Michigan Election Security Advisory Commission

Report and Recommendations

October 2020

Contents

Membership[1]

Tripp Adams, Michigan chapter lead for the Truman National Security Project

Tina Barton, Rochester Hills city clerk

David Becker (co-chair), executive director and founder of the nonprofit Center for Election Innovation & Research

Barb Byrum, Ingham County clerk.

Richard DeMillo, Charlotte B. and Roger C. Warren professor of computer science at Georgia Tech

Chris DeRusha, chief security officer for the state of Michigan

Joshua M. Franklin, president and co-founder of OutStack Technologies

Cathy M. Garrett, Wayne County clerk

J. Alex Halderman (co-chair), professor of computer science and engineering at the University of Michigan and director of the university's Center for Computer Security and Society.

Liz Howard, election security counsel with the Democracy Program at the Brennan Center for Justice

Rachel Huddleston, publications/communications associate for Michigan Protection & Advocacy Service, Inc. in Lansing.

Matthew V. Masterson (non-voting liaison), senior cybersecurity advisor, Office of Cybersecurity and Communications, U.S. Department of Homeland Security.

Walter R. Mebane Jr., professor of political science and statistics at the University of Michigan.

Jennifer Morrell, former election official in Utah and Colorado

Tim Snow, Kalamazoo county clerk and register of deeds

Maurice Turner, senior technologist at the Center for Democracy & Technology.

Dan Wallach, professor of computer science and Rice Scholar at the Baker Institute for Public Policy at Rice University

Wayne Williams, former Colorado secretary of state and former El Paso county clerk and recorder

[1] Chris DeRusha participated in the Advisory Commission in his capacity as chief security officer for the state of Michigan. He has since left that position.

Introduction

Secretary of State Jocelyn Benson convened the Election Security Advisory Commission in March 2019. The Advisory Commission's mandate is to develop a list of election security best practices and reforms and strategies to ensure the security of elections in Michigan. The group's membership includes election officials, voting and election experts, computer and data scientists, and IT and security professionals. Its work is funded through a federal grant for election security.

The Advisory Commission met four times:

April 16, 2019 in Ann Arbor
June 17, 2019 in Kalamazoo
July 29, 2019 in Detroit
October 16, 2019 in Grand Rapids

The Advisory Commission also held public hearings at its Detroit and Grand Rapids meetings. A subgroup focusing on risk-limiting audits also met twice by teleconference. The Secretary of State immediately began to address concerns and preliminary recommendations that were discussed at the Commission's meetings, and such progress is recognized throughout this document.

These recommendations are based on committee meetings that took place in 2019 and do not specifically address the ongoing COVID-19 pandemic.

Background

Following the 2016 Presidential Election, intelligence, law enforcement, and national security agencies reported on efforts by foreign-government-aligned entities to interfere in U.S. elections through cyberattacks, disinformation campaigns, and other methods. Although the extent of foreign interference represented a new type of threat to election security, this was not the first time that concerns had been raised about vulnerabilities in election security in the United States.

State elections are run with a patchwork of physical, technological, and human infrastructure, all with potential weaknesses that if left unaddressed could undermine the integrity of the election system and confidence of the electorate. Elements that must be safeguarded from attack range from the physical equipment used to cast and count ballots, to the databases in which voter records are kept, to the voters themselves, who can fall victim to false information and manipulation designed to sow confusion and discord in the election process.

In response to these threats, progress has been made to better defend American elections. A large majority of votes nationwide are now cast using paper ballots, reducing the potential for votes to be altered or lost in a cyberattack. Increased cooperation across levels of government, and between government officials and civil society, has led to better coordination and information sharing. Federal funding has helped states make key upgrades and investments.

Michigan has made significant advances in election security that create an excellent foundation for further improvements. In the most recent round of voting machines purchases, all counties in Michigan acquired new paper-based voting equipment, including optical scanners and ballot-marking devices. The state also upgraded the Qualified Voter File computer system, which houses the voter registration database and other management election management functions.

Proposal 2018-3, enacted by ballot initiative in the November 2018 election, amended the Michigan Constitution to provide several new rights for Michigan voters, including the right to greater election security. Specifically, Article II, Section 4 of the Michigan Constitution now grants the right to have results of statewide elections audited.

Still, there is general recognition that more progress must be made to counter emerging threats. The Election Security Advisory Commission recommendations in this regard cover a broad range of issues affecting Michigan's election system.

A. Voter Registration and IT Security

The Advisory Commission discussed a set of issues related to the security of Michigan's voter registration database, the Qualified Voter File (QVF). The QVF is maintained at the state level by the Secretary of State, and it is used by officials in Michigan's 1,520 local and 83 county election jurisdictions to maintain voter records and manage elections.

Accordingly, the QVF is one of the most critical aspects of Michigan's election security. This is especially true given that voter registration databases were a focus of the 2016 Russian attacks against election infrastructure. The Senate Intelligence Committee has reported that attackers directed by the Russian actors likely conducted research on election systems in all 50 states, including targeting voter registration systems in some states, and that, in at least one state, the attackers gained access to the database and had the technical ability to alter or delete registration data.

No investigations have concluded that voter records were changed in the Russian attacks, but they demonstrate the potential threat. If attackers were to gain access to Michigan's voter registration database or management software, they could cancel or alter voter registration records in an attempt to severely disrupt election administration processes. Although Michigan's QVF has recently undergone software and security upgrades, the Advisory Commission recommends further improvements to the system.

1. Prioritize implementation of multifactor authentication

Multifactor authentication (MFA) is a crucial defense against unauthorized access to databases. If a bad actor obtains a user's credentials through a phishing attack or other means, MFA makes it considerably more difficult to use those credentials to log into the system.

MFA requires a user to authenticate through two or more different methods, so that a password alone is insufficient to gain access. Even if attackers were to steal a user's password, they would still be unable to access the system without an additional factor – for example, a code sent to the authorized user's mobile phone or physical access to a specific USB security key.

The Advisory Commission strongly recommends prioritizing MFA implementation and completing it as soon as possible. The Advisory Commission also recommends exploring MFA methods that do not rely on cell phone access, such as security tokens that can serve as a second authentication factor. These devices provide even stronger protection than codes sent to a cell phone.

In response to the Commission's initial comments at hearings, the Secretary of State began implementing MFA for QVF prior to the March 2020 presidential primary election with state users and pilot local jurisdictions. The current implementation of MFA uses a One Time Password (OTP) authenticator application on smart phones which does not require cellphone communication and is similar in security to a USB based token. Implementation will continue to expand across local jurisdictions until full implementation. The primary challenge for implementation will be acclimating local clerks to using MFA, given their varying levels of technical experience with secondary devices used for authentication.

2. Evaluate user access to ensure appropriate number of users and levels of permissions

Because elections are run primarily at the city or township level, with county officials also maintaining critical election functions, QVF users are spread throughout the state at all levels of government. Currently, more than 3,000 users in 1,520 municipal jurisdictions, 83 county jurisdictions, and the state level have access to QVF. These users have differing levels of access based on their jurisdiction and the needs of their role. The high number of users also means there is significant churn among the user base as some election officials and staff leave their jobs and others are hired.

The Advisory Commission discussed the Secretary of State's approach to designating and updating user access to the QVF.

The Advisory Commission recommends that the Secretary of State regularly monitor user activity and conduct periodic review and audit of user access, permissions, and activity to ensure that QVF users have only the necessary level of access and are using it appropriately, and that unneeded accounts are disabled promptly.

3. Expand monitoring of suspicious activities

Improperly controlled access to the QVF or other state, county, or local government networks may allow access to malicious actors, which poses a threat to election infrastructure, and the sooner anomalous activity can be identified or contained, the better the chance of preventing or mitigating damage. The Advisory Commission discussed tools to detect and identify threats that could lead to corruption or manipulation of voter registration information or other election data.

The Advisory Commission recommends that the Secretary of State expand efforts to monitor voter registration data for anomalous changes or patterns of changes, and ensure they are explained. Currently the Secretary of State periodically monitors QVF use, and the Secretary of State is also working with the Vote Shield program, which monitors public voter registration data to identify anomalous changes or trends to voter registration data after the fact. The Advisory Commission recommends building on these tools to more regularly monitor voter registration changes in a comprehensive, systematic, and real-time fashion. Additionally, the Secretary of State should continue to participate in the ERIC Electronic Registration Information Center (ERIC) to ensure cross-state voter data reports are available.

The Advisory Commission recommends that the Secretary of State continue its current practice of creating frequent backups of registration data. Backups provide a defense against unauthorized modification of the database and against threats such as ransomware that could make the system unavailable. Backups should be created as frequently as feasible, encompass as much data and code as feasible, and be regularly stored securely offline and tested to ensure they are retrievable if needed. Backups must be done in a way that ensures registration files can be restored in the event of a disruption.

The Advisory Commission also recommends the use of network and endpoint-based threat detection software. Through partnership with the Department of Technology, Management and Budget (DTMB), Michigan State Police (MSP), and others, the state already has extensive data-monitoring at the state level. At the county and local level, there is significantly less uniformity in data monitoring.

The Advisory Commission recommends that the Secretary of State find ways to extend data monitoring and threat detection to local jurisdictions, beginning at the county level. Neighboring states provide useful models in exploring this technology; Indiana has made commercial security tools available to county

governments. Illinois has established a cyber navigator program to assist local jurisdictions in creating defenses and responding to cyber threats.

The Advisory Commission recommends that security staff for the Secretary of State share information, coordinate effort, strengthen federal partnerships, and otherwise work with counterparts across county and local governments to determine the most effective means of improving IT security through the deployment of election security resources, including federal election security grant funding.[2]

4. Cultivate mature software engineering security practices

The Advisory Commission discussed additional methods by which the Secretary of State could test and improve data security infrastructure on an ongoing basis. The Commission identified several opportunities for improvement.

a. ***Regularly perform source code security audits or reviews, and penetration testing.*** *The Advisory Commission recommends that the Secretary of State commission both source code security audits and penetration testing on a frequent and regular basis, at a minimum annually.*

The state has in the past commissioned a vendor to conduct some penetration testing, but not on a regular schedule. The Advisory Commission recommends that the Secretary of State conduct additional testing, do so at regular intervals, and prioritize fixing any issues discovered during such audits and testing.

b. ***Maximize leverage of resources from federal and state partners, civil society, and industry.*** *The Advisory Commission recommends that the Secretary of State build on existing relationships to expand security infrastructure testing and*

[2] *See* Department of Homeland Security, "Election Infrastructure Security Funding Considerations" (June 2018), https://www.dhs.gov/sites/default/files/publications/Election%20Infrastructure%20Security%20Funding%20Considerations%20Final.pdf.

evaluation. To the extent additional partnerships are needed, the Secretary of State should work to establish them.

Currently, the Secretary of State and DTMB hold regular meetings with the Michigan State Police and federal agencies. The MSP has an advanced cybersecurity agency that constantly communicates security information to state partners.

The Secretary of State should fully leverage federal resources, including capacity to conduct additional exercises (such as tabletop and phishing exercises), security testing and data sharing, to supplement MSP resources.

The Advisory Commission also recommends maximizing civil society, academic, and industry resources to the extent possible, including through existing relationships with non-profit and for-profit security groups.

c. ***Publicly post a security point-of-contact for vulnerability reports from outside entities***. Currently there is no specific contact point for individuals who identify security concerns with election infrastructure to report their findings. Accordingly, security experts and "white hat" hackers do not necessarily have an avenue to share their findings expeditiously (and, where necessary, with the appropriate degree of confidentiality).

The Advisory Commission recommends the establishment of an election-specific point of contact for reporting election security vulnerabilities. This could include specific personnel designated as a point of contact; publicly posting a reporting tool; and creating specific phone, e-mail, or web contact information.

Currently, models for identifying and submitting security vulnerabilities exist through the partnership between Michigan Cyber Command and MiC3, the

Michigan Civilian Cyber Corps. A Cyber 211 program in which reports can be filed is also being piloted in West Michigan.

5. Expand security training and requirements for election officials and other QVF users

Currently, QVF users must complete security training and accreditation prior to using the system. After users are accredited, they can access continuing training and information materials electronically, but they are not required to undergo ongoing training. Since local election officials are not under the direct supervision of the Secretary of State, the state's ability to ensure compliance with state practices regarding QVF is generally limited to conditioning use on such compliance.

The Advisory Commission recommends that the Secretary of State explore conditioning access to the Qualified Voter File on the completion of ongoing security training and exercises. For example, the Secretary of State could require as a condition of using QVF that users agree to undergo additional training as needed, or to be subject to simulated phishing attempts and other security exercises. The QVF user agreement could also require that users agree to comply with security practices as designated by the Secretary of State. The Secretary should also condition election technology grants on completion of required security curricula.

The Advisory Commission also recommends building education about security best practices into training that the Secretary of State provides to clerks for other election administration purposes. Recommended subjects include information on good password, authentication, and cyber-hygiene practices, maintaining end-point security, and resisting common social-engineering techniques such as phishing.

6. Ensure voter registration databases and systems are well secured

Under Proposal 2018-3, along with legislation passed in 2018, several methods of voter registration are now available, including automatic voter registration as a result of driver's license transactions, online voter registration, and registration on Election Day at city and township clerks' offices.

The Advisory Commission recommends that the Secretary of State review each new form of registration to ensure they do not create security vulnerabilities, such as by creating data vulnerabilities or failing to adequately authenticate the voter. This assessment should include a full review of data inputs and outputs for the QVF to ensure that proper access controls and security protocols are in place. Many of the other recommendations in this section, such as software engineering security practices, should also be applied to these new registration methods.

7. Contain failures and maintain resilience through procedural fail-safes

Michigan's election system makes heavy use of computerized equipment on and surrounding Election Day. All levels of government distribute information via websites. City and township clerks manage voter registration tasks, including same-day registration and absentee ballot issuance, using the QVF. Precincts use electronic pollbooks to sign voters in and issue ballots, provide electronic ballot marking devices for voters who need or request them, and use computerized optical scanners to count paper ballots.

Optical scanners in some jurisdictions are connected to the Internet or to cellular networks after tabulation, exposing them to potential election-day cyberattacks. There is also the possibility of disruption due to power outages, software problems, or other issues that interfere with the ordinary operation of electronic equipment on Election Day.

The Advisory Commission recommends that clerk offices and polling places ensure they have sufficient written plans to continue to run the election if the computerized equipment malfunctions, including continuity of operations and cyber incident response plans. These plans should be reviewed and exercised prior to each election. Contingency plans should be shared with the public in order to support confidence.

All equipment, including ballot marking devices, should be carefully tested prior to the opening of polls. Election inspector resources should be allocated to assist voters with disabilities if accessible devices for those voters fail. Clerks should have backup paper pollbooks prepared in advance in case electronic pollbooks are not functioning on Election Day. These pollbooks should always be delivered to the polling locations with all other Election Day materials. Procedures should be in place to securely store paper ballots and tabulate them later in case the optical scanners fail.

Polling places should have ample emergency and provisional ballots available in the event that the voter registration list has been corrupted. Provisional envelope ballots should be used only as a last resort if a voter's registration status cannot be resolved with the city or township clerk.

Staffing should be adequate to allow each polling place to continue running efficiently, and avoid excessively long waits for voters, even if the electronic poll books or optical scanners are not working.

B. Post-Election Audits

Proposal 2018-3 grants Michigan voters the right to have election results audited. Post-election audits review the records of an election to identify errors and verify that proper procedures were followed or that outcomes were correct.

Currently, two types of audits are conducted in Michigan: procedural audits, which verify whether jurisdictions properly followed election procedures, and tabulation audits, in which all ballots are recounted by hand in randomly selected precincts to verify that votes were recorded correctly. Neither of these auditing procedures currently results in a statewide review of ballots to determine whether all ballots were counted properly; currently, the only method available to fully verify the outcome is a hand recount.

Michigan began piloting Risk-Limiting Audits (RLA) in 2018. RLAs, which have been used extensively in Colorado and are being introduced in other states, are audits that examine a sufficient number of paper ballots to confirm the reported outcome of an election. An RLA inspects enough ballots to ensure that the chance that the reported outcome differs from the outcome that would be reported by a full hand-count is lower than a pre-determined probability called the "risk limit." In most cases, an RLA requires only a small number of ballots to be inspected, but when election results are close, more ballots need to be examined to meet the risk limit. Progressively more ballots are audited until either the reported outcome is confirmed to within the risk limit or it is demonstrated to be incorrect. RLAs provides strong evidence to support confidence in election outcomes, and they will never invalidate a correctly reported result.

Michigan conducted RLA pilots beginning in 2019 and culminating in a successful state-wide pilot following the 2020 presidential primary election.

1. Implement risk-limiting audits as a cybersecurity defense

The Advisory Commission recommends that Michigan conduct statewide risk-limiting audits as soon as it is logistically feasible to do so. The Commission determined that risk-limiting audits, if implemented rigorously, can provide a robust defense against fraud, create a deterrent against cyberattacks on the state's election infrastructure, and improve voter confidence.

A voter-verified paper trail is necessary for RLAs, and Michigan already has individual hand-marked or voter-verifiable paper records of every vote. Paper ballots are a best practice in election security, and the Advisory Commission commends their use and strongly recommends that the state continue to use them.

As part of the further adoption of RLAs, the Advisory Commission recommends that the state provide a standard definition of what an RLA is and what it seeks to accomplish. The Advisory Commission recommends the starting-point definition, "a procedure that guarantees an acceptable minimum probability of correcting the reported election outcome if it differs from the outcome that would be obtained from a full hand count of all ballots."

The Advisory Commission noted that additional resources would be needed on the state, county, and local levels to conduct statewide RLAs. *The Advisory Commission recommends exploring sources of funding in addition to federal election security funding made available to states through the Help America Vote Act*.

2. Develop RLA procedures in close partnership with appropriate entities

The Advisory Commission recommends that the Secretary of State work closely with local and county election officials, peer officials in other states, and RLA experts to determine appropriate RLA procedures for Michigan.

The Secretary of State should establish oversight over RLAs in cooperation with partners at the county level. The state should then develop RLA procedures collaboratively with representation from all levels of government. The State should draw on experiences from other states and advice from civil society groups and academic experts who specialize in RLA methodologies and technologies.

Currently, Michigan has experimented with approaches to conducting RLAs, and this experience provides a valuable baseline for expanding audits statewide. Available options include ballot comparison, in which individual paper ballots are compared to the corresponding digital records from the tabulation system, and ballot polling, in which the outcome of the election is compared to the outcome reflected by a random sample of ballots.

Variations on these methods compare batches on ballots rather than individual ballots. There are also different methods of randomly selecting the ballots to be audited and of determining how many ballots need to be audited to satisfy the risk limit. Risk limits in pilots typically vary from 5 to 10 percent.

Auditing procedures should ensure that the ballots are physically secured and that a strong chain of custody is maintained. Other important logistical details include preparation of all materials needed to conduct RLAs, including ballot manifests maintained at the county level. Procedures must also account for variations in how absent voter ballots are stored (in separate absent voter counting boards in some jurisdictions, and along with in-person ballots in other jurisdictions).

Audit design should also consider the role of members of the public and outside validators in the auditing process. While the Secretary of State can help coordinate audits at the local and county level, independent observers—perhaps from non-government entities or other states—can provide additional value and credibility. Roles of outside observers and auditors should be coordinated with but distinct from state-level functions.

Without dictating which specific method or combination of methods is best, the Advisory Commission recommends the state draw on its own experience and that of other states to develop RLA methodologies for statewide audits, in collaboration with local partners.

3. Determine parameters for full RLA implementation

Now that the state has successfully completed its RLA pilots, the Advisory Commission recommends that the Secretary of State develop the parameters of a full RLA program, beginning with an audit of the November 2020 election. RLA implementation will depend on the availability of software tools for managing audits. Important implementation choices will include the selection of efficient RLA protocols for Michigan's election practices and determining appropriate risk limits.

The November 2020 election will have multiple statewide races, in addition to races at other jurisdictional levels that could audited, as is always the case with even-year November elections. The SOS should determine which races will be subject to RLAs.

The Advisory Commission recommends setting a goal of auditing all federal races and top-of-ticket statewide races. If this is not yet logistically feasible, the Advisory Commission recommends prioritizing top-of-ticket statewide races and expanding to other Federal races as soon as possible. For November 2020, at minimum the goal should be to audit the Presidential election.

4. Consider statutory changes to further support RLAs

The Advisory Commission considered the role that RLAs can play in the review and confirmation of elections given the current statutory framework, which requires county canvasses to be completed within 14 days of an election. Under current law, there are several obstacles to conducting an RLA as part of the certification process. Provisional ballots can be counted until the sixth day following the election, leaving as little as eight days to complete the county canvass. Seals on ballot containers cannot be broken until the county canvass is complete or else the ability to conduct a recount consistent with state law would be compromised. Even if ballots could be removed, audited, and replaced in

time to complete the county canvass, there would be little time to take any necessary corrective action prior to certification.

All pilot RLAs conducted in the state thus far have taken place after the official results have been certified. These pilots were not intended to actually verify the outcome of any given election, but instead focused on improving the methodology of the audits themselves. If any errors in the actual count had been discovered, it would have been too late to correct the issue within the context of the certification process. If audits are ultimately designed to be part of the certification process, they could be conducted before the official results are certified (and recounted, if necessary) and play a part in the official canvass of votes. Ultimately RLAs will be most useful if they are carried out before certification.

The Advisory Commission recommends that the Secretary of State pursue the following legislative changes to facilitate risk-limiting audits:

a. *Extend the county canvass period to be longer than the current 14 days, to provide additional time for pre-certification audits.*

b. *Allow ballot boxes to be opened and re-sealed by qualified and sworn staff for the purpose of conducting risk-limiting audits, while preserving the ability to recount ballots. Conducting an audit properly should not render a precinct unrecountable.*

c. *Develop criteria under which the results of a risk-limiting audit would lead to a full recount, if the audit determines that the reported election outcome may be inaccurate.*

d. *Consider moving the August primary to June (perhaps replacing the May election date) to allow a longer period between primary and general election dates and better accommodate an extended auditing and certification period.*

e. *If a risk-limiting audit cannot be completed before certification, determine the appropriate legal remedy, if any, if a later risk-limiting audit fails to confirm the outcome of the election or suggests that the outcome of the outcome is inaccurate (whether a contest, right of action, special election, or other remedy).*

5. Provide transparency and public education

The Advisory Commission discussed issues related to transparency and public education in the RLA process. In addition to confirming that the outcomes of elections are correct, RLAs are also designed to increase confidence in elections by showing voters that the outcomes can be trusted. RLAs work in concert with paper ballots to ensure that even if there was a problem with other election technology, such as optical scanners or the election management system, the issue would be caught and fixed by counting the physical ballots, which are on paper and cannot be hacked. A rigorous RLA should provide evidence to convince the public that the election outcome is correct.

The Advisory Commission highlighted several key elements for using RLAs to increase public trust:

First, the Advisory Commission recommends that all methodology involving risk-limiting audits should be clearly explained to the public. All critical elements of the RLA—how the risk limit is set, the statistical formula used to determine when the limit is met, how ballots are randomly selected, the method of ballot polling or comparison used, and other elements—should be documented publicly and clearly explained.

Second, all important steps in the audit should be conducted in public view, and data and documentation should be published online. It should be possible for any member of the public, the media, candidates, or other interested parties to review the audit and obtain any information necessary to evaluate the audit.

While some materials, such as ballots, might not be possible to make available in all cases due to privacy concerns, they should be open to public inspection during the audit, and all other elements of the audit should be in public view and documented to the extent possible.

Third, the Secretary of State should partner with civil society groups and local officials to provide public education surrounding audits, why they are important, and how they work. The Secretary of State should develop an accurate, simple account of audits and how they work. These communications should be message-tested and public opinion tested to see which terminology resonates with members of the public and which does not.

Fourth, the Secretary of State should partner with trusted messengers to spread the word about audits and why they are important. This includes local leaders from different parties, different areas of the state, and other states as necessary. The Secretary of State should also identify stakeholders in the media and other opinion leaders who can be helpful in explaining how RLAs work and the goals of the practice.

Finally, it is important to start public education and engagement of stakeholders well before an election. If parties and candidates are brought in early, the audit process can help both the apparent winner and apparent loser accept the audit process and its role in verifying the outcome of the election. This can help mitigate the concerns a losing candidate and his or her supporters might have that the outcome was not fair and any incentive to suggest that the election was not accurate.

6. Continue use of other types of audits in addition to Risk Limiting Audits

The Advisory Commission recommends that Michigan continue to conduct procedural audits and hand recounts of random precincts, in addition to RLAs.

Procedural audits serve a separate, important function of ensuring that election officials have done their jobs properly, for example by programming election equipment following established protocols. This has independent value and should be continued. The Secretary of State should continue to seek aggressive procedural audits to ensure local jurisdictions are administering elections properly. Procedural audits that discover errors should result in repercussions, including remediation, additional resources and monitoring, and additional training.

Auditing by hand recounts of random precincts boosts public confidence by counting every ballot in a given precinct. Although counting all ballots for all races in all jurisdictions is not feasible, random audits supplement the statewide benefit of RLAs by providing additional confidence at the local level.

C. Countering Misinformation and Disinformation

The Advisory Commission discussed the threat that false information disseminated about elections could pose to high-profile elections. Intelligence assessments from the Federal Bureau of Investigation and Department of Homeland Security determined that undermining confidence in U.S. elections is a critical component of foreign election interference strategies. These efforts could take multiple forms, from sharing intentionally false information about elections (disinformation) to fostering confusion with the goal of amplifying misinformation, to stoking tensions among different political parties and interest groups in an effort to undermine national unity and acceptance of democracy.

Recognizing that these attacks could come on many fronts, the Advisory Commission considered ways in which the Secretary of State could foster partnerships to counter the spread (whether intentional or unintentional) of false information about elections. The Advisory Commission also discussed

points of emphasis for promoting confidence in election processes in response to unsupported claims of election misconduct or irregularities.

1. *Coordinate accurate information sharing among local officials*

The Advisory Commission discussed the importance of local officials, especially municipal and county clerks, receiving reports of false information being spread about elections, as well as their importance in responding with corrective, accurate information.

The Advisory Commission recommends that the Secretary of State establish a structure to notify local officials of false or misleading reports about elections in real time so that local officials can respond through local channels. This effort should include ensuring local officials participate in the Election Infrastructure-Information Sharing and Analysis Center (EI-ISAC) and share reports of misleading information with both EI-ISAC and CISA.

2. *Form bilateral partnerships to counter misinformation and instill confidence*

The Advisory Commission discussed the difficulty of countering election misinformation given the increasing propensity of the electorate to receive information through silos. Voters may be distrustful of election officials or media sources that they perceive to be ideologically opposed to or biased against their own preferences.

In light of this reality, the Advisory Commission recommends that the Secretary of State build and facilitate bilateral partnerships to counter misinformation and provide accurate, trusted election information. For example, in addition to forming partnerships with Secretaries of State of different political parties and from different states, the Secretary of State should promote these partnerships on the county and local level. For example, neighboring clerks with different party

identifications could partner on messages to their communities. To the extent political demographic trends might make this difficult in some areas of the state, officials should consider partnerships with clerks from other parts of the state as well.

Local officials already have networks that could be used to facilitate these partnerships, including the Michigan Association of Municipal Clerks, Michigan Association of County Clerks, Michigan Council of Election Officials, Michigan Townships Association, Michigan Municipal League, and Michigan Association of Counties. The Secretary of State should work with these organizations to promote partnerships sharing trusted information and countering misinformation.

3. Develop a rapid-response strategy to counter misinformation at the State level

The Advisory Commission discussed the importance of the Secretary of State developing systems to quickly share and amplify accurate information in response to false reports before and on election day. The Secretary of State's relatively limited direct ability to reach the public must be augmented through public media and other state officials and partners.

The Advisory Commission recommends that the Secretary of State develop a plan to anticipate and respond quickly to reports on Election Day with previously developed, off-the-shelf explanations of election processes and procedures that can be shared both before and after misleading information is circulated.

The Secretary of State should work with media and local officials in advance of election day to establish lines of communication that can be used to share this information as necessary.

Additionally, the Secretary of State should develop a list of topics likely to be raised in the leadup to election day and on election day. A major point of emphasis should be aspects of the election system that are easily misunderstood and could be exploited by entities looking to foster distrust in elections. This strategy should include a realistic assessment of actual vulnerabilities and the presentation of these vulnerabilities in context.

The Secretary of State should also be prepared for concerted, targeted information attacks on social media. The Secretary should communicate with social media companies to maximize the ability to identify and respond to these attacks should they occur.

4. *Share information on data security best practices with campaigns*

Political campaigns and candidates could also be the target of attacks. Those attempting to undermine or interfere with elections could attempt to breach campaign websites, databases, and email accounts to identify and share damaging information or spread false information. *Accordingly, the Advisory Commission recommends that the Secretary of State develop training materials for campaigns and candidates to help them protect themselves against phishing attacks and other vulnerabilities.*

D. Election Night Reporting

Election officials are under pressure from the media, candidates, and members of the public to report election results quickly on election night. This is particularly the case in a presidential election, in which national media aggregate 50 different sets of state election results to try to project the winner of the electoral college as quickly as possible.

In Michigan, as in other states, the official canvass of votes never happens on election night. The county canvass of election results is not complete until 14 days after an election, and frequently includes ballots that were not originally counted on election night, including envelope provisional ballots and military and overseas ballots which may be counted after Election Day if ballots were sent out late.

Nonetheless, in an effort to report election outcomes quickly, precincts send *unofficial* results to county clerks in electronic form. The procedures for doing so are developed by individual counties. There are three primary ways in which this occurs: (1) physical delivery of removable drives with election results; (2) uploading to the county election management system; and (3) using cellular modems connected to tabulators to send unofficial results.

Connecting tabulators to the Internet or other external networks creates significant risks. Although many jurisdictions that do so have security features such as private networks and encryption, nothing connected to the Internet is completely secure. It is possible that unofficial results could be intercepted or manipulated, that the locality's election management system server could be attacked remotely over the network, or that optical scanners could themselves be remotely attacked. The added convenience of providing unofficial results more quickly may not be enough to justify these risks to election integrity and voter confidence. For these reasons, the U.S. Senate Select Committee on Intelligence has recommended that new voting machines should have wireless networking capabilities removed or rendered inert.[3]

1. Phase out the "modeming in" of election night results

The Advisory Commission recommends that jurisdictions phase out the use of wireless modems, even to transmit unofficial results, and that jurisdictions never

[3] See U.S. Senate Select Committee on Intelligence, "Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election—Volume 1: Russian Efforts Against Election Infrastructure" (2019), page 59. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

connect election management systems or tabulators to an external network, even using an intermediate server or firewall. We are cognizant of the realities facing election officials as they attempt to phase out this long-standing practice and recognize that it may be difficult to make this change during the 2020 election cycle.

A safer means of transmission is to physically deliver election media for tabulation. Election media should never be attached to an Internet-connected computer. It should be sealed in an evidence bag or other security container at the polling place, and the integrity of the seal should be verified before reading the results into the election management system. Local protocols should also include a documented chain of custody for the election media.

2. Build redundancies into electronic reporting

The Advisory Commission recommends that jurisdictions implement additional procedures to ensure that unofficial election night result reports are accurate. For example, each precinct could call the county and verbally verify a match with the unofficial results received by the county via physical delivery of media. Public posting of results tapes at polling locations provides an additional safeguard.

3. Observe best practices when using removable drives

Many jurisdictions use removable media to copy unofficial results out of their election management systems for posting to Internet sites. Local jurisdictions should take steps to minimize the possibility removable media could compromise the election management system. Jurisdictions should use only encrypted removable drives to transfer unofficial results. To avoid the possibility that the drive could become infected and spread malicious software into the election management system, a new removable drive should be used for each transfer operation.

4. **Prioritize accuracy and prepare communication plans in the event election-night reports are late or inaccurate**

The advisory committee recommends prioritizing accuracy over speed in election night reporting. *To the extent more secure, accurate methods of election night reporting will take longer, the Advisory Commission recommends local jurisdictions pursue the more secure and accurate method.*

The Secretary of State should work with counties to develop a communication plan for media and the public in the event that election night reports are late to arrive, whether because a precinct has a larger than expected number of ballots to process, the precinct is taking time to reconcile ballot totals and pollbook entries, or the transmission of unofficial results is taking longer than expected

5. **Conduct a county-by-county assessment of security practices in election night reporting, and address greatest deficiencies immediately**

The Advisory Commission recommends that the Secretary of State assess each jurisdiction's method of transmitting election results to identify the greatest areas of vulnerability, help to remediate them and expand redundancies in reporting to counteract any failures. The Secretary of State should also consider expanding the functionality of statewide election night results reporting.

E. Emergency/Disaster Preparedness

The Advisory Commission discussed a set of issues pertaining to state and local officials' level of preparedness for emergencies or natural disasters on Election Day. Storms, power outages, acts of violence, or other disruptions all have the potential to disrupt elections, particularly given the volume of tasks to be completed in a short period of time, with little margin for error, for an election to be conducted successfully.

1. Conduct statewide, countywide, and local exercises

The Advisory Commission recommends the Secretary of State coordinate exercises to prepare election officials and other government units for emergencies or disasters on election day. Tabletop exercises can be utilized to run through various emergency scenarios, test vulnerabilities, and assess preparedness.

Because disasters and emergencies could manifest themselves at various levels of government, exercises should be held within and across jurisdictions. For example, the Secretary of State should coordinate statewide tabletop exercises with county and municipal election officials and other state agencies such as the Michigan State Police. In turn, counties and municipalities should conduct their own exercises with their counterparts in local government, including information technology, law enforcement, and governing authority bodies.

The Department of Homeland Security has coordinated tabletop exercises in Michigan and across the country, and these exercises provide a useful model for additional exercises within the state.

2. Develop robust emergency response plans at the state and local level

All election jurisdictions should have a detailed and robust, emergency response plan in writing. *The Advisory Commission recommends that the Secretary of State develop a written plan with specific actions to be taken in response to various unexpected incidents on and around election day.*

The policy should specify roles and responsibilities both within and outside of the Department of State. To the extent this plan involves cooperation from other agencies such as the Department of Technology, Management, and

Budget and the Michigan State Police, the Department of State should communicate with these agencies in developing the policy.

The Secretary of State should promote this plan as a model for local jurisdictions to develop their own emergency and disaster response plans. Both state and local plans should be tested with tabletop exercises and other training exercises.

3. Prepare mitigation plans for election equipment and polling places

The Advisory Commission recommends that the Secretary of State and local jurisdictions develop policies to mitigate emergencies or unexpected events on election day that could render election functions inoperable or delay the voting process. There should be sufficient materials to cover several hours of disruption. This should include:

- Paper backups of voter registration lists and pollbooks provided to every polling location.
- Sufficient emergency paper ballot processing materials (including auxiliary bins) and related contingency plans in case voting tabulators are not functioning, and detailed training to ensure proper protocols are followed.
- Sufficient provisional ballot materials.
- Communication plans in the event that polling places are inaccessible or open late.
- Plans to extend voting hours if ordered by the courts, including provisional supplies needed for extended hours.
- Sufficient ballots to account for all registered voters in addition to eligible individuals who register on election day. Jurisdictions should review ballot supply and consider the potential need for ballots in excess of the statutory minimum of 100% of registered voters.
- Sufficient staffing to maintain efficient polling place operations if pollbooks or scanners are not functional.
- Backup plans in case official information such as polling place location and voter registration status is not available via official websites.

- Communication plans in the event unofficial results are delayed for any reason.

F. Additional Areas of Recommendation

The Advisory Commission identified additional subjects of focus for the Secretary of State and local jurisdictions to improve security practices.

1. Physical and Equipment Security

The Advisory Commission recommends that the Secretary of State work with local jurisdictions to regularly perform a jurisdiction-by-jurisdiction assessment and review of the physical security of election equipment. The assessment should ensure, at minimum, that all election equipment is in the appropriate setting after use, is physically locked, has tamper-evident seals correctly applied, and is stored in well secured facilities. Equipment inventories should be maintained and should record the correct serial numbers and seal numbers. The scope of the review should include both polling place equipment and election management systems.

To the extent jurisdictions are not adequately securing equipment, county and state officials should ensure these problems are remedied. The state should provide resources and training as necessary to upgrade physical security.

2. Software Updates

The Advisory Commission recommends that the Secretary of State ensure that procedures are in place at the local and county level to ensure that software running on polling place equipment, election management systems, and other election-related computer systems is promptly upgraded when new versions are available from the manufacturer.

Outdated software is a major source of vulnerabilities, and applying software updates promptly is essential to ensure that known vulnerabilities are corrected.

For polling-place equipment, the State should maintain a list of the current software version and patch set that has been tested by a federally accredited lab (as required in Michigan). Localities should work with their vendors to see that only these versions are used in elections.

Localities should also establish a patch management framework for all computer systems used to support the election, including equipment used to access the Qualified Voter File. Security patches should be installed promptly, and outdated or unsupported hardware and software should be replaced.

3. Vendor Accountability and Reporting

The Advisory Commission recommends that the Secretary of State and county clerks demand greater transparency and accountability from election vendors. State and local election officials rely upon commercial software and equipment for many aspects of the election process. Vendors should encourage independent security reviews by establishing a vulnerability disclosure program, proactively share any known security threats, and be transparent about potential vulnerabilities, whether past, present, or future. To the extent vendors know of system-wide or localized security improvements that could be made, they should proactively inform election officials. If vendors fail to comply with their duty to proactively notify election officials of potential incidents, the Secretary of State should work with counties to ensure there are appropriate consequences. Current and future contracts should be leveraged to facilitate this process.

The Secretary of State and counties should document security concerns and vendor responses. Information on security concerns should be shared both within and across states served by the vendors.

4. Local Election Official Training and Resources

To the extent not covered in the recommendations above, the Advisory Commission recommends that the Secretary of State implement comprehensive security standards and training and requirements for local officials. These should include, at minimum:

- Additional security training as part of clerk accreditation (new and ongoing)
- Membership in the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)
- Utilization of DHS vulnerability scanning and penetration testing
- Implementation of cyber navigator programs
- Best practices for password creation, changes, maintenance, and security
- Regular review of user accounts, following the principle of least privilege
- Regular software patching and updates
- Awareness of phishing risks and phishing exercises
- Preparation and planning for incidents involving malware, ransomware, or denial of service attacks
- Education about Website defacement risks
- Recommendations concerning the adoption of HTTPS and use of official TLDs, such as .gov
- Regular backups of election and database information
- Best practices for information sharing across jurisdictions

5. Electronic ballot return for overseas voters

The Commission discussed the issue of electronic ballot return for overseas voters. Many states allow military or overseas voters to return ballots electronically through email, fax, or the Internet. Currently, Michigan sends ballots out electronically, but they must be returned by mail.

The Advisory Commission does not recommend introducing electronic ballot return for overseas voters, because no available technology that is adequately secure at the present time. Some states that have previously implemented electronic return have discontinued it because of security concerns. Although some security risks can be mitigated—for example, requiring cryptographic identity validation through the military's common access card system can mitigate some risks of unauthorized access—there is no method to reliably secure the ballot all the way to the local jurisdiction.

To the extent new technologies emerge to address these concerns, the Secretary of State should evaluate them; however, the Advisory Commission is not convinced that tools currently in use in other states achieve adequate security and concurs with the National Academies that the Internet should not be used for the return of marked ballots at the present time.[4] The Secretary of State should explore other methods of improving the voting experience of mi

[4] National Academies of Sciences, Engineering, and Medicine, *Securing the Vote: Protecting American Democracy* (2018), recommendation 5.11. https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy.