.com/codes/maryland/2016/election-law/title-9/subtitle-2/section-9-201/; Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

713 Md. Code § 33.08.05.04, available at http://mdrules.elaws.us/comar/33.08.05.04; Maryland State Board of Elections, "Re: State Board of Elections—Joint Chairman's Report on the 2016 Post-Election Tabulation Audit," December 22, 2016, available at http://www.elections.state.md.us/press_room/documents/PostElectionTabulationAuditLegislativeReport.pdf.

714 Maryland State Board of Elections, "Re: State Board of Elections."

715 Md. Code § 33.08.05.04.

716 Linda H. Lamone and Nikki Charlson, interview with author, September 15, 2017; Maryland State Board of Elections, "Re: State Board of Elections."

717 Md. Code § 33.08.05.04.

718 Linda H. Lamone and Nikki Charlson, interview with author, September 15, 2017.

719 Linda H. Lamone and Nikki Charlson, interview with author, September 15, 2017.

720 Linda H. Lamone and Nikki Charlson, interview with author, September 15, 2017.

721 Personal correspondence from Linda H. Lamone, September 27, 2017.

722 Md. Code § 33.08.05.03, available at http://mdrules.elaws.us/comar/33.08.05.03.

723 Personal correspondence from Linda H. Lamone, September 27, 2017.

724 Smith and others, "Counting Votes 2012."

725 Personal correspondence from Nikki Charlson, October 27, 2017.

726 Personal correspondence from Nikki Charlson, October 27, 2017.

727 Smith and others, "Counting Votes 2012."

728 Smith and others, "Counting Votes 2012."

729 Personal correspondence from Nikki Charlson, October 27, 2017.

730 Md. Elec. Code § 9-310 (2016), available at http://law.justia.com/codes/maryland/2016/election-law/title-9/subtitle-3/section-9-310/; Linda H. Lamone and Nikki Charlson, interview with author, September 15, 2017.

731 Linda H. Lamone and Nikki Charlson, interview with author, September 15, 2017; Md. Elec. Code § 9-102 (2016), available at http://law.justia.com/codes/maryland/2016/election-law/title-9/subtitle-1/section-9-102/.

732 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

733 Md. Code § 33.10.02.14, available at http://mdrules.elaws.us/comar/33.10.01.14.

734 Personal correspondence from Linda H. Lamone, September 27, 2017; Md. Code § 33.10.01.16, available at http://mdrules.elaws.us/comar/33.10.01.16.

735 Md. Code § 33.10.02.14.

736 Md. Code § 33.10.02.14.

737 Norden and Vandewalker, "Securing Elections From Foreign Interference."

738 Michelle Tassinari, Director and Legal Counsel for the Elections Division of the Secretary of the Commonwealth of Massachusetts, interview with author, September 22, 2017.

739 Michelle Tassinari, interview with author, September 22, 2017.

740 Michelle Tassinari, interview with author, September 22, 2017.

741 Michelle Tassinari, interview with author, September 22, 2017.

742 Michelle Tassinari, interview with author, September 22, 2017.

743 Local officials have limited access to the voter registration system, in that they cannot upload, download, or open any applications—including internet browsers—on the designated voter registration computer. The state oversees all local activity and monitors for disruptive activity. Michelle Tassinari, interview with author, September 22, 2017.

744 Some localities make limited use of electronic poll books during early voting. Michelle Tassinari, interview with author, September 22, 2017; The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

745 Michelle Tassinari, interview with author, September 22, 2017; Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

746 Mass. Gen. Law 54 § 109A (2016), available at https://malegislature.gov/Laws/GeneralLaws/PartI/TitleVIII/Chapter54/Section109A.

747 Mass. Gen. Law 54 § 109A.

748 Mass. Gen. Law 54 § 109A.

749 Mass. Gen. Law 54 § 109A.

750 Mass. Gen. Law 54 § 109A.

751 Michelle Tassinari, interview with author, September 22, 2017.

752 Mass. Gen. Law 54 § 109A.

753 Mass. Gen. Law 54 § 109A; Michelle Tassinari, interview with author, September 22, 2017.

754 Michelle Tassinari, interview with author, September 22, 2017.

755 Michelle Tassinari, interview with author, September 22, 2017.

756 Smith and others, "Counting Votes 2012."

757 Smith and others, "Counting Votes 2012."

758 Personal correspondence from Michelle Tassinari, November 2, 2017.

759 However, according to Michelle Tassinari: "Only official records from each precinct are those that are reviewed and signed by the poll workers. For those municipalities using voting equipment, this means that the tape that comes from the machine is unofficial and only after a process of review and verification do any precinct results become official."

760 Personal correspondence from Michelle Tassinari, November 2, 2017.

761 National Conference of State Legislatures, "Electronic Transmission of Ballots."

762 Michelle Tassinari, interview with author, September 22, 2017.

763 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

764 Mass. Gen. Law 54 § 33F (2016), available at https://malegislature.gov/Laws/GeneralLaws/PartI/TitleVIII/Chapter54/Section33F.

765 Michelle Tassinari, interview with author, September 22, 2017.

766 Mass. Gen. Law 54 § 33F; Michelle Tassinari, interview with author, September 22, 2017.

767 Norden and Vandewalker, "Securing Elections From Foreign Interference."

768 Personal correspondence from Sally Williams, State Elections Director, October 26, 2017.

769 Personal correspondence from Sally Williams, October 26, 2017.

770 Sally Williams, interview with author, September 22, 2017.

771 Sally Williams, interview with author, September 22, 2017.

772 Sally Williams, interview with author, September 22, 2017.

773 Sally Williams, interview with author, September 22, 2017.

774 Sally Williams, interview with author, September 22, 2017.

775 Sally Williams, interview with author, September 22, 2017.

776 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

777 Sally Williams, interview with author, September 22, 2017; The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books.

778 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

779 Personal correspondence from Sally Williams, October 26, 2017.

780 Bennett and others, "Cash-strapped states brace for Russian hacking fight."

781 Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

782 Personal correspondence from Sally Williams, October 26, 2017.

783 The Michigan Bureau of Elections is responsible for randomly selecting precincts and may select additional precincts to be reviewed. Discrepancies are used as educational materials for future trainings of election officials. The review is not conducted in a public forum and the results are made publicly available. The review has no bearing on official election results, even if a machine error is found to have occurred. Michigan Department of State Bureau of Elections, "Post-Election Audit Manual" (2016), available at https://www.michigan.gov/documents/sos/Post_Election_Audit_Manual_418482_7.pdf; Sally Williams, interview with author, September 22, 2017.

784 Sally Williams, personal correspondence, January 5, 2018.

785 Sally Williams, personal correspondence, January 5, 2018.

786 Smith and others, "Counting Votes 2012."

787 As part of the reconciliation process, state law permits poll workers to remove excess ballots at random. However, according to state officials, that law is not carried out. Personal correspondence from Sally Williams, October 26, 2017.; Smith and others, "Counting Votes 2012."

788 Personal correspondence from Sally Williams, October 26, 2017.; Smith and others, "Counting Votes 2012."

789 Smith and others, "Counting Votes 2012."

790 Both the precinct canvass and county-level canvass are open to the public. Personal correspondence from Sally Williams, October 26, 2017.

791 National Conference of State Legislatures, "Electronic Transmission of Ballots."

792 Sally Williams, interview with author, September 22, 2017.

793 Personal correspondence from Sally Williams, October 26, 2017.; Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

794 Personal correspondence from Sally Williams, October 26, 2017.

795 Personal correspondence from Sally Williams, October 26, 2017.; Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

796 Personal correspondence from Sally Williams, October 26, 2017.

797 Mich. Comp. Law § 168.798 (2016), available at http://law.justia.com/codes/michigan/2016/chapter-168/statute-act-116-of-1954/division-116-1954-xxviii/division-116-1954-xxviii-voting-machines/section-168.798/.

798 Mich. Comp L § 168.798.

799 Sally Williams, interview with author, September 22, 2017.

800 Norden and Vandewalker, "Securing Elections From Foreign Interference."

801 In addition, "The appropriate state or local official shall provide security measures to prevent unauthorized access" to the voter registration system. Minn. Stat. § 201.022 (2016), available at https://www.revisor.mn.gov/statutes/?id=201.022; Minn. Stat. § 201.061 (2016), available at https://www.revisor.mn.gov/statutes/?id=201.061.

802 Minn. Stat. § 201.061; Anderson, "Voter Registration Websites for 35 States Are Vulnerable to Voter ID Theft."

803 Minnesota IT Services, "Security Services," available at https://mn.gov/mnit/programs/security/security-svc.jsp (last accessed October 2017).

804 Minn. Stats § 201.061; https://mn.gov/mnit/programs/security/security-svc.jsp; Minnesota IT Services, "Security Services."

805 Personal correspondence from Gary Poser, Elections Director, November 8, 2017.

806 Gary Poser, interview with the author, September 6, 2017.

807 Only two counties have committed to purchasing electronic poll books. Minn. Stat. § 201.225 (2016), available at https://www.revisor.mn.gov/statutes?id=201.225; Gary Poser, interview with the author, September 6, 2017.

808 Jurisdictions using electronic poll books are to certify at least 30 days before the election that the electronic poll books meet all of the requirements in Minn. Stat. § 201.225. Personal correspondence from Gary Poser, November 8, 2017.

809 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

810 Personal correspondence from Gary Poser, November 8, 2017.

811 Callum Borchers, "What we know about the 21 states targeted by Russian hackers," *The Washington Post*, September 23, 2017, available at https://www.washingtonpost.com/news/the-fix/wp/2017/09/23/what-we-know-about-the-21-states-targeted-by-russian-hackers/?utm_term=.e8b4f38a6765.

812 Minn. Stat. § 206.80 (2016), available at https://www.revisor.mn.gov/statutes/?id=206.80; Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

813 Minn. Stat. § 206.89 (2016), available at https://www.revisor.mn.gov/statutes/?id=206.89.

814 Verified Voting, "State Audit Laws – Minnesota," March 2017, available at https://www.verifiedvoting.org/state-audit-laws/minnesota/.

815 Minn. Stat. § 206.89.

816 Minn. Stat. § 206.89.

817 Minn. Stat. § 206.89.

818 Minn. Stat. § 206.89.

819 Minn. Stat. § 206.89; Gary Poser, interview with the author, September 6, 2017.

820 Minn. Stat. § 206.89; Gary Poser, interview with the author, September 6, 2017.

821 Gary Poser, interview with the author, September 6, 2017.

822 Minn. Stat. § 206.89; Office of the Minnesota Secretary of State, "2016: Post-Election Review Guide," available at http://www.sos.state.mn.us/media/2701/post-election-review-guide.pdf (last accessed October 2017).

823 Minn. Stat. § 206.89.

824 Minn. Stat. § 206.89.

825 Smith and others, "Counting Votes 2012."

826 Smith and others, "Counting Votes 2012."

827 Smith and others, "Counting Votes 2012."

828 Personal correspondence from Gary Poser, October 26, 2017..

829 Smith and others, "Counting Votes 2012."

830 Personal correspondence from Gary Poser, October 26, 2017..

831 Smith and others, "Counting Votes 2012."

832 National Conference of State Legislatures, "Electronic Transmission of Ballots."

833 Minn. Stat. § 206.57 (2016), available at https://www.revisor.mn.gov/statutes/?id=206.57.

834 In Minnesota, the counties are responsible for purchasing new voting machines and some have done so in recent years. In 2013, several Twin Cities metro area counties replaced hundreds of old optical scan machines for newer models. Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference"; Laurie Blake, "Faster, More Reliable Voting Machines Coming in Metro Area," *Star Tribune*, July 5, 2013, available at http://www.startribune.com/faster-more-reliable-voting-machines-coming-in-metro-area/214447951/.

835 Minn. Senate File 1, (2017), available at https://www.revisor.mn.gov/bills/text.php?number=SF1&version=1&session_year=2017&session_number=1; Office of the Minnesota Secretary of State, "Secretary Simon's Push to Replace Minnesota's Aging Election Equipment Signed Into Law," May 31, 2017, available at http://www.sos.state.mn.us/about-the-office/news-room/secretary-simon-s-push-to-replace-minnesota-s-aging-election-equipment-signed-into-law/.

836 Minn. Stat. § 206.83 (2016), available at https://www.revisor.mn.gov/statutes/?id=206.83.

837 Minn. Stat. § 206.83.

838 Minn. Stat. § 206.83.

839 Norden and Vandewalker, "Securing Elections From Foreign Interference."

840 Charlie Case, Chief Information Officer and Kim Turner, Assistant Secretary of State, interview with author, September 22, 2017.

841 Charlie Case and Kim Turner, interview with author, September 22, 2017.

842 Charlie Case and Kim Turner,interview with author, September 22, 2017.

843 Charlie Case and Kim Turner, interview with author, September 22, 2017.

844 Charlie Case and Kim Turner, interview with author, September 22, 2017.

845 Charlie Case and Kim Turner, interview with author, September 22, 2017.

846 Charlie Case and Kim Turner, interview with author, September 22, 2017; Miss. Code § 23-15-125 (2016), available at http://law.justia.com/codes/mississippi/2016/title-23/chapter-15/article-3/e.-registration-records/section-23-15-125/; The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

847 Personal correspondence from Leah Rupp Smith, Assistant Secretary of State of Communications, November 8, 2017.

848 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

849 Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

850 Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

851 Charlie Case and Kim Turner,, interview with author, September 22, 2017; National Conference of State Legislatures, "Post-Election Audits."

852 Smith and others, "Counting Votes 2012."

853 Smith and others, "Counting Votes 2012."

854 Personal correspondence from Leah Rupp Smith, Assistant Secretary of State of Communications, November 8, 2017.

855 Smith and others, "Counting Votes 2012."

856 Personal correspondence from Leah Rupp Smith, November 8, 2017.

857 National Conference of State Legislatures, "Electronic Transmission of Ballots."

858 Charlie Case and Kim Turner, interview with author, September 22, 2017.

859 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

860 Miss. Code § 23-15-481 (2016), available at http://codes.findlaw.com/ms/title-23-elections/ms-code-sect-23-15-481.html; Miss. Code § 23-15-521 (2016), available at http://codes.findlaw.com/ms/title-23-elections/ms-code-sect-23-15-521.html.

861 Charlie Case and Kim Turner, interview with author, September 22, 2017; Miss. Code §§ 23-15-481, 23-15-521.

862 Charlie Case and Kim Turner, interview with author, September 22, 2017.

863 Norden and Vandewalker, "Securing Elections From Foreign Interference."

864 Eric Fey, Democratic Director of Elections, St. Louis County, interview with author, September 28, 2017.

865 Office of Administration, "Information Security," available at https://oa.mo.gov/itsd/it-governance/information-security (last accessed October 2017).

866 Office of Administration, "Information Security."

867 Eric Fey, interview with author, September 28, 2017.

868 Eric Fey, interview with author, September 28, 2017.

869 Mo. Rev. Stat. § 115.230 (2016), available at http://law.justia.com/codes/missouri/2016/title-ix/chapter-115/section-115.230/.

870 Eric Fey, interview with author, September 28, 2017.

871 Eric Fey, interview with author, September 28, 2017.

872 Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

873 15 Mo. Code § 30-10.110, available at https://www.sos.mo.gov/cmsimages/adrules/csr/current/15csr/15c30-10.pdf.

874 Verified Voting, "State Audit Laws – Missouri," March 2017, available at https://www.verifiedvoting.org/state-audit-laws/missouri/.

875 15 Mo. Code § 30-10.110.

876 15 Mo. Code § 30-10.110.

877 15 Mo. Code § 30-10.110.

878 Missouri does not allow early voting. Eric Fey, interview with author, September 28, 2017.

879 Counties will sometimes hand count all ballots in a particularly close race where a recount is likely. Eric Fey, interview with author, September 28, 2017.

880 15 Mo. Code § 30-10.110.

881 Eric Fey, interview with author, September 28, 2017.

882 15 Mo. Code § 30-10.110.

883 Eric Fey, interview with author, September 28, 2017

884 Smith and others, "Counting Votes 2012."

885 Smith and others, "Counting Votes 2012."

886 Smith and others, "Counting Votes 2012."

887 Smith and others, "Counting Votes 2012."

888 Smith and others, "Counting Votes 2012."

889 Specifically, those serving in a "hostile fire area." National Conference of State Legislatures, "Electronic Transmission of Ballots"; Missouri Secretary of State, "Military Overseas Voting Access Portal," available at https://www.sos.mo.gov/elections/govotemissouri/registeroverseas (last accessed October 2017); "Combat Zone, Hostile Fire or Imminent Danger* Areas," available at https://www.sos.mo.gov/CMSImages/ElectionGoVoteMissouri/HostileFirezones.pdf (last accessed October 2017).

890 Mo. Rev. Stat. § 115.225 (2016), available at http://law.justia.com/codes/missouri/2016/title-ix/chapter-115/section-115.225/; U.S. Election Assistance Commission, "State Requirements and the Federal Voting System Testing and Certification Program."

891 Eric Fey, interview with author, September 28, 2017.

892 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

893 15 Mo. Code § 30-10.040, available at https://www.sos.mo.gov/cmsimages/adrules/csr/current/15csr/15c30-10.pdf; Mo. Rev. Stat. § 115.233 (2016), available at http://law.justia.com/codes/missouri/2016/title-ix/chapter-115/section-115.233/.

894 Eric Fey, interview with author, September 28, 2017; 15 Mo. Code § 30-10.040; Mo. Rev. Stat. § 115.233.

895 Mo. Rev. Stat. § 115.233.

896 Norden and Vandewalker, "Securing Elections From Foreign Interference."

897 Department of Administration, State Information Technology Services Division, "Montana Operations Manual" (2016), available at https://montana.policytech.com/dotNet/documents/?docid=769&public=true.

898 Dana Corson, Director of Elections and Voter Services, interview with author, October 11, 2017.

899 Dana Corson, interview with author, October 11, 2017.

900 Personal correspondence from Dana Corson, October 27, 2017; Department of Administration, State Information Technology Services Division, "Montana Operations Manual."

901 Dana Corson, interview with author, October 11, 2017.

902 Montana State Information Technology Services Division, "SANS Securing the Human Training," available at http://sitsd.mt.gov/Information-Security/Cybersecurity-Training-Awareness-Program (last accessed October 2017).

903 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

904 Personal correspondence from Dana Corson, October 27, 2017.

905 Personal correspondence from Dana Corson, October 27, 2017.

906 Personal correspondence from Dana Corson, October 27, 2017; Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

907 Mont. Code § 13-17-503 (2015), available at http://leg.mt.gov/bills/mca/13/17/13-17-503.htm; Mont. Code § 13-17-507 (2015), available at http://leg.mt.gov/bills/mca/13/17/13-17-507.htm.

908 Personal correspondence from Dana Corson, October 27, 2017.

909 Verified Voting, "State Audit Laws – Montana," March 2017, available at https://www.verifiedvoting.org/state-audit-laws/montana/.

910 Mont. Code § 13-17-503.

911 Mont. Code § 13-17-503.

912 Mont. Code § 13-17-503.

913 Personal correspondence from Dana Corson, February 10, 2018.

914 Mont. Code § 13-17-507.

915 Mont. Code § 13-17-507; Mont. Code § 13-17-506 (2015), available at http://leg.mt.gov/bills/mca/13/17/13-17-506.htm.

916 Mont. Code §§ 13-17-503, 13-17-506.

917 Mont. Code § 13-17-507.

918 Smith and others, "Counting Votes 2012."

919 Smith and others, "Counting Votes 2012."

920 Personal correspondence from Dana Corson, October 27, 2017; Mont. Code § 13-15-403 (2015), available at http://leg.mt.gov/bills/mca/13/15/13-15-403.htm.

921 Smith and others, "Counting Votes 2012."

922 Personal correspondence from Dana Corson, October 27, 2017.

923 Smith and others, "Counting Votes 2012."

924 National Conference of State Legislatures, "Electronic Transmission of Ballots."

925 Personal correspondence from Dana Corson, October 27, 2017; Mont. Code § 44.3.1711 (2015), available at http://www.mtrules.org/gateway/ruleno.asp?RN=44%2E3%2E1711.

926 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

927 Mont. Code § 13-17-212 (2015), available at http://leg.mt.gov/bills/mca/13/17/13-17-212.htm.

928 Mont. Code § 13-17-212.

929 Mont. Code § 13-17-212; Mont. Reg. § 44.3.1712, available at http://mtrules.org/gateway/RuleNo.asp?RN=44%2E3%2E1712.

930 Norden and Vandewalker, "Securing Elections From Foreign Interference."

931 Wayne Bena, Deputy Secretary of State for Elections, and Laura Strimple, Director of Communications, interview with author, September 22, 2017.

932 Wayne Bena and Laura Strimple, interview with author, September 22, 2017.

933 Wayne Bena and Laura Strimple, interview with author, September 22, 2017.

934 Wayne Bena and Laura Strimple, interview with author, September 22, 2017.

935 Personal correspondence from Wayne Bena, January 24, 2018.

936 Wayne Bena and Laura Strimple, interview with author, September 22, 2017.

937 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books"; Brennan Center for Justice, "VRM in the States."

938 Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

939 Wayne Bena and Laura Strimple, personal correspondence, November 16, 2017;National Conference of State Legislatures, "Post-Election Audits."

940 National Conference of State Legislatures, "Post-Election Audits."

941 Personal correspondence from Wayne Bena, November 17, 2017.

942 Smith and others, "Counting Votes 2012."

943 Smith and others, "Counting Votes 2012."

944 Smith and others, "Counting Votes 2012."

945 Smith and others, "Counting Votes 2012."

946 Personal correspondence from Wayne Bena, October 30, 2017; Personal correspondence from Wayne Bena, November 17, 2017; Neb. Code § 32-1049.

947 Wayne Bena and Laura Strimple, personal correspondence, November 17, 2017."

948 National Conference of State Legislatures, "Electronic Transmission of Ballots."

949 Wayne Bena and Laura Strimple, interview with author, September 22, 2017.

950 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

951 Neb. Code § 32-1049 (2016), available at http://law.justia.com/codes/nebraska/2016/chapter-32/statute-32-1049/.

952 Wayne Bena and Laura Strimple, interview with author, September 22, 2017; Bagga, Losco, and Scheele, "Pre-Election Logic and Accuracy Testing and Post-Election Audit Initiative."

953 Wayne Bena and Laura Strimple, interview with author, September 22, 2017.

954 Norden and Vandewalker, "Securing Elections From Foreign Interference."

955 Personal correspondence from Wayne Thorley, October 12, 2017.

956 Personal correspondence from Wayne Thorley, October 12, 2017.

957 Personal correspondence from Wayne Thorley, October 12, 2017.

958 Personal correspondence from Wayne Thorley, October 12, 2017.

959 Personal correspondence from Wayne Thorley, January 24, 2018; Letter from Wayne Thorley, February 10, 2018, on file with author.

960 Justus Wendland, Help America Vote Act Administrator, Wayne Thorley, Deputy Secretary of State for Elections, and Jennifer Russell, Executive Assistant to the Secretary of State, interview with author, September 8, 2017.

961 Nev. Rev. Stat. § 293.095 (2015), available at https://www.leg.state.nv.us/NRS/NRS-293.html#NRS293Sec095; The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

962 Justus Wendland, Wayne Thorley, and Jennifer Russell, interview with author, September 8, 2017.

963 Justus Wendland, Wayne Thorley, and Jennifer Russell, interview with author, September 8, 2017; The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

964 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

965 News Staff, "Nevada Governor Signs Bill to Create Office of Cyber Defense Coordination," Government Technology, June 6, 2017, available at http://www.govtech.com/policy/Nevada-Governor-Signs-Bill-to-Create-Office-of-Cyber-Defense-Coordination.html; Nev. Assembly Bill 471 (2017), available at https://legiscan.com/NV/text/AB471/id/1624602/Nevada-2017-AB471-Enrolled.pdf.

966 News Staff, "Nevada Governor Signs Bill to Create Office of Cyber Defense Coordination."

967 News Staff, "Nevada Governor Signs Bill to Create Office of Cyber Defense Coordination."

968 In 2004, Nevada became the first state to require VVPR for all of its electronic touch-screen voting machines. Nev. Rev. Stat. § 293.2696 (2015), available at https://www.leg.state.nv.us/NRS/NRS-293.html#NRS293Sec2696; Nev. Rev. Stat. § 293B.082 (2015), available at https://www.leg.state.nv.us/nrs/NRS-293B.html#NRS293BSec082; Nev. Rev. Stat. § 293B.084 (2015), available at https://www.leg.state.nv.us/nrs/NRS-293B.html#NRS293BSec082; Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

969 Justus Wendland, Wayne Thorley, and Jennifer Russell, interview with author, September 8, 2017; Letter from Wayne Thorley, February 10, 2018, on file with author.

970 Justus Wendland, Wayne Thorley, and Jennifer Russell, interview with author, September 8, 2017; Letter from Wayne Thorley, February 10, 2018, on file with author.

971 Nev. Rev. Stat. § 293.255 (2015), available at https://www.leg.state.nv.us/NAC/NAC-293.html#NAC293Sec255.

972 Verified Voting, "State Audit Laws – Nevada," March 2017, available at https://www.verifiedvoting.org/state-audit-laws/nevada/; Letter from Wayne Thorley, February 10, 2018, on file with author.

973 Nev. Rev. Stat. § 293.255; Justus Wendland, Wayne Thorley, and Jennifer Russell, interview with author, September 8, 2017.

974 Nev. Rev. Stat. § 293.255.

975 Nev. Rev. Stat. § 293.255; Justus Wendland, Wayne Thorley, and Jennifer Russell, interview with author, September 8, 2017.

976 Personal correspondence from Wayne Thorley, October 12, 2017.

977 Personal correspondence from Wayne Thorley, October 12, 2017.

978 Nev. Rev. Stat. § 293.255; personal correspondence from Wayne Thorley, October 12, 2017.

979 Nev. Rev. Stat. § 293.255.

980 Personal correspondence from Wayne Thorley, October 12, 2017.

981 Smith and others, "Counting Votes 2012."

982 Smith and others, "Counting Votes 2012."

983 Smith and others, "Counting Votes 2012."

984 Personal correspondence Email from Wayne Thorley, December 13, 2017.; NRS 293B.330, available at https://www.leg.state.nv.us/nrs/NRS-293B.html#NRS293BSec330.

985 Smith and others, "Counting Votes 2012."

986 Nev. Rev. Stat. § 293.323 (2015), available at https://www.leg.state.nv.us/NRS/NRS-293.html#NRS293Sec323; National Conference of State Legislatures, "Electronic Transmission of Ballots"; We are told that Nevada has a UOCAVA ballot return rate of 91.2 percent, due, at least in part, to the state's Effective Absentee System for Elections (EASE) online ballot delivery system; Letter from Wayne Thorley, February 10, 2018, on file with author.

987 Nev. Rev. Stat. § 293.2696; Justus Wendland, Wayne Thorley, and Jennifer Russell, interview with author, September 8, 2017.

988 Justus Wendland, Wayne Thorley, and Jennifer Russell, interview with author, September 8, 2017.

989 Justus Wendland, Wayne Thorley, and Jennifer Russell, interview with author, September 8, 2017.

990 Nev. Assembly Bill 519 (2017), available at https://www.leg.state.nv.us/Session/79th2017/Reports/history.cfm?ID=1183; Justus Wendland, Wayne Thorley, and Jennifer Russell, interview with author, September 8, 2017.

991 Prior to each federal election cycle, Nevada requires each system component, including the software and firmware, to match the identity of the operating system with that on file with the National Software Reference Library. (NAC 293B.110 / https://www.leg.state.nv.us/NAC/NAC-293B.html#NAC293BSec110) ; Nev. Rev. Stat. § 293B.150 (2015), available at https://www.leg.state.nv.us/nrs/NRS-293B.html#NRS293BSec150; Nev. Rev. Stat. § 293B.155, available at https://www.leg.state.nv.us/nrs/NRS-293B.html#NRS293BSec150.

992 Personal correspondence from Wayne Thorley, October 12, 2017.

993 Nev. Rev. Stat. §**§** 293B.150, 293B.155.

994 According to a personal correspondence from Assistant Secretary of State Anthony Stevens, "New Hampshire has determined that openly publishing the details of its cyber security efforts would be, by itself, a degradation of those strategies. Refer to New Hampshire Revised Statutes Annotated 654:45, which requires the New Hampshire Secretary of State to 'Provide adequate technological security measures to deter unauthorized access to the records contained in the voter database.'" Personal correspondence from Anthony Stevens, Assistant Secretary of State, October 26, 2017.

995 Personal correspondence from Anthony Stevens, Assistant Secretary of State, October 25, 2017; Norden and Vandewalker, "Securing Elections From Foreign Interference."

996 Personal correspondence from Anthony Stevens, October 25, 2017.

997 New Hampshire City & Town Clerks Association, "ElectioNet Intro Training," available at http://nhctca.com/?page_id=931 (last accessed October 2017).

998 NH Labor News, "Trial Poll Book Devices Are Step Toward Modernizing, Securing, and Streamlining Elections," June 1, 2017, available at http://nhlabornews.com/2017/06/new-hampshire-legislature-becomes-34th-state-to-allow-electronic-poll-books/; Associated Press, "Vendor Chosen to Evaluate Electronic Poll Book Systems," *US News*, September 5, 2017, available at https://www.usnews.com/news/best-states/new-hampshire/articles/2017-09-05/vendor-chosen-to-evaluate-electronic-poll-book-systems.

999 N.H. Rev. Stat. § 656:1-a (2016), available at http://law.justia.com/codes/new-hampshire/2016/title-lxiii/chapter-656/section-656-1-a/; N.H. Rev. Stat. § 656:41 (2016), available at http://law.justia.com/codes/new-hampshire/2016/title-lxiii/chapter-656/section-656-41/.

1000 National Conference of State Legislatures, "Post-Election Audits"; Verified Voting, "State Audit Laws – New Hampshire," March 2017, available at https://www.verifiedvoting.org/state-audit-laws/new%20hampshire/.

1001 Smith and others, "Counting Votes 2012."

1002 Smith and others, "Counting Votes 2012."

1003 Smith and others, "Counting Votes 2012."

1004 Smith and others, "Counting Votes 2012."

1005 Smith and others, "Counting Votes 2012."

1006 National Conference of State Legislatures, "Electronic Transmission of Ballots."

1007 U.S. Election Assistance Commission, "State Requirements and the Federal Voting System Testing and Certification Program."

1008 New Hampshire uses the term "counting device" as opposed to "voting machine." However, for the purposes of uniformity and simplicity, we call all voting or counting devices—including optical scanners—"voting machines" for the purposes of this report. Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

1009 N.H. Rev. Stat. § 656:42 (2016), available at http://law.justia.com/codes/new-hampshire/2016/title-lxiii/chapter-656/section-656-42.

1010 N.H. Rev. Stat. § 656:42.

1011 N.H. Rev. Stat. § 656:42.

1012 Norden and Vandewalker, "Securing Elections From Foreign Interference."

1013 Robert Giles, Director, New Jersey Division of Elections, interview with author, November 17, 2017.

1014 Anderson, "Voter Registration Websites for 35 States Are Vulnerable to Voter ID Theft."

1015 Robert Giles, interview with author, September 19, 2017.

1016 Robert Giles, interview with author, September 19, 2017.

1017 Robert Giles, interview with author, September 19, 2017.

1018 Robert Giles, interview with author, September 19, 2017.

1019 Robert Giles, interview with author, September 19, 2017.

1020 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books"; National Conference of State Legislatures, "Electronic Poll Books."

1021 State law specifies that "by January 1, 2009, each voting machine shall produce an individual permanent paper record for each vote cast" with this important caveat: "The provisions of paragraph (1) of this subsection shall be suspended until: (i) the Secretary of State and the State Treasurer certify in writing that sufficient funds have been provided by the federal government and received by the State to offset the entire cost of ensuring that each voting machine used in this State produces an individual permanent paper record for each vote cast; or (ii) the annual appropriation act contains an appropriation of sufficient funds to ensure that each voting machine used in this State produces an individual permanent paper record for each vote cast and such appropriated funds have not been reserved by the Governor under a spending reduction plan; or (iii) the Secretary of State and the State Treasurer certify in writing that sufficient funds have been provided by the federal government and received by the State, and the annual appropriation act contains an appropriation of sufficient unreserved funds, to ensure, when such funds are combined, that each voting machine used in this State produces an individual paper record for each vote cast." Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

1022 NJ A 1563, available at https://custom.statenet.com/public/resources.cgi?id=ID:bill:NJ2018000A1563&ciq=ncsl15&client_md=62dc876d3f54e0164598a7005bbf2515&mode=current_text (last accessed January 2018).

1023 Robert Giles, interview with author, September 19, 2017.

1024 N.J. Rev. Stat. § 19:61-9 (2016), available at http://www.nj.gov/state/dos_statutes-elections-19-60-63.shtml#ele_19_61_9.

1025 Smith and others, "Counting Votes 2012."

1026 Smith and others, "Counting Votes 2012."

1027 Smith and others, "Counting Votes 2012."

1028 Smith and others, "Counting Votes 2012."

1029 While not required by law, we are told this is done in practice. Robert Giles, interview with author, November 17, 2017.

1030 Robert Giles, interview with author, November 17, 2017.

1031 National Conference of State Legislatures, "Electronic Transmission of Ballots."

1032 Robert Giles, interview with author, September 19, 2017.

1033 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

1034 N.J. Rev. Stat. § 19:53A-8 (2016), available at http://law.justia.com/codes/new-jersey/2016/title-19/section-19-53a-8/; State of New Jersey Division of Elections, "Mandatory Pre-Election Testing Protocols: AVC Advantage Voting Machines," available at https://www.eac.gov/assets/1/28/AVC%20Advantage%20Mandatory%20Pre-Election%20Testing%20Protocols%20Updated%206-15-2015.pdf (last accessed October 2017).

1035 N.J. Rev. Stat. § 19:53A-8.

1036 Personal correspondence from Kari Fresquez, Elections Director, January 3, 2018.

1037 State law requires the New Mexico secretary of state to take steps to minimize the risk of unauthorized disclosure and to decommission any accounts and usernames of election officials immediately after resignation, and also to maintain a backup voter registration database in case of emergency. N.M. Stat. § 1-5-18 (2016), available at http://law.justia.com/codes/new-mexico/2016/chapter-1/article-5/section-1-5-18/; N.M. Admin. Law § 1.10.35.11, available at http://164.64.110.239/nmac/parts/title01/01.010.0035.htm; Kari Fresquez, interview with author, September 6, 2017.

1038 N.M. Admin. Law § 1.10.35.11; personal correspondence from Kari Fresquez, September 25, 2017.

1039 N.M. Admin. Law § 1.10.35.11; personal correspondence from Kari Fresquez, September 25, 2017.

1040 Personal correspondence from Kari Fresquez, September 25, 2017.

1041 Personal correspondence from Kari Fresquez, September 25, 2017.

1042 The cybersecurity training began in 2016, largely in response to reports that the voter registration systems of Illinois and Arizona had been targeted by hackers earlier that year. Those events were incorporated into the lesson plan as learning tools, as was a discussion on security protections and the proper use of voter registration systems. Kari Fresquez, interview with author, September 6, 2017.

1043 N.M. Stat. § 1-3-4 (2016), available at http://law.justia.com/codes/new-mexico/2016/chapter-1/article-3/section-1-3-4/; The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

1044 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

1045 Kari Fresquez, interview with author, September 6, 2017; The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

1046 Poll book vendors are available to provide on-the-ground IT and system support when needed. The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books"; Kari Fresquez, interview with author, September 6, 2017.

1047 Personal correspondence from Kari Fresquez, January 3, 2017.

1048 Kari Fresquez, interview with author, September 6, 2017.

1049 N.M. Stat. § 1-9-7.1 (2016), available at http://law.justia.com/codes/new-mexico/2016/chapter-1/article-9/section-1-9-7.1/; N.M. Stat. § 1-9-5 (2016), available at http://law.justia.com/codes/new-mexico/2016/chapter-1/article-9/section-1-9-5/; Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

1050 N.M. Stat. § 1-14-13.2 (2016), available at http://law.justia.com/codes/new-mexico/2016/chapter-1/article-14/section-1-14-13.2/.

1051 Verified Voting, "State Audit Laws – New Mexico," March 2017, available at https://www.verifiedvoting.org/state-audit-laws/new%20mexico/.

1052 N.M. Stat. § 1-14-13.2.

1053 N.M. Stat. § 1-14-13.2.

1054 Ibid.

1055 Personal correspondence from Kari Fresquez, October 24, 2017; Verified Voting, "State Audit Laws – New Mexico."

1056 N.M. Stat. § 1-14-13.2.

1057 N.M. Stat. § 1-14-13.2.

1058 N.M. Stat. § 1-14-13.2; Ballotpedia, "Election Results Certification Dates, 2016."

1059 Personal correspondence from Kari Fresquez, September 25, 2017.

1060 Smith and others, "Counting Votes 2012."

1061 Personal correspondence from Kari Fresquez, October 24, 2017.

1062 Personal correspondence from Kari Fresquez, October 24, 2017.

1063 Personal correspondence from Kari Fresquez, October 24, 2017; Smith and others, "Counting Votes 2012."

1064 Smith and others, "Counting Votes 2012."

1065 N.M. Stat. § 1-6B-8 (2016), available at http://law.justia.com/codes/new-mexico/2016/chapter-1/article-6b/section-1-6b-8/; National Conference of State Legislatures, "Electronic Transmission of Ballots."

1066 N.M. Stat. § 1-9-14 (2016), available at http://law.justia.com/codes/new-mexico/2016/chapter-1/article-9/section-1-9-14/.

1067 Kari Fresquez, interview with author, September 6, 2017; Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

1068 N.M. Stat. § 1-11-6.1 (2016), available at http://law.justia.com/codes/new-mexico/2016/chapter-1/article-11/section-1-11-6.1/.

1069 Personal correspondence with Kari Fresquez, October 24, 2017.

1070 Norden and Vandewalker, "Securing Elections From Foreign Interference."

1071 New York State Department of Financial Services, "Summary of New 23 NYCRR 500," available at http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf-500sapa.pdf (last accessed October 2017).

1072 New York State Board of Elections, "Annual Report" (2016), available at https://www.elections.ny.gov/NYSBOE/download/AnnualReport2016.pdf.

1073 New York State Board of Elections, "Annual Report."

1074 New York State Board of Elections, "Annual Report."

1075 New York State Board of Elections, "Annual Report."

1076 State of New York, "Cyber Security Resources for Local Government" (2017), available at https://its.ny.gov/sites/default/files/documents/cyber_security_resources_for_local_government_2017-06-07.pdf.

1077 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

1078 Kenneth Lovett, "Cuomo to Order Review of N.Y. Election Cyber Security in Light of Potential Hacking Threats," *Daily News*, June 20, 2017, available at http://www.nydailynews.com/news/politics/cuomo-order-review-n-y-voting-cyber-security-article-1.3261068.

1079 Kenneth Lovett, "Cuomo to Order Review of N.Y. Election Cyber Security in Light of Potential Hacking Threats."

1080 Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

1081 N.Y. Elec. Law § 9-211 (2016), available at http://law.justia.com/codes/new-york/2016/eln/article-9/title-2/9-211/.

1082 N.Y. Elec. Law § 9-211.

1083 N.Y. Elec. Law § 9-211.

1084 N.Y. Elec. Law § 9-211.

1085 Interview with Robert Brehm, co-executive director, New York State Board of Elections, February 7, 2018.

1086 Local boards of elections are permitted to require a complete audit of all voting machines or systems within their jurisdiction if discrepancies arise. The state board of elections is required to create a uniform contingency plan for local county boards of elections to follow in the event of a discrepancy between the initial tally and audit results. Such plans are to include information on when an audit may expand to include additional machines or systems. N.Y. Elec. Law § 9-211; 9 N.Y. Code § 6210.18, available at https://govt.westlaw.com/nycrr/Document/I5c54c4e18b2e11dfbe5dec62e7eacc45.

1087 Interview with Robert Brehm, co-executive director, New York State Board of Elections, February 7, 2018.

1088 Audits are conducted within 15 days after each general or special election and within seven days after every primary or village election. N.Y. Elec. Law § 9-211.

1089 The state board of elections is required to create a uniform contingency plan for local county boards of elections to follow in the event of a discrepancy between the initial tally and audit results. Such plans are to include information on when an audit may expand to include additional machines or systems. N.Y. Elec. Law § 9-211.

1090 NY S 7144, available at https://custom.statenet.com/public/resources.cgi?id=ID:bill:NY2017000S7144&ciq=ncsl15&client_md=5e9396135690a75f200b67bb92e23e51&mode=current_text (last accessed January 2018).

1091 Smith and others, "Counting Votes 2012."

1092 Smith and others, "Counting Votes 2012."

1093 Smith and others, "Counting Votes 2012."

1094 Interview with Robert Brehm, co-executive director, New York State Board of Elections, February 7, 2018.

1095 Interview with Robert Brehm, co-executive director, New York State Board of Elections, February 7, 2018.

1096 National Conference of State Legislatures, "Electronic Transmission of Ballots."

1097 N.Y. Elec. Law § 7-201 (2016), available at http://law.justia.com/codes/new-york/2016/eln/article-7/title-2/7-201/; U.S. Election Assistance Commission, "State Requirements and the Federal Voting System Testing and Certification Program."

1098 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

1099 N.Y. Elec. Law § 7-206 (2016), available at http://law.justia.com/codes/new-york/2016/eln/article-7/title-2/7-206/.

1100 N.Y. Elec. Law § 7-206.

1101 Interview with Robert Brehm, co-executive director, New York State Board of Elections, February 7, 2018.

1102 Norden and Vandewalker, "Securing Elections From Foreign Interference."

1103 Personal correspondence from Emily Lippolis, Agency Legal Counsel, North Carolina State Board of Elections, October 31, 2017.

1104 Brian Neesby, Chief Data Officer, North Carolina State Board of Elections, interview with author, September 13, 2017.

1105 Personal correspondence from Brian Neesby, October 31, 2017.

1106 Personal correspondence from Emily Lippolis, November 15, 2017.

1107 Personal correspondence from Marc Burris, Chief Information Officer, North Carolina State Board of Elections, October 31, 2017.

1108 Brian Neesby, interview with author, September 13, 2017.

1109 Personal correspondence from Marc Burris, October 31, 2017.

1110 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books"; N.C. Gen. Stat. § 163.166.7.

1111 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

1112 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

1113 Personal correspondence from Josh Lawson, General Counsel, North Carolina State Board of Elections, October 31, 2017.

1114 Verified Voting, "The Verifier—Polling Place Equipment—November 2016"; N.C. Gen. Stat. § 163-165.7 (2015), available at http://www.ncleg.net/EnactedLegislation/Statutes/PDF/BySection/Chapter_163/GS_163-165.7.pdf.

1115 Personal correspondence from Emily Lippolis, October 31, 2017.

1116 N.C. Gen. Stat. § 163-182.1 (2015), available at http://law.justia.com/codes/north-carolina/2015/chapter-163/article-15a/section-163-182.1/.

1117 Verified Voting, "State Audit Laws – North Carolina," March 2017, available at https://www.verifiedvoting.org/state-audit-laws/north%20carolina/.

1118 N.C. Gen. Stat. § 163-182.1.

1119 N.C. Gen. Stat. § 163-182.1; personal correspondence from Veronica Degraffenreid, Head of Election Preparation & Support, State Board of Elections, October 31, 2017.

1120 N.C. Gen. Stat. § 163-182.1.

1121 N.C. Gen. Stat. § 163-182.1.

1122 Brian Neesby, interview with author, September 13, 2017.

1123 Personal correspondence with Brian Neesby, February 10, 2018.

1124 N.C. Gen. Stat. § 163-182.1; Personal correspondence email from Emily Lippolis, October 31, 2017.

1125 Personal correspondence Email from Emily Lippolis, October 31, 2017.

1126 N.C. Gen. Stat. § 163-182.1; Brian Neesby, interview with author, September 13, 2017.

1127 N.C. Gen. Stat. § 163-182.1; personal correspondence from Emily Lippolis, October 31, 2017.

1128 Personal correspondence with Brian Neesby, February 10, 2018.

1129 Smith and others, "Counting Votes 2012."

1130 Personal correspondence from Emily Lippolis, October 31, 2017.

1131 Personal correspondence from Emily Lippolis, October 31, 2017.

1132 Smith and others, "Counting Votes 2012."

1133 Personal correspondence from Emily Lippolis, December 12, 2017.

1134 National Conference of State Legislatures, "Electronic Transmission of Ballots."

1135 8 N.C. Admin. Code § 04.0302, available at http://reports.oah.state.nc.us/ncac/title%2008%20-%20elections/chapter%2004%20-%20voting%20equipment/08%20ncac%2004%20.0302.pdf; 8 N.C. Admin. Code § 04.0301, available at http://reports.oah.state.nc.us/ncac/title%2008%20-%20elections/chapter%2004%20-%20voting%20equipment/08%20ncac%2004%20.0301.pdf; N.C. Gen. Stat. § 163-165.7.

1136 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

1137 N.C. Gen. Stat. § 163-33.2 (2015), available at http://law.justia.com/codes/north-carolina/2015/chapter-163/article-4/section-163-33.2/; 8 N.C. Admin. Code § 04.0307, available at http://reports.oah.state.nc.us/ncac/title%2008%20-%20elections/chapter%2004%20-%20voting%20equipment/08%20ncac%2004%20.0307.pdf; Brian Neesby, interview with author, September 13, 2017.

1138 8 N.C. Admin. Code § 04.0307.

1139 John Arnold, Director of Elections, interview with author, September 18, 2017; Norden and Vandewalker, "Securing Elections From Foreign Interference."

1140 John Arnold, interview with author, September 18, 2017.

1141 John Arnold, interview with author, September 18, 2017.

1142 Personal correspondence with John Arnold, November 17, 2017.

1143 John Arnold, interview with author, September 18, 2017.

1144 Ibid.

1145 John Arnold, interview with author, September 18, 2017.

1146 John Arnold, interview with author, September 18, 2017.

1147 N.D. Admin. Code § 16.1-06-21; The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

1148 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

1149 John Arnold, interview with author, September 18, 2017.

1150 John Arnold, interview with author, September 18, 2017.

1151 Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

1152 National Conference of State Legislatures, "Post-Election Audits"; Verified Voting, "State Audit Laws – North Dakota," March 2017, available at https://www.verifiedvoting.org/state-audit-laws/north%20dakota/.

1153 N.D. Admin. Code § 16.1-06-15, available at http://www.legis.nd.gov/cencode/t16-1c06.pdf#nameddest=16p1-06-15; John Arnold, interview with author, September 18, 2017.

1154 Smith and others, "Counting Votes 2012."

1155 Smith and others, "Counting Votes 2012."

1156 Smith and others, "Counting Votes 2012."

1157 Smith and others, "Counting Votes 2012."

1158 Smith and others, "Counting Votes 2012."

1159 National Conference of State Legislatures, "Electronic Transmission of Ballots."

1160 N.D. Admin. Code § 72-06-01-02, available at http://www.legis.nd.gov/information/acdata/pdf/72-06-01.pdf.

1161 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

1162 Dave Thompson, "Aging voting machines could pose a challenge for counties," Prairie Public News, January 2, 2018, available at http://news.prairiepublic.org/post/aging-voting-machines-could-pose-challenge-counties#stream/0.

1163 N.D. Admin. Code § 16.1-06-15; John Arnold, interview with author, September 18, 2017.

1164 N.D. Admin. Code § 16.1-06-15; John Arnold, interview with author, September 18, 2017.

1165 N.D. Admin. Code § 16.1-06-15; John Arnold, interview with author, September 18, 2017.

1166 Norden and Vandewalker, "Securing Elections From Foreign Interference."

1167 Rene March, "Ohio Taps National Guard to Defend Election System From Hackers," CNN, November 1, 2016, available at http://www.cnn.com/2016/11/01/politics/election-hacking-cyberattack/index.html; Breland, "State Declines DHS Security for Voting Machines."

1168 Ohio Rev. Stat. § 3506.021, available at http://codes.ohio.gov/orc/3506.021v1; The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

1169 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

1170 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

1171 Ohio Rev. Stat. § 3506.10, available at http://codes.ohio.gov/orc/3506.10; Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

1172 H. B. No. 467, available at http://www.ohiohouse.gov/kathleen-clyde (last accessed January 2018); H. B. No. 466, available at http://www.ohiohouse.gov/kathleen-clyde (last accessed January 2018); The Ohio House of Representatives, "Clyde Announces Cybersecurity Legislation To Make Elections Safe And Secure," January 11, 2018, available at http://www.ohiohouse.gov/kathleen-clyde/press/clyde-announces-cybersecurity-legislation-to-make-elections-safe-and-secure; Mary Kilpatrick, "Ohio Lawmaker Prepares to Introduce Elections Cybersecurity Bills," GovTech, January 11, 2018, available at http://www.govtech.com/security/Ohio-Lawmaker-Prepares-to-Introduce-Elections-Cybersecurity-Bills.html.

1173 Jon Husted, "Directive 2014-36," October 29, 2014, available at https://www.sos.state.oh.us/globalassets/elections/directives/2014/dir2014-36.pdf.

1174 Jon Husted, "Directive 2014-36."

1175 Jon Husted, "Directive 2014-36."

1176 Jon Husted, "Directive 2014-36."

1177 Jon Husted, "Directive 2014-36."

1178 Jon Husted, "Directive 2014-36."

1179 Jon Husted, "Directive 2014-36."

1180 Jon Husted, "Directive 2014-36."

1181 Jon Husted, "Directive 2014-36"; Verified Voting, "State Audit Laws – Ohio," March 2017, available at https://www.verifiedvoting.org/state-audit-laws/ohio/.

1182 Jon Husted, "Directive 2014-36."

1183 Jon Husted, "Directive 2014-36."

1184 Jon Husted, "Directive 2014-36."

1185 Smith and others, "Counting Votes 2012."

1186 Smith and others, "Counting Votes 2012."

1187 Smith and others, "Counting Votes 2012."

1188 Smith and others, "Counting Votes 2012."

1189 Smith and others, "Counting Votes 2012."

1190 Smith and others, "Counting Votes 2012."

1191 Ohio Rev. Stat. § 3511.05, available at http://codes.ohio.gov/orc/3511.05v1; National Conference of State Legislatures, "Electronic Transmission of Ballots."

1192 Ohio Sunset Review Committee, "Agency Questionnaire: Ohio Board of Voting Machine Examiners," available at http://sunset.legislature.ohio.gov/Assets/Files/ohio-board-of-voting-machine-examiners-questionnaire.pdf (last accessed October 2017); U.S. Election Assistance Commission, "State Requirements and the Federal Voting System Testing and Certification Program."

1193 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

1194 Letter from Ohio Secretary of State Jon Husted to Ohio Governor John Kasich, December 14, 2017, available at https://www.sos.state.oh.us/globalassets/media-center/news/2017/20171214.pdf.

1195 Ohio Rev. Stat. § 3506.14, available at http://codes.ohio.gov/orc/3506.14v1.

1196 Ohio Rev. Stat. § 3506.14.

1197 Norden and Vandewalker, "Securing Elections From Foreign Interference."

1198 State of Oklahoma, "Information Security Policy, Procedures, Guidelines" (2015), available at https://www.ok.gov/cio/documents/InfoSecPPG.pdf.

1199 State of Oklahoma, "Information Security Policy, Procedures, Guidelines."

1200 State of Oklahoma, "Information Security Policy, Procedures, Guidelines."

1201 State of Oklahoma, "Information Security Policy, Procedures, Guidelines."

1202 Survey response from Mitchell Antle, Election Commissioner.

1203 26 Okla. Stat. § 26-6-102.1 (2016), available at http://law.justia.com/codes/oklahoma/2016/title-26/section-26-6-102.1/; Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

1204 Survey response from Mitchell Antle.

1205 Smith and others, "Counting Votes 2012."

1206 Smith and others, "Counting Votes 2012."

1207 Smith and others, "Counting Votes 2012."

1208 Smith and others, "Counting Votes 2012."

1209 Smith and others, "Counting Votes 2012."

1210 Federal Voting Assistance Program, "Oklahoma," available at https://www.fvap.gov/vao/vag/chapter2/oklahoma (last accessed October 2017); National Conference of State Legislatures, "Electronic Transmission of Ballots."

1211 Survey response from Mitchell Antle.

1212 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

1213 Survey response from Mitchell Antle; 26 Okla. Stat. § 26-9-115 (2016), available at https://www.oscn.net/applications/oscn/DeliverDocument.asp?CiteID=78637.

1214 State law requires notification be sent to the county chair of each political party and a representative is permitted to observe the testing, but is silent on providing notice to the general public. Survey response from Mitchell Antle; 26 Okla. Stat. § 26-9-115.

1215 Norden and Vandewalker, "Securing Elections From Foreign Interference."

1216 Steve Trout, Elections Director, interview with author, September 15, 2017.

1217 Personal correspondence from Steve Trout, September 25, 2017.

1218 Personal correspondence from Steve Trout, September 25, 2017.

1219 Personal correspondence from Steve Trout, September 25, 2017.

1220 Personal correspondence from Steve Trout, September 25, 2017.

1221 Personal correspondence from Steve Trout, January 24, 2018.

1222 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

1223 Bennett and others, "Cash-strapped states brace for Russian hacking fight."

1224 Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

1225 Ore. Rev. Stat. § 254.529 (2015), available at http://law.justia.com/codes/oregon/2015/volume-06/chapter-254/section-254.529/.

1226 Verified Voting, "State Audit Laws – Oregon," March 2017, available at https://www.verifiedvoting.org/state-audit-laws/oregon/.

1227 Ore. Rev. Stat. § 254.529.

1228 Ore. Rev. Stat. § 254.529.

1229 Ore. Rev. Stat. § 254.529.

1230 Ore. Rev. Stat. § 254.529.

1231 Ore. Rev. Stat. § 254.529.

1232 Survey response from Steve Trout.

1233 Ore. Rev. Stat. § 254.529.

1234 Ore. Rev. Stat. § 254.529; Steve Trout, interview with author, September 15, 2017.

1235 Ore. Admin. Law § 165-007-0290, available at http://arcweb.sos.state.or.us/pages/rules/oars_100/oar_165/165_007.html; Ore. Rev. Stat. § 254.529.

1236 Personal correspondence from Steve Trout, October 27, 2017.; Ore. Rev. Stat. § 254.529.

1237 Smith and others, "Counting Votes 2012."

1238 Smith and others, "Counting Votes 2012."

1239 Smith and others, "Counting Votes 2012."

1240 Smith and others, "Counting Votes 2012."

1241 Smith and others, "Counting Votes 2012."

1242 Smith and others, "Counting Votes 2012."

1243 Smith and others, "Counting Votes 2012."

1244 National Conference of State Legislatures, "Electronic Transmission of Ballots."

1245 Survey response from Steve Trout.

1246 Some counties purchased new voting machines last year. Personal correspondence from Steve Trout, October 27, 2017; Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

1247 Ore. Rev. Stat. § 254.235 (2015), available at https://www.oregonlegislature.gov/bills_laws/ors/ors254.html; Ore. Rev. Stat. § 254.485 (2015), available at https://www.oregonlegislature.gov/bills_laws/ors/ors254.html.

1248 Steve Trout, interview with author, September 15, 2017.

1249 Ore. Rev. Stat. §**§** 254.235, 254.485.

1250 Norden and Vandewalker, "Securing Elections From Foreign Interference."

1251 Jonathan Marks, Commissioner for the Bureau of Commissions of Elections and Legislation, Michael Moser, Deputy Commissioner for the Bureau of Commissions of Elections and Legislation, Kalonji Johnson, Director of Policy, Pennsylvania Department of State, and Jessica Myers, Deputy Director of Policy, Pennsylvania Department of State, interview with author, September 11, 2017.

1252 Pennsylvania Department of State, "Statement in Response to Harvard Study on Voter Registration Website Security" (2017), available at http://www.dos.pa.gov/Documents/9.7.17%20-%20DOS%20Statement%20-%20Harvard%20Study%20on%20VR%20Website%20Security.pdf.

1253 Pennsylvania Department of State, "Statement in Response to Harvard Study on Voter Registration Website Security."

1254 Pennsylvania Department of State, "Statement in Response to Harvard Study on Voter Registration Website Security."

1255 Pennsylvania Department of State, "Statement in Response to Harvard Study on Voter Registration Website Security."

1256 Personal correspondence from Jessica Myers, October 31, 2017.

1257 25 Pa. Cons. Stat. § 1402 (2016), available at http://law.justia.com/codes/pennsylvania/2016/title-25/chapter-14/section-1402/; The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

1258 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

1259 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books"; Jonathan Marks, Michael Moser, Kalonji Johnson, and Jessica Myers, interview with author, September 11, 2017.

1260 Personal correspondence from Jessica Myers, October 31, 2017.

1261 Jonathan Marks, Michael Moser, Kalonji Johnson, and Jessica Myers, interview with author, September 11, 2017.

1262 Jonathan Marks, Michael Moser, Kalonji Johnson, and Jessica Myers, interview with author, September 11, 2017.

1263 Verified Voting, "The Verifier—Polling Place Equipment—November 2016"; Michael Rubinkam, "Pennsylvania to Require Voting Machines With Paper Backup," U.S. News, February 9, 2018, available at https://www.usnews.com/news/best-states/pennsylvania/articles/2018-02-09/pennsylvania-to-require-voting-machines-with-paper-backup.

1264 Advisory Committee on Voting Technology, "Voting Technology in Pennsylvania."

1265 25 Pa. Cons. Stat. § 3031.17, available at http://codes.findlaw.com/pa/title-25-ps-elections-electoral-districts/pa-st-sect-25-3031-17.html.

1266 Verified Voting, "State Audit Laws – Pennsylvania," March 2017, available at https://www.verifiedvoting.org/state-audit-laws/pennsylvania/.

1267 25 Pa. Cons. Stat. § 3031.17.

1268 25 Pa. Cons. Stat. § 3031.17.

1269 25 Pa. Cons. Stat. § 3031.17.

1270 25 Pa. Cons. Stat. § 3031.17.

1271 Personal correspondence from Jessica Myers, October 31, 2017..

1272 Jonathan Marks, Michael Moser, Kalonji Johnson, and Jessica Myers, interview with author, September 11, 2017.

1273 Personal correspondence from Jessica Myers, November 3, 2017.

1274 Smith and others, "Counting Votes 2012"; 25 Pa. Cons. Stat. § 3061, available at http://codes.findlaw.com/pa/title-25-ps-elections-electoral-districts/pa-st-sect-25-3061.html; 25 Pa. Cons. Stat. § 3031.13, available at http://codes.findlaw.com/pa/title-25-ps-elections-electoral-districts/pa-st-sect-25-3031-13.html; 25 Pa. Cons. Stat. § 3062, available at http://codes.findlaw.com/pa/title-25-ps-elections-electoral-districts/pa-st-sect-25-3062.html; 25 Pa. Cons. Stat. § 3065, available at http://codes.findlaw.com/pa/title-25-ps-elections-electoral-districts/pa-st-sect-25-3065.html; 25 Pa. Cons. Stat. § 3067, available at http://codes.findlaw.com/pa/title-25-ps-elections-electoral-districts/pa-st-sect-25-3067.html; 25 Pa. Cons. Stat. § 3068, available at http://codes.findlaw.com/pa/title-25-ps-elections-electoral-districts/pa-st-sect-25-3068.html; 25 Pa. Cons. Stat. § 3066, available at http://codes.findlaw.com/pa/title-25-ps-elections-electoral-districts/pa-st-sect-25-3066.html.

1275 Smith and others, "Counting Votes 2012"; 25 Pa. Cons. Stat. §§ 3061, 3031.13, 3066.

1276 Smith and others, "Counting Votes 2012"; 25 Pa. Cons. Stat. § 3154, available at http://codes.findlaw.com/pa/title-25-ps-elections-electoral-districts/pa-st-sect-25-3154.html.

1277 Smith and others, "Counting Votes 2012"; 25 Pa. Cons. Stat. §§ 3061, 3031.13, § 3068.

1278 Smith and others, "Counting Votes 2012"; 25 Pa. Cons. Stat. §§ 3061, 3031.13, 3068.

1279 National Conference of State Legislatures, "Electronic Transmission of Ballots."

1280 25 Pa. Cons. Stat. § 3031.5, available at http://codes.findlaw.com/pa/title-25-ps-elections-electoral-districts/pa-st-sect-25-3031-5.html; Jonathan Marks, Michael Moser, Kalonji Johnson, and Jessica Myers, interview with author, September 11, 2017.

1281 New voting machines are purchased at the county level; some counties purchased new machines as recently as 2016. Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference"; Jonathan Marks, Michael Moser, Kalonji Johnson, and Jessica Myers, interview with author, September 11, 2017.

1282 25 Pa. Cons. Stat. § 3031.14.14, available at http://codes.findlaw.com/pa/title-25-ps-elections-electoral-districts/pa-st-sect-25-3031-14.html; Jonathan Marks, Michael Moser, Kalonji Johnson, and Jessica Myers, interview with author, September 11, 2017.

1283 25 Pa. Cons. Stat. § 3031.14.14.

1284 25 Pa. Cons. Stat. § 3031.14.14.

1285 Norden and Vandewalker, "Securing Elections From Foreign Interference."

1286 Election officials will not be able to log onto the state voter registration database unless they sign on from a trusted network, using a registered Mac address and network password. Rob Rock, Director of Elections, interview with author, September 7, 2017.

1287 Every change to the voter registration system is tracked and logged with the ID and unique identifier of the individual who made the alteration. Rob Rock, interview with author, September 7, 2017.

1288 Personal correspondence from Rob Rock, October 30, 2017.

1289 Rob Rock, interview with author, September 7, 2017.

1290 Rob Rock, interview with author, September 7, 2017.

1291 Rob Rock, interview with author, September 7, 2017; Eliza Newlin Carney, "On Election Security, Feds Flounder While States Make Strides," *The American Prospect*, October 26, 2017, available at http://prospect.org/article/election-security-feds-flounder-while-states-make-strides.

1292 State of Rhode Island, "Rhode Islanders Welcome State-of-the-Art Voting Systems," Press release, July 21, 2016, available at http://www.ri.gov/press/view/28126.

1293 Rob Rock, interview with author, September 7, 2017.

1294 Rob Rock, interview with author, September 7, 2017.

1295 Rob Rock, interview with author, September 7, 2017.

1296 Carney, "On Election Security, Feds Flounder While States Make Strides."

1297 Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

1298 Common Cause, "Rhode Island Takes Important Step to Secure Elections With Post-Election Audits," Press Release, September 20, 2017, available at http://www.commoncause.org/press/press-releases/rhode-island-takes-important-step-to-secure-elections-with-risk-limiting-audits.html.

1299 Personal correspondence from John Marian, Executive Director, Common Cause Rhode Island, October 3, 2017.

1300 H—5704, available at http://webserver.rilin.state.ri.us/BillText/BillText17/HouseText17/H5704A.pdf.

1301 Smith and others, "Counting Votes 2012."

1302 Smith and others, "Counting Votes 2012."

1303 Smith and others, "Counting Votes 2012."

1304 Smith and others, "Counting Votes 2012."

1305 Smith and others, "Counting Votes 2012."

1306 Rob Rock, interview with author, September 7, 2017.

1307 R.I. Gen. Law § 17-19-3 (2016), available at http://webserver.rilin.state.ri.us/Statutes/TITLE17/17-19/17-19-3.HTM.

1308 State of Rhode Island, "Rhode Islanders Welcome State-of-the-Art Voting Systems."

1309 R.I. Gen. Law § 17-19-14 (2016), available at http://law.justia.com/codes/rhode-island/2016/title-17/chapter-17-19/section-17-19-14/.

1310 R.I. Gen. Law § 17-19-14.

1311 R.I. Gen. Law § 17-19-14.

1312 Personal correspondence from Marci Andino, State Elections Director, October 25, 2017.

1313 Survey response from Marci Andino.

1314 Survey response from Marci Andino.

1315 Survey response from Marci Andino.

1316 Survey response from Marci Andino.

1317 Survey response from Marci Andino.

1318 Survey response from Marci Andino.

1319 South Carolina Election Commission, "Poll Managers Handbook" (2016), available at https://www.scvotes.org/files/PMHandbook/SEC%20MNL%201100-201604%20Poll%20Managers%20Handbook.pdf; The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

1320 Survey response from Marci Andino.

1321 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

1322 Personal correspondence from Marci Andino, October 25, 2017.; Sgt. Brad Mincey, "South Carolina National Guard activates first Cyber Protection Battalion," U.S. Army, October 24, 2017.

1323 Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

1324 South Carolina Election Commission, "Election Audits in South Carolina," available at https://www.scvotes.org/election-audits-south-carolina (last accessed January 12, 2017).

1325 According to Marci Andino, State Election Commission Director. Jamie Lovegrove, "South Carolina election agency can withhold cybersecurity documents, attorney general's office says," Post and Courier, December 19, 2017, available at https://www.postandcourier.com/politics/south-carolina-election-agency-can-withhold-cybersecurity-documents-attorney-general/article_f701f432-e4df-11e7-a35f-fb0bb1c8b408.html.

1326 Personal correspondence from Marci Andino, October 25, 2017.

1327 Smith and others, "Counting Votes 2012."

1328 Smith and others, "Counting Votes 2012."

1329 Personal correspondence from Marci Andino, October 25, 2017.

1330 Personal correspondence from Marci Andino, October 25, 2017.

1331 National Conference of State Legislatures, "Electronic Transmission of Ballots"; Survey response from Marci Andino.

1332 SC Code § 7-13-1620 (2016), available at http://www.scstatehouse.gov/code/t07c013.php; Survey response from Marci Andino.

1333 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

1334 Survey response from Marci Andino.

1335 S.C. Code § 7-13-1390 (2016), available at http://www.scstatehouse.gov/code/t07c013.php.

1336 S.C. Code § 7-13-1390; survey response from Marci Andino.

1337 Personal correspondence from Robert A. Litz, Minnehaha County Auditor, October 25, 2017.

1338 Survey response from Robert A. Litz.

1339 Survey response from Robert A. Litz.

1340 One county official told us that he believes this is done at the state level. Personal correspondence from Robert A. Litz, October 25, 2017.

1341 One county official told us that he believes this is done at the state level. Personal correspondence from Robert A. Litz, October 25, 2017.

1342 Survey response from Robert A. Litz.

1343 Survey response from Robert A. Litz.

1344 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books"; S.D. Cod. Law § 12-18-5.

1345 Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

1346 Survey response from Robert A. Litz.

1347 Personal correspondence from Robert A. Litz, October 25, 2017.

1348 Personal correspondence from Robert A. Litz, October 25, 2017.

1349 All mailed ballots are accounted for, as are the number of sent and unreturned ballots. Only ballots returned by 7:00 p.m. on Election Day are ultimately counted. Personal correspondence from Robert A. Litz, October 25, 2017.

1350 Smith and others, "Counting Votes 2012."

1351 Smith and others, "Counting Votes 2012."

1352 S.D. Cod. Law § 12-19-5 (2016), available at http://law.justia.com/codes/south-dakota/2016/title-12/chapter-19/section-12-19-5/.

1353 S.D. Cod. Law § 12-17B-2 (2016), available at http://law.justia.com/codes/south-dakota/2016/title-12/chapter-17b/section-12-17b-2/.

1354 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

1355 S.D. Cod. Law § 12-17B-5 (2016), available at http://law.justia.com/codes/south-dakota/2016/title-12/chapter-17b/section-12-17b-5/.

1356 In Minnehaha County, South Dakota, testing is conducted three times prior to a primary election and twice prior to a general election. There, 10 days advance public notice is required. Survey response from Robert A. Litz; S.D. Cod. Law § 12-17B-5.

1357 S.D. Cod. Law § 12-17B-5.

1358 Norden and Vandewalker, "Securing Elections From Foreign Interference."

1359 Tenn. Code § 2-7-112 (2016), available at http://law.justia.com/codes/tennessee/2016/title-2/chapter-7/section-2-7-112/.

1360 Tenn. Code § 2-7-114 (2016), available at http://law.justia.com/codes/tennessee/2016/title-2/chapter-7/section-2-7-114/; Tenn. Code § 2-7-113 (2016), available at http://law.justia.com/codes/tennessee/2016/title-2/chapter-7/section-2-7-113/; Tenn. Code § 2-9-109 (2016), available at http://law.justia.com/codes/tennessee/2016/title-2/chapter-9/section-2-9-109/; Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

1361 Tenn. Code § 2-20-103 (2016), available at http://law.justia.com/codes/tennessee/2016/title-2/chapter-20/section-2-20-103/.

1362 Verified Voting, "State Audit Laws – Tennessee," March 2017, available at https://www.verifiedvoting.org/state-audit-laws/tennessee/.

1363 Verified Voting, "State Audit Laws – Tennessee."

1364 Tenn. Code § 2-20-103.

1365 "According to the 2000 federal census or any subsequent federal census." Tenn. Code § 2-20-103.

1366 Tenn. Code § 2-20-103.

1367 Tenn. Code § 2-20-103.

1368 Tenn. Code § 2-20-103.

1369 Tenn. Code § 2-20-103.

1370 Tenn. Code § 2-20-103.

1371 Tenn. Code § 2-20-103.

1372 Tenn. Code § 2-20-103.

1373 Tenn. Code § 2-20-103.

1374 Smith and others, "Counting Votes 2012."

1375 Smith and others, "Counting Votes 2012."

1376 Smith and others, "Counting Votes 2012."

1377 Personal correspondence from Mark Goins, Coordinator of Elections, October 30, 2017; Tenn. Code § 2-8-104 (2016), available at https://law.justia.com/codes/tennessee/2016/title-2/chapter-8/section-2-8-104/.

1378 Smith and others, "Counting Votes 2012."

1379 Personal correspondence from Mark Goins, October 30, 2017. Tenn. Code § 2-8-104.

1380 TN H 1310; S 1027, available at https://custom.statenet.com/public/resources.cgi?id=ID:bill:TN2017000H1310&ciq=ncsl15&client_md=e639f9c13b762f51f805eb037916e447&mode=current_text (last accessed January 2018).

1381 Tenn. Code § 2-6-501 (2016), available at http://law.justia.com/codes/tennessee/2016/title-2/chapter-6/part-5/section-2-6-501/; Tenn. Code § 2-6-502 (2016), available at http://law.justia.com/codes/tennessee/2016/title-2/chapter-6/part-5/section-2-6-502/; National Conference of State Legislatures, "Electronic Transmission of Ballots."

1382 Personal correspondence from Mark Goins, October 30, 2017; Tenn. Code § 2-9-117 (2016), available at http://law.justia.com/codes/tennessee/2016/title-2/chapter-9/section-2-9-117/.

1383 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

1384 Tenn. Admin. Law § 1360-2-12-.08, available at http://publications.tnsosfiles.com/rules/1360/1360-02/1360-02-12.pdf.

1385 Tenn. Admin. Law § 1360-02-13-.14, available at http://publications.tnsosfiles.com/rules/1360/1360-02/1360-02-13.20150126.pdf.

1386 Tenn. Admin. Law § 1360-2-12-.08.

1387 Tenn. Admin. Law § 1360-02-13-.14.

1388 Tenn. Admin. Law § 1360-2-12-.08.

1389 Tenn. Admin. Law § 1360-02-13-.14

1390 Norden and Vandewalker, "Securing Elections From Foreign Interference."

1391 Anna M. Tinsley, "Election Security: Officials Say Texas Voter Databases Haven't Been Hacked," *Star Telegram*, October 8, 2016, available at http://www.star-telegram.com/news/politics-government/election/article106950227.html.

1392 Tinsley, "Election Security."

1393 Tinsley, "Election security."

1394 Keith Ingram, Director of Elections and Christina Adkins, Staff Attorney for the Elections Division Legal Section, interview with author, October 4, 2017.

1395 U.S. Election Assistance Commission, "EAC Meeting Moves Election Cybersecurity Protections Forward," Press release, July 27, 2017, available at https://www.eac.gov/news/2017/07/27/eac-meeting-moves-election-cybersecurity-protections-forward/.

1396 According to Bruce High, an IT official in Harris County, "Harris County is working with Homeland Security and the FBI to protect our systems and the information on them." Jmihir Zaveri, "Harris County, Texas, Officials Won't Say Whether Election Systems Were Targeted," *Government Technology*, July 17, 2017, available at http://www.govtech.com/security/Harris-County-Texas-Officials-Wont-Say-Whether-Election-Systems-Were-Targeted.html.

1397 Keith Ingram, interview with author, October 4, 2017.

1398 Travis County has provided training on how to detect and respond to phishing attempts and on "clean computing" best practices. Dana DeBeauvoir, Travis County Election Clerk, interview with author, September 14, 2017.

1399 Texas Code § 63.002 (2015), available at http://law.justia.com/codes/texas/2015/election-code/title-6/chapter-63/; Dana DeBeauvoir, interview with author, September 14, 2017.

1400 Dana DeBeauvoir, interview with author, September 14, 2017.

1401 Personal correspondence with Keith Ingram, December 22, 2017.

1402 Keith Ingram, interview with author, October 4, 2017.

1403 Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

1404 Texas Code § 127.201 (2015), available at http://law.justia.com/codes/texas/2015/election-code/title-8/chapter-127/.

1405 Texas Code § 127.202, available at https://law.justia.com/codes/texas/2015/election-code/title-8/chapter-127/.

1406 Verified Voting, "State Audit Laws – Texas," March 2017, available at https://www.verifiedvoting.org/state-audit-laws/texas/.

1407 Texas Code § 127.201.

1408 Texas Code § 127.201.

1409 Texas Code § 127.202 (2015), available at http://law.justia.com/codes/texas/2015/election-code/title-8/chapter-127/.

1410 Texas Code § 127.201.

1411 Survey response from Dana DeBeauvoir.

1412 Texas Secretary of State, "Election Advisory No. 2012-03," available at http://www.sos.state.tx.us/elections/laws/advisory2012-03.shtml (last accessed October 2017).

1413 The post-election audit is open to candidates and their representatives. Texas Code § 127.201; Personal correspondence from Keith Ingram, November 2, 2017.

1414 Personal correspondence from Dana DeBeauvoir, September 21, 2017.

1415 Texas Code § 127.201.

1416 Verified Voting, "State Audit Laws – Texas."

1417 Personal correspondence from Keith Ingram, December 22, 2017: "Section 65.013 of the Code provides that every presiding judge has to prepare a ballot register to reconcile the total number of ballots received at a polling place, defectively printed ballots, ballots provided to voters, spoiled ballots and unused ballots.Similarly, a reconciliation of votes is expected to be performed by entities using DREs as much as possible with what has been prescribed under state law."

1418 Personal correspondence with Keith Ingram, December 22, 2017; Texas Code § 65.014, available at http://www.statutes.legis.state.tx.us/Docs/EL/htm/EL.65.htm; Texas Code § 65.013, available at http://www.statutes.legis.state.tx.us/Docs/EL/htm/EL.65.htm.

1419 Personal correspondence with Keith Ingram, December 22, 2017.

1420 Smith and others, "Counting Votes 2012."

1421 Personal correspondence from Keith Ingram, December 22, 2017.

1422 Personal correspondence from Keith Ingram, December 22, 2017.; Texas Code § 105.004, available at http://www.statutes.legis.state.tx.us/Docs/EL/htm/EL.105.htm.

1423 Keith Ingram, interview with author, October 4, 2017; Dana DeBeauvoir, interview with author, September 14, 2017.

1424 At least one county is in the process of soliciting bids for new machines. Dana DeBeauvoir, interview with author, September 14, 2017; Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

1425 Texas Code §§ 127.091–127.096 (2015), available at http://law.justia.com/codes/texas/2015/election-code/title-8/chapter-127/; Texas Code § 127.152 (2015), available at http://law.justia.com/codes/texas/2015/election-code/title-8/chapter-127/; Texas Code § 129.023, available at http://www.statutes.legis.state.tx.us/Docs/EL/htm/EL.129.htm.

1426 Texas Code §§ 127.091–127.096, 127.152.

1427 Two additional tests are conducted on machines, once after votes are cast but immediately before counting begins and again immediately after final counting. Texas Code §§ 127.091–127.096, 127.152.

1428 Norden and Vandewalker, "Securing Elections From Foreign Interference."

1429 Personal correspondence from Mark Thomas, Director of Elections, October 27, 2017.

1430 Personal correspondence from Mark Thomas, September 25, 2017.

1431 Personal correspondence from Mark Thomas, September 25, 2017.

1432 Personal correspondence from Mark Thomas, September 25, 2017.

1433 Personal correspondence from Mark Thomas, September 25, 2017.

1434 Survey response from Mark Thomas.

1435 National Conference of State Legislatures, "Electronic Poll Books."

1436 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

1437 Survey response from Mark Thomas.

1438 Personal correspondence from Mark Thomas, September 25, 2017.

1439 Personal correspondence from Mark Thomas, September 25, 2017.

1440 Some counties in Utah are vote-by-mail counties. Utah Code § 20A-5-302 (2016), available at https://le.utah.gov/xcode/Title20A/Chapter5/20A-5-S302.html; Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

1441 Office of the Lieutenant Governor, "Election Policy," October 17, 2006, available at https://www.verifiedvoting.org/wp-content/uploads/2017/03/ElectionX-Policy.pdf.

1442 Verified Voting, "State Audit Laws – Utah," March 2017, available at https://www.verifiedvoting.org/state-audit-laws/utah/.

1443 Office of the Lieutenant Governor, "Election Policy"; personal correspondence from Mark Thomas, October 27, 2017

1444 Verified Voting, "State Audit Laws – Utah."

1445 Ibid.

1446 Survey response from Mark Thomas.

1447 Office of the Lieutenant Governor, "Election Policy."

1448 Personal correspondence from Mark Thomas, October 27, 2017.

1449 Survey response from Mark Thomas.

1450 Personal correspondence from Mark Thomas, October 27, 2017.

1451 "The poll workers, election officers, and other persons may not manually count any votes before delivering the ballots to the counting center." Utah Code § 20A-4-103, available at https://le.utah.gov/xcode/Title20A/Chapter4/20A-4-S103.html?v=C20A-4-S103_1800010118000101; Smith and others, "Counting Votes 2012."

1452 Smith and others, "Counting Votes 2012"; Utah Code § 20A-4-103; Utah Code § 20A-4-102, available at https://le.utah.gov/xcode/Title20A/Chapter4/20A-4-S102.html?v=C20A-4-S102_1800010118000101; Utah Code § 20A-5-404, available at https://le.utah.gov/xcode/Title20A/Chapter5/20A-5-S404.html.

1453 See, for example, County of Salt Lake, "2015 Municipal General Election Statement of Votes Cast," November 17, 2015, available at https://slco.org/clerk/elections/election-results/.

1454 Personal correspondence from Mark Thomas, October 27, 2017.

1455 Personal correspondence from Mark Thomas, October 27, 2017; Utah Code § 20A-4-102.

1456 Smith and others, "Counting Votes 2012."

1457 Smith and others, "Counting Votes 2012."

1458 Smith and others, "Counting Votes 2012."

1459 Personal correspondence from Mark Thomas, October 27, 2017; Utah Code § 20A-4-105, available at https://le.utah.gov/xcode/Title20A/Chapter4/20A-4-S304.html?v=C20A-4-S304_1800010118000101.

1460 Utah Code § 20A-16-404, available at https://le.utah.gov/xcode/Title20A/Chapter16/20A-16-S404.html?v=C20A-16-S404_1800010118000101; National Conference of State Legislatures, "Electronic Transmission of Ballots"; survey response from Mark Thomas.

1461 Utah Code § 20A-5-802, available at https://le.utah.gov/xcode/Title20A/Chapter5/20A-5-S802.html?v=C20A-5-S802_2017050920170509.

1462 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

1463 Survey response from Mark Thomas.

1464 Personal correspondence from Mark Thomas, October 27, 2017.

1465 Personal correspondence from Mark Thomas, October 27, 2017.

1466 In 2015, the state developed new electronic management software, which applies to the statewide voter checklist and campaign finance filings, among other things. Will Senning, Director of Elections and Campaign Finance, and Chris Winters, Deputy Secretary of State, interview with author, September 7, 2017.

1467 Personal correspondence from Will Senning, September 22, 2017.

1468 Personal correspondence from Will Senning, September 22, 2017; Anderson, "Voter Registration Websites for 35 States Are Vulnerable to Voter ID Theft."

1469 Personal correspondence from Will Senning, September 22, 2017..

1470 Will Senning and Chris Winters, interview with author, September 7, 2017.

1471 Personal correspondence from Will Senning, September 22, 2017..

1472 Will Senning and Chris Winters, interview with author, September 7, 2017.

1473 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

1474 Bennett and others, "Cash-strapped states brace for Russian hacking fight."

1475 17 Vt. Stat. § 2481, available at http://legislature.vermont.gov/statutes/section/17/051/02481; 17 Vt. Stat. § 2493, available at http://legislature.vermont.gov/statutes/section/17/051/02493.

1476 17 Vt. Stat. § 2493.

1477 Verified Voting, "State Audit Laws – Vermont," March 2017, available at https://www.verifiedvoting.org/state-audit-laws/vermont/.

1478 Verified Voting, "State Audit Laws – Vermont."

1479 17 Vt. Stat. § 2493.

1480 Will Senning and Chris Winters, interview with author, September 7, 2017.

1481 Will Senning and Chris Winters, interview with author, September 7, 2017.

1482 Personal correspondence from Will Senning, September 22, 2017.

1483 17 Vt. Stat. § 2493; Vermont Secretary of State, "Elections Calendar of Events," November 2016, available at https://www.sec.state.vt.us/elections/elections-calendar-of-events.aspx?month=11&year=2016&page=1.

1484 17 Vt. Stat. § 2493.

1485 Smith and others, "Counting Votes 2012."

1486 Smith and others, "Counting Votes 2012."

1487 Smith and others, "Counting Votes 2012."

1488 Smith and others, "Counting Votes 2012."

1489 Smith and others, "Counting Votes 2012."

1490 National Conference of State Legislatures, "Electronic Transmission of Ballots."

1491 Will Senning and Chris Winters, interview with author, September 7, 2017.

1492 17 Vt. Stat. § 2493; U.S. Election Assistance Commission, "State Requirements and the Federal Voting System Testing and Certification Program"; Will Senning and Chris Winters, interview with author, September 7, 2017.

1493 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

1494 Will Senning and Chris Winters, interview with author, September 7, 2017.

1495 17 Vt. Stat. § 2493.

1496 Personal correspondence from Will Senning, September 22, 2017.

1497 17 Vt. Stat. § 2493; personal correspondence from Will Senning, September 22, 2017.

1498 Norden and Vandewalker, "Securing Elections From Foreign Interference."

1499 Virginia abides by the cybersecurity framework provided by the National Institute of Standards and Technology. Office of the Governor, "Governor McAuliffe Announces Virginia Adopts National Cybersecurity Framework," Press release, February 12, 2014, available at https://governor.virginia.gov/newsroom/newsarticle?articleId=3284; National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity" (2014), available at https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

1500 Edgardo Cortes, Commissioner of Elections, interview with author, October 5, 2017.

1501 See generally, Office of the Governor, "Governor McAuliffe Announces Virginia Adopts National Cybersecurity Framework"; National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity."

1502 The state department of elections partners closely with the state IT agency for IT assistance and for conducting audits and scans to detect system vulnerabilities. Edgardo Cortes, Commissioner of Elections, and Liz Howard, Deputy Commissioner, interview with author, September 12, 2017; Office of the Governor, "Governor McAuliffe Announces Virginia Adopts National Cybersecurity Framework"; National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity."

1503 Edgardo Cortes and Liz Howard, interview with author, September 12, 2017.

1504 Edgardo Cortes and Liz Howard, interview with author, September 12, 2017.

1505 Approximately 24 counties still rely on paper voter registration lists for checking in voters. Edgardo Cortes and Liz Howard, interview with author, September 12, 2017; The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

1506 In counties that do test their poll books, testing typically occurs the weekend before Election Day. Edgardo Cortes and Liz Howard, interview with author, September 12, 2017; The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books.

1507 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

1508 Jason Shueh, "38 Governors Sign Cybersecurity Compact," State Scoop, July 17, 2017, available at http://statescoop.com/38-governors-sign-cybersecurity-compact.

1509 National Governors Associations, "Meet the Threat: States Confront the Cyber Challenge: Memo on State Cybersecurity Response Plans," available at https://ci.nga.org/files/live/sites/ci/files/1617/docs/MemoOnStateCybersecurityResponsePlans.pdf (last accessed July 2017).

1510 Bennett and others, "Cash-strapped states brace for Russian hacking fight."

1511 Bennett and others, "Cash-strapped states brace for Russian hacking fight."

1512 Chalfant, "Virginia Scraps Touchscreen Voting Machines."

1513 Graham Moomaw, "In Emergency Meeting, Virginia Elections Board Votes to Scrap All Touch-Screen Voting Machines," *Richmond Times-Dispatch*, September 8, 2017, available at http://www.richmond.com/news/virginia/government-politics/virginia-elections-board-to-hold-emergency-meeting-to-consider-scrapping/article_61e8030f-bcc2-5e50-aa41-06c12621ec7e.html.

1514 Va. Code § 24.2-671.1 (2016), available at https://law.lis.virginia.gov/vacode/title24.2/chapter6/section24.2-671.1/.

1515 Va. Code § 24.2-671.1.

1516 Va. Code § 24.2-671.1.

1517 Va. Code § 24.2-671.1.

1518 The state department of elections is responsible for setting standards and procedures for the risk-limiting audits, and is looking closely at Colorado's risk-limiting audit procedures as a potential model. Va. Code § 24.2-671.1; Edgardo Cortes and Liz Howard, interview with author, September 12, 2017.

1519 The problems identified by the authors of "Counting Votes 2012"—namely, that the state's precinct-level ballot accounting procedures only applied to optical scan jurisdictions and not DRE jurisdictions—are no longer relevant because the state recently switched over to an entirely paper-based voting system. Smith and others, "Counting Votes 2012."

1520 Smith and others, "Counting Votes 2012."

1521 Smith and others, "Counting Votes 2012."

1522 Smith and others, "Counting Votes 2012."

1523 Smith and others, "Counting Votes 2012."

1524 Smith and others, "Counting Votes 2012."

1525 Edgardo Cortes and Liz Howard, interview with author, September 12, 2017; National Conference of State Legislatures, "Electronic Transmission of Ballots."

1526 Va. Code § 24.2-629 (2016), available at https://law.lis.virginia.gov/vacode/title24.2/chapter6/section24.2-629/; Edgardo Cortes and Liz Howard, interview with author, September 12, 2017.

1527 Several counties purchased new voting machines in 2016 and others—like Manassas County—are currently in the process of purchasing new machines. Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference"; Manassas, Virginia, "New Optical Scanners," available at http://www.manassascity.org/2243/New-Optical-Scanners (last accessed August 2017).

1528 Edgardo Cortes and Liz Howard, interview with author, September 12, 2017.

1529 Edgardo Cortes and Liz Howard, interview with author, September 12, 2017.

1530 Edgardo Cortes and Liz Howard, interview with author, September 12, 2017.

1531 Norden and Vandewalker, "Securing Elections From Foreign Interference."

1532 Washington Secretary of State, "System Security," available at https://www.sos.wa.gov/elections/System-Security.aspx (last accessed October 2017).

1533 Washington Secretary of State, "System Security."

1534 Washington Secretary of State, "System Security."

1535 Washington Secretary of State, "System Security."

1536 Washington Secretary of State, "System Security."

1537 Survey response from Stuart Holmes, Voting Information Systems Manager.

1538 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

1539 Bennett and others, "Cash-strapped states brace for Russian hacking fight."

1540 Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

1541 Wash. Rev. Code § 29A.60.095 (2016), available at http://law.justia.com/codes/washington/2016/title-29a/chapter-29a.60/section-29a.60.095/; Wash. Rev. Code § 29A.12.150 (2016), available at http://law.justia.com/codes/washington/2016/title-29a/chapter-29a.12/section-29a.12.150/; Wash. Rev. Code § 29A.12.085 (2016), available at http://law.justia.com/codes/washington/2016/title-29a/chapter-29a.12/section-29a.12.085/; Wash. Admin. Code § 434-335-040, available at http://apps.leg.wa.gov/wac/default.aspx?cite=434-335-040; Verified Voting, "State Audit Laws – Washington," March 2017, available at https://www.verifiedvoting.org/state-audit-laws/washington/.

1542 Wash. Rev. Code § 29A.60.185 (2016), available at http://law.justia.com/codes/washington/2016/title-29a/chapter-29a.60/section-29a.60.185/.

1543 Wash. Rev. Code § 29A.60.185.

1544 Wash. Rev. Code § 29A.60.185.

1545 Wash. Rev. Code § 29A.60.185; Wash. Admin. Code § 434-262-105, available at http://apps.leg.wa.gov/wac/default.aspx?cite=434-262-105.

1546 Wash. Admin. Code § 434-262-105.

1547 Personal correspondence from Stuart Holmes, November 16, 2017; Wash. Admin. Code § 434-262-105.

1548 Wash. Rev. Code § 29A.60.170 (2016), available at http://law.justia.com/codes/washington/2016/title-29a/chapter-29a.60/section-29a.60.170/.

1549 Wash. Rev. Code § 29A.60.170.

1550 Wash. Rev. Code § 29A.60.170.

1551 Wash. Rev. Code § 29A.60.170.

1552 Wash. Rev. Code § 29A.60.170; Wash. Admin. Code § 434-261-108, available at http://apps.leg.wa.gov/wac/default.aspx?cite=434-261-108.

1553 Survey response from Stuart Holmes.

1554 Aside from the mandatory and voluntary audits mentioned above, the state requires a full recount of both paper ballots and DRE machine output if the margin of victory between the candidates is less than 0.5 percent and fewer than 2,000 votes. Similarly, if the margin of victory on a statewide measure is less than 0.5 percent and fewer than 2,000 votes, a recount of both paper ballots and DRE machine output is required. In a statewide race or measure, if the difference of the margin of victory between the candidates or responses is less than 0.25 percent and fewer than 1,000 votes, a manual recount of paper ballots and DRE machine output is required. For all other races, if the margin of victory between the candidates is fewer than 150 votes and 0.25 percent, a manual recount of paper ballots and DRE machine output is required. Wash. Rev. Code § 29A.60.170; Personal correspondence Email from Stuart Holmes, November 16, 2017.

1555 WA S 6202, available at https://custom.statenet.com/public/resources.cgi?id=ID:bill:WA2017000S6202&ciq=ncsl15&client_md=61e3682eaf9204554ccfcb7923e266eb&mode=current_text (last accessed January 2018).

1556 Wash. Admin. Code § 434-262-105.

1557 Wash. Admin. Code § 434-262-105.

1558 Smith and others, "Counting Votes 2012."

1559 Personal correspondence from Stuart Holmes, November 3, 2017.

1560 Smith and others, "Counting Votes 2012."

1561 Smith and others, "Counting Votes 2012."

1562 Smith and others, "Counting Votes 2012."

1563 Personal correspondence from Stuart Holmes, November 3, 2017.

1564 Smith and others, "Counting Votes 2012."

1565 Smith and others, "Counting Votes 2012."

1566 National Conference of State Legislatures, "Electronic Transmission of Ballots."

1567 Survey response from Stuart Holmes.

1568 Wash. Admin. Code § 434-335-040; Wash. Admin. Code § 434.335.010, available at http://apps.leg.wa.gov/wac/default.aspx?cite=434-335-010; Wash. Admin. Code § 434-235-030, available at http://apps.leg.wa.gov/wac/default.aspx?cite=434-335-030.

1569 Survey response from Stuart Holmes; Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

1570 Personal correspondence from Stuart Holmes, November 3, 2017.

1571 Personal correspondence from Stuart Holmes, November 3, 2017.

1572 WA H 2388, available at https://custom.statenet.com/public/resources.cgi?id=ID:bill:WA2017000H2388&ciq=ncsl15&client_md=ea6570e2275e01ce1f858aa77b3efd0b&mode=current_text (last accessed January 2018).

1573 Wash. Rev. Code § 29A.12.130 (2016), available at http://law.justia.com/codes/washington/2016/title-29a/chapter-29a.12/section-29a.12.130/; Wash. Admin. Code § 434-335-520, available at http://apps.leg.wa.gov/wac/default.aspx?cite=434-335-520; Wash. Admin. Code § 434-335-550, available at http://apps.leg.wa.gov/wac/default.aspx?cite=434-335-550; Wash. Admin. Code § 434-335-560, available at http://apps.leg.wa.gov/wac/default.aspx?cite=434-335-560.

1574 Personal correspondence from Stuart Holmes, November 3, 2017..

1575 Wash. Rev. Code § 29A.12.130; WA Admin. Code §§ 434-335-520, 434-335-550, 434-335-560.

1576 Norden and Vandewalker, "Securing Elections From Foreign Interference."

1577 Personal correspondence from Brittany Westfall, Statewide Voter Registration System Coordinator, October 4, 2017.

1578 Anderson, "Voter Registration Websites for 35 States Are Vulnerable to Voter ID Theft."

1579 Personal correspondence from Brittany Westfall, October 4, 3017.

1580 Chuck Flannery, Deputy Secretary of State, Brittany Westfall, Statewide Voter Registration System Coordinator, and Donald Kersey, Deputy Legal Counsel, interview with author, September 8, 2017.

1581 Chuck Flannery, Brittany Westfall, and Donald Kersey, interview with author, September 8, 2017.

1582 W.Va. Code § 3-4A-17 (2016), available at http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=03&art=4a&section=17; W.Va. Code § 3-4A-13 (2016), available at http://law.justia.com/codes/west-virginia/2016/chapter-3/article-4a/section-3-4a-13/; The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

1583 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

1584 W.Va. Code § 3-4A-17; The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

1585 According to assistant communications director Steven Allen Adams, "When we began crafting the position description, it became apparent that the best fit would be someone with security clearance, and access to tools and intelligence … Since we were going to continue seeking the help of the Guard's expertise in monitoring and securing the elections space, it was decided that hiring a member of the Guard through Military Authority was the logical step." Doug Chapin, "ElectionlineWeekly On Partnership Between West Virginia SoS, Air National Guard," Election ACA, October 13, 2017, available at http://editions.lib.umn.edu/electionacademy/2017/10/13/electionlineweekly-on-partnership-between-west-virginia-sos-air-national-guard/.

1586 W.Va. Code § 3-4A-9 (2016), available at http://law.justia.com/codes/west-virginia/2016/chapter-3/article-4a/section-3-4a-9/; Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

1587 W.Va. Code § 3-4A-28 (2016), available at http://law.justia.com/codes/west-virginia/2016/chapter-3/article-4a/section-3-4a-28/; Verified Voting, "State Audit Laws – West Virginia," March 2017, available at https://www.verifiedvoting.org/state-audit-laws/west%20virginia/.

1588 W.Va. Code § 3-4A-28.

1589 Ibid.

1590 Chuck Flannery, Brittany Westfall, and Donald Kersey, interview with author, September 8, 2017.

1591 W.Va. Code § 3-4A-28.

1592 W.Va. Code § 3-4A-28' W.Va. Code § 3-4A-27 (2016), available at https://law.justia.com/codes/west-virginia/2016/chapter-3/article-4a/section-3-4a-27/; Verified Voting, "State Audit Laws - West Virginia," available at; West Virginia Secretary of State's Office, "2016 Best Practices Guide for Canvass and Recount" (2016), available at https://www.eac.gov/assets/1/28/2016%20Canvassing%20and%20Recount%20Manual.pdf.

1593 W.Va. Code § 3-4A-28.

1594 W.Va. Code § 3-4A-28.

1595 Smith and others, "Counting Votes 2012."

1596 Smith and others, "Counting Votes 2012."

1597 Smith and others, "Counting Votes 2012."

1598 Smith and others, "Counting Votes 2012."

1599 Smith and others, "Counting Votes 2012."

1600 Smith and others, "Counting Votes 2012."

1601 Chuck Flannery, Brittany Westfall, and Donald Kersey, interview with author, September 8, 2017; W.Va. Code § 3-3-5 (2016), available at http://law.justia.com/codes/west-virginia/2016/chapter-3/article-3/section-3-3-5/; National Conference of State Legislatures, "Electronic Transmission of Ballots."

1602 W.Va. Code § 3-4A-8 (2016), available at http://law.justia.com/codes/west-virginia/2016/chapter-3/article-4a/section-3-4a-8/; Chuck Flannery, Brittany Westfall, and Donald Kersey, interview with author, September 8, 2017.

1603 Local election officials are reportedly looking at purchasing new machines for future elections. Chuck Flannery, Brittany Westfall, and Donald Kersey, interview with author, September 8, 2017; Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

1604 W.Va. Code § 3-4A-8.

1605 Chuck Flannery, Brittany Westfall, and Donald Kersey, interview with author, September 8, 2017; W.Va. Code § 3-4A-26 (2016), available at http://law.justia.com/codes/west-virginia/2016/chapter-3/article-4a/section-3-4a-26/; W.Va. Code § 3-4A-13 (2016), available at https://law.justia.com/codes/west-virginia/2016/chapter-3/article-4a/section-3-4a-13/.

1606 W.Va. Code § 3-4A-26; W.Va. Code § 3-4A-13.

1607 W.Va. Code § 3-4A-26; W.Va. Code § 3-4A-13.

1608 Survey response from Michael Haas, Administrator, Wisconsin Elections Commission.

1609 State of Wisconsin, Department of Administration, "State of Wisconsin: Cybersecurity Strategy" (2017), available at https://det.wi.gov/Documents/Cybersecurity%20Strategy%202017.pdf.

1610 Michael Haas, interview with author, October 5, 2017.

1611 State of Wisconsin, Department of Administration, "State of Wisconsin."

1612 State of Wisconsin, Department of Administration, "State of Wisconsin."

1613 Michael Haas, interview with author, October 5, 2017.

1614 Survey response from Michael Haas.

1615 Survey response from Michael Haas.

1616 Wis. Stat. § 6.79 (2016), available at https://docs.legis.wisconsin.gov/statutes/statutes/6/III/79rict; survey response from Michael Haas.

1617 Survey response from Michael Haas.

1618 Michael Haas, Administrator, Wisconsin Elections Commission, Richard Rydecki, Elections Supervisor, and Meagan Wolfe, assistant administrator of the Wisconsin Elections Commission, interview with author, September 7, 2017.

1619 Survey response from Michael Haas.

1620 Wisconsin Elections Commission, "Voting Equipment Use by Wisconsin Municipalities," 2017, available at http://elections.wi.gov/elections-voting/voting-equipment/voting-equipment-use; Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

1621 Wis. Stat. § 7.08(6) (2016), available at https://docs.legis.wisconsin.gov/statutes/statutes/7.

1622 Government Accounting Board, "Voting System Audit Requirements," available at http://elections.wi.gov/sites/default/files/memo/162/voting_system_audit_requirements_pdf_14275.pdf (last accessed October 2017).

1623 Verified Voting, "State Audit Laws – Wisconsin," March 2017, available at https://www.verifiedvoting.org/state-audit-laws/wisconsin/.

1624 Government Accounting Board, "Voting System Audit Requirements."

1625 Ibid.

1626 Survey response from Michael Haas.

1627 Survey response from Michael Haas.

1628 Government Accounting Board, "Voting System Audit Requirements."

1629 Michael Haas, Richard Rydecki, and Meagan Wolfe, interview with author, September 7, 2017; Survey response from Michael Haas.

1630 Michael Haas, Richard Rydecki, and Meagan Wolfe, interview with author, September 7, 2017.

1631 Michael Haas, Richard Rydecki, and Meagan Wolfe, interview with author, September 7, 2017.

1632 State law does permit election officials to revisit certification of voting equipment based on the results of an audit. Personal correspondence from Michael Haas, November 15, 2017.

1633 Michael Haas, Richard Rydecki, and Meagan Wolfe, interview with author, September 7, 2017.

1634 Smith and others, "Counting Votes 2012."

1635 Smith and others, "Counting Votes 2012."

1636 Smith and others, "Counting Votes 2012."

1637 Personal correspondence from Michael Haas, November 15, 2017.

1638 Smith and others, "Counting Votes 2012."

1639 Personal correspondence from Michael Haas, November 15, 2017.

1640 Smith and others, "Counting Votes 2012."

1641 Personal correspondence from Michael Haas, November 15, 2017..

1642 Personal correspondence from Michael Haas, November 15, 2017.

1643 National Conference of State Legislatures, "Electronic Transmission of Ballots."

1644 Wis. Stat. § 7.01(1)(e) (2016), available at https://docs.legis.wisconsin.gov/code/admin_code/el/7; survey response from Michael Haas.

1645 Survey response from Michael Haas.

1646 Norden and Vandewalker, "Securing Elections From Foreign Interference."

1647 Wis. Stat. § 5.84 (2016), available at https://docs.legis.wisconsin.gov/statutes/statutes/5/III/84/.

1648 Wis. Stat. § 5.84.

1649 Wis. Stat. § 5.84.

1650 Norden and Vandewalker, "Securing Elections From Foreign Interference."

1651 16 Wyo. Admin. Code § 002.0005.16.10222013, available at https://rules.wyo.gov/Search.aspx; survey response from Debra Lee, Laramie County Clerk.

1652 Survey response from Debra Lee.

1653 The computer used from the remote location must have current anti-virus software installed. 16 Wyo. Admin. Code § 002.0005.16.10222013; survey response from Debra Lee.

1654 Survey response from Debra Lee.

1655 Personal correspondence from Kai Schon, State Election Director, November 6, 2017.

1656 Survey response from Debra Lee.

1657 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books"; National Conference of State Legislatures, "Electronic Poll Books."

1658 The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books."

1659 Although the Pew Charitable Trusts lists Wyoming as one of those states that makes paper voter registration lists available at all polling places that use electronic poll books, at least one county told us that they do not have backup paper voter registration lists available on Election Day. The Pew Charitable Trusts, "A Look at How—and How Many—States Adopt Electronic Poll Books"; survey response from Debra Lee.

1660 Personal correspondence from Kai Schon, November 6, 2017.

1661 16 Wyo. Admin. Code § 002.0005.16.10222013; survey response from Debra Lee.

1662 9 Wyo. Admin. Code § 002.0005.9.10222013, available at https://rules.wyo.gov/Search.aspx; 8 Wyo. Admin. Code § 002.0005.8.10222013, available at https://rules.wyo.gov/Search.aspx; Verified Voting, "The Verifier—Polling Place Equipment—November 2016."

1663 Wyo. Stat. § 22-11-109 (2016), available at http://soswy.state.wy.us/Forms/Publications/2017ElectionCode.pdf.

1664 Smith and others, "Counting Votes 2012"; 13 Wyo. Admin. Code § 002.0005.13.12152009, available at https://rules.wyo.gov/Search.aspx.

1665 Smith and others, "Counting Votes 2012."

1666 Smith and others, "Counting Votes 2012."

1667 Smith and others, "Counting Votes 2012."

1668 Smith and others, "Counting Votes 2012."

1669 3 Wyo. Admin. Code § 002.0005.3.10222013, available at https://rules.wyo.gov/Search.aspx; National Conference of State Legislatures, "Electronic Transmission of Ballots."

1670 In addition, Wyoming also requires the voting machine to have been tested, used, and certified under standards separately adopted and implemented in at least two states for use in federal elections in those states. 12 Wyo. Admin. Code § 002.0005.12.10222013, available at https://rules.wyo.gov/Search.aspx; survey response from Debra Lee.

1671 Norden and Famighetti, "America's Voting Machines at Risk"; Norden and Vandewalker, "Securing Elections From Foreign Interference."

1672 Survey response from Debra Lee.

1673 Wyo. Stat. § 22-10-108 (2016), available at http://soswy.state.wy.us/Forms/Publications/2017ElectionCode.pdf.

1674 Notice must be provided to the county chairman of each political party and each independent candidate. However, the law does not require that the general public be notified of testing. Wyo. Stat. § 22-10-108.

1675 Wyo. Stat. § 22-10-108; 9 Wyo. Admin. Code § 002.0005.9.10222013; 8 Wyo. Admin. Code § 002.0005.8.10222013.

Our Mission

The Center for American Progress is an independent, nonpartisan policy institute that is dedicated to improving the lives of all Americans, through bold, progressive ideas, as well as strong leadership and concerted action. Our aim is not just to change the conversation, but to change the country.

Our Values

As progressives, we believe America should be a land of boundless opportunity, where people can climb the ladder of economic mobility. We believe we owe it to future generations to protect the planet and promote peace and shared global prosperity.

And we believe an effective government can earn the trust of the American people, champion the common good over narrow self-interest, and harness the strength of our diversity.

Our Approach

We develop new policy ideas, challenge the media to cover the issues that truly matter, and shape the national debate. With policy teams in major issue areas, American Progress can think creatively at the cross-section of traditional boundaries to develop ideas for policymakers that lead to real change. By employing an extensive communications and outreach effort that we adapt to a rapidly changing media landscape, we move our ideas aggressively in the national policy debate.

Center for American Progress

1333 H STREET, NW, 10TH FLOOR, WASHINGTON, DC 20005 • TEL: 202-682-1611 • FAX: 202-682-1867 • WWW.AMERICANPROGRESS.ORG