UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF INDIANA
INDIANAPOLIS DIVISION

AMERICAN COUNCIL OF THE BLIND OF INDIANA, et. al,	)	
Plaintiffs,	)	
v.	)	No. 1:20-cv-3118-JMS-MJD
INDIANA ELECTION COMMISSION, et. al.,	)	
Defendants.	)	

DEFENDANTS' CROSS-MOTION FOR SUMMARY JUDGMENT AND DESIGNATION OF EXHIBITS

Defendants, by counsel, and pursuant to Rule 56 of the Federal Rules of Procedure, move this Court to enter judgment in favor of Defendants because Indiana's absentee voting system for print-disabled voters does not violate federal law.

1. On December 7, 2020, Plaintiffs—three individual voters and two advocacy groups—filed suit against state election officials, alleging violations of the Americans with Disabilities Act and Section 504 of the Rehabilitation Act of 1973 [Filing No. 1].

2. Fourteen months into the litigation, and on the eve of the May 2022 primary election, Plaintiffs sought a preliminary injunction [Filing No. 81], which the Court denied in part, and granted in part [Filing No. 100; Filing No. 106]. The Court preliminarily enjoined state officials from enforcing the traveling-board

requirement for print-disabled voters voting in the primary election [Filing No. 100; Filing No. 106].

3. On May 18, 2022, Plaintiffs filed a motion for summary judgment and permanent injunction, and in the alternative, requested another preliminary injunction [Filing No. 127].

4. The Court should deny Plaintiffs' motion for summary judgment and instead grant summary judgment to Defendants for four reasons: First, Plaintiffs lack standing because the alleged discrimination is not traceable to Defendants' conduct. Second, Indiana's absentee voting system for print-disabled voters does not violate the ADA or the Rehabilitation Act because Indiana law specifically authorizes the travel board to take a disability-accessible voting machine to the home of a print-disabled voter so that such a voter may vote privately and independently. Third, the expansion of the UOCAVA system to print-disabled voters, through Senate Enrolled Act 398, will provide yet another accommodation for print-disabled voters to vote privately and independently from their own home. And fourth, Plaintiffs' desired accommodation—internet voting through an RAVBM tool—would fundamentally alter the nature of Indiana's elections system by forcing the State to purchase and implement an internet-voting scheme that has never been tested or used by Indiana's policymakers.

5. In support of Defendants' cross-motion for summary judgment and their response in opposition to Plaintiffs' motion for summary judgment, Defendants submit the following exhibits:

a. Exhibit 1: Indiana Election Division Declaration, dated June 15, 2022

b. Exhibit 2: Federal Government's Study on Risk Management for Electronic Ballot Delivery, Marking, and Return, May 2020

6. Defendants also rely and cite to other evidence already in the Court's record, including the following:

a. Indiana Election Division Deposition, Filing No. 80-7

b. Indiana Election Commission Deposition, Filing No. 126-32

c. Indiana Secretary of State Deposition, Filing No. 80-8

d. Indiana Election Administrator's Manual, Filing No. 91-1

e. Civix Deposition, Filing No. 126-29

f. Plaintiffs' Appendix of Exhibits in support of their motion for summary judgment, Filing No. 126

g. Plaintiffs' affidavits in support of their motion for preliminary injunction, Filing Nos. 80-1, 80-3

7. Defendants submit a combined brief in support of its motion for summary judgment contemporaneously with this motion.

WHEREFORE, Defendants respectfully request the Court enter judgment in favor of Defendants.

Respectfully submitted,

THEODORE E. ROKITA
Attorney General of Indiana

Date: June 15, 2022

By: Caryn N. Szyper
Aaron T. Craft
Deputy Attorneys General
OFFICE OF INDIANA ATTORNEY GENERAL

TODD ROKITA
Indiana Government Center South, 5th Floor
302 West Washington Street
Indianapolis, Indiana 46204-2770
Phone: (317) 232-6297/(317) 232-4774
Fax: (317) 232-7979
Email: Caryn.Szyper@atg.in.gov;
Aaron.Craft@atg.in.gov

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF INDIANA
INDIANAPOLIS DIVISION

AMERICAN COUNCIL OF THE BLIND OF INDIANA, et. al,	)	
Plaintiffs,	)	
v.	)	No. 1:20-cv-3118-JMS-MJD
INDIANA ELECTION COMMISSION, et. al.	)	
Defendants.	)	

DECLARATION OF THE INDIANA ELECTION DIVISION

J. Bradley King and Angela Nussmeyer, adults competent to testify, and being duly sworn upon their oath, say:

1. The Indiana Election Division is a bipartisan office. We are the co-directors of the Division, appointed by the Governor. The Indiana Election Division cannot take any action or provide the official position of the office unless both co-directors agree.

2. The Election Division assists the Indiana Election Commission and the Indiana Secretary of State in the administration of Indiana election laws, including: overseeing and implementing the National Voter Registration Act and the Help America Vote Act of 2002 (HAVA); maintaining maps and legal descriptions of all precincts in Indiana; approving proposed precinct boundary changes for conformity with state law, subject to any challenge being filed with the Commission; maintaining campaign finance reports filed by candidates for state legislative and statewide offices

and by political action committees and regular party committees that contribute to candidates for these offices; managing statutorily required statewide voter list maintenance project in odd-numbered years; approving uniform election and registration forms; advising and instructing local election officials on election administration; publishing brochures and manuals to assist candidates, political parties, the media, and the general public in understanding election administration issues; accepting candidate filings for federal, statewide, state legislative, and judicial offices, including prosecuting attorneys; publishing election returns on the Division's web site; and providing information regarding voter registration and absentee ballot procedures to military and overseas voters.

3. The Election Division serves in an advisory capacity in the actual operation of elections, whereas county boards of elections are tasked with the responsibility for preparing for and administering elections, including approving applications for absentee voting, and producing, dispatching, receiving, and counting absentee ballots.

4. The Election Division does not produce ballots used for absentee voting or on Election Day for Indiana's elections. It does, however, provide guidance and assistance to counties in ballot format and layout to ensure conformity with state law. But counties are not required to consult the Election Division, and the Election Division does not formally approve any county's Election Day or absentee ballots.

5. The Election Division does not have the power to compel county election officials to take or refrain from taking particular action. Nor does the Division have any enforcement authority.

6. Indiana law provides five ways to vote: (1) in-person voting on Election Day; (2) absentee in-person voting during the early voting period; (3) absentee voting by mail; (4) absentee voting by traveling board; and (5) absentee voting by military and overseas voters (called "UOCAVA voters").

7. In the last two primary elections held in nonpresidential, general election years, most voters in Indiana cast their ballots in-person on Election Day rather than by one of the available absentee-voting methods.

a. For example, during the May 2022 primary election, the election turnout was 14%, and only 27% of those who voted cast an absentee ballot—the remainder voted in-person on Election Day.

b. And during the May 2018 primary election, the election turnout was 20%, and only 20% of those who voted cast an absentee ballot—the remainder voted in-person on Election Day.

8. State law requires voters to be able to personally mark their own vote-by-mail ballot and affix their signature or mark (indicating their signature) on the absentee-ballot security envelope. This is a critical component of mail-in absentee voting where the voter attests that he or she personally marked the ballot. That attestation ensures that the voter whose name is on the ballot is the voter who cast the ballot, which adds another layer of security to our elections and promotes public trust

in the integrity of elections. Requiring that the voter himself or herself mark the ballot and sign the affidavit also avoids a situation where the voter is coerced by another into voting a particular way.

9. Under Indiana Code section 3-5-2-50.3, a "voter with print disabilities" means "an individual who is unable to independently mark a paper ballot or ballot card due to blindness, low vision, or physical disability that impairs manual dexterity."

10. But Indiana law provides print-disabled voters with four options to cast a ballot.

11. First, a print-disabled voter may vote in-person on Election Day using an accessible voting machine at the polling location. State and federal law require that all polling locations have at least one accessible machine to allow all voters to vote privately and independently. Ind. Code § 3-11-15-13.3(d)–(e); 52 U.S.C. § 21081(a)(3)(B). All 92 counties use voting systems certified by the Indiana Election Commission, and those systems are tested for compliance with accessibility standards to include accessible voting systems. The bipartisan Election Day judges may assist the voter in making the voting machine accessible—for example, if the voter uses a sip-and-puff mechanism, then the bipartisan judges may connect the voter's assistive device to the accessible voting machine. If the voter needs assistance marking the ballot, the voter may use a person of his or her choosing, so long as that person is not the voter's employer or union representative—the person assisting the voter must complete an affidavit of voter assistance at the polls before entering the voting

booth. The voter may also ask for assistance in marking the ballot from the precinct judges, who are members of the precinct election board. Ind. Code § 3-11-9-3.

12. Second, a print-disabled voter may vote absentee in-person using an accessible voting machine at the early-voting location (the clerk's office or a satellite location) during the early-voting period, which begins 28 days before Election Day and ends at noon the day before Election Day. Just as on Election Day, each early-voting location must have an accessible voting machine available to allow all voters to vote privately and independently, and all 92 counties use voting systems certified by the Indiana Election Commission, which include accessible equipment. And just as on Election Day, the voter may request assistance from either a person of the voter's choosing or the bipartisan absentee-voter board that oversees the early voting location in connecting the voter's assistive technology to the voting machine (if applicable) or in marking the ballot.

13. Third, print-disabled voters may vote absentee by traveling board. The bipartisan traveling voter board serves to protect print-disabled and other vulnerable voters from coercion or improper influence. Print-disabled voters have both a right to vote privately and independently and a right to receive assistance if help is needed in casting a ballot. This method of absentee voting is available starting 19 days before Election Day and is completed the day before the election, barring emergencies on Election Day that may permit the county election board to send a travel-board team out on Election Day. State law provides two traveling-board options:

a. First, the default option is that the traveling board goes to the voter's

residence with a ballot card used with an optical-scan voting machine or a traditional hand-counted paper ballot for the voter to mark. If the voter is unable to mark the ballot, then the traveling board may assist the voter in marking his or her absentee ballot.

b. Second, a county election board may adopt by unanimous vote a resolution authorizing the traveling board to take an accessible voting machine to the voter's residence. The voter may then cast the ballot in the same manner as would occur if he or she voted absentee in person.

   i. Although the voter may require assistance from the traveling board to hook up certain devices to the voting system (e.g., sip-and-puff device), once the voting system is made accessible the voter is able to vote privately and independently using the adaptive technology offered by the voting system. State law does not require the traveling board members to stay by the voter's side while the voter marks and casts his or her absentee ballot. Additionally, if the accessible voting machine uses an optical-scan ballot card, the traveling board can assist the voter with enclosing his or her marked ballot in a security envelope and may additionally certify that the voter is a voter with disabilities who is unable to sign the absentee-ballot security envelope. In contrast, when voting by mail, a voter must be able to sign his or her name or make a mark on the security envelope, and only the voter's power of attorney can attest to the voter's

signature after completing the affidavit of assistance on the absentee-ballot security envelope and enclosing the POA with the voter's ballot.

ii. State law is clear that the decision to authorize the traveling board to take a voting machine to a voter's residence lies exclusively with the county election boards. Neither the Secretary of State, the Election Division, nor the Election Commission has power to compel a county election board to adopt a resolution authorizing the traveling board to take an accessible voting machine to a voter's residence.

c. On June 3, 2022, the Election Division, by its contractor, sent a survey to county election officials asking whether their respective counties had adopted a resolution authorizing the county's traveling board to take an accessible voting machine to a voter's residence. The results from that survey show that at least 16 counties have already authorized this option and several more counties expect to adopt a unanimous resolution in the near future, before the November 2022 general election.

14. In addition to in-person voting and voting by traveling board, under Senate Enrolled Act 398, which became effective in July 2021, print-disabled voters qualify to vote absentee in a similar manner that UOCAVA voters cast absentee ballots.

15. SEA 398 requires the Secretary of State, with the approval of the Election Division, to "develop a system that complies with the Web Content Guidelines."

Ind. Code § 3-11-4-5.8(f). In September 2021, the Secretary issued an order adopting procedures for print-disabled voters. Since that time, the Election Division has been in the process of developing that system at the state level:

a. The Division's initial focus was to create an ABS-VPD form that is compatible with print-disabled voters' assistive-technology.

   i. The Division first developed the dual application, which was approved and made available to the public in paper form on February 17, 2022.

   ii. Also, beginning in late January 2022, the Division initiated efforts through Civix, its statewide-voter-registration-system (SVRS) vendor, to make the ABS-VPD form available online to voters after logging into their customized voter-portal page at indianavoters.com so that voters could electronically submit the application and county officials could process the online combined form to register to vote and request an absentee ballot.

      1. The Division's vendor modified SVRS so county officials could manually enter and process the voter's registration request and, separately, the voter's absentee request once the voter-registration change was accepted.

      2. The Division's vendor also modified SVRS to receive the online ABS-VPD form, diverting voter registration and absentee re-

quests to specialized hoppers, which allow county users to process the requests in a specific order.

3. Additionally, the new ABS-VPD form type was added to SVRS, which becomes part of the voter's record. The voter is then able to access that data at indianavoters.com to determine if his or her absentee request was approved, to monitor when county officials sent the ballot, to verify that county officials received the ballot, and to monitor whether the absentee request or absentee ballot was rejected or not received.

iii. After user-acceptance testing, which identified some bugs and defects that needed fixing after launch, the Division released the online version of the ABS-VPD for use by voters and county election officials on April 21, 2022. This launch was during the State's black-out period, where enhancements generally are not pushed into SVRS to limit risk to election functions. After releasing the new module, a bug was discovered that did not include the voter's party-affiliation selection for ABS-Mail applications submitted online, which had the unintended consequence of some voters having their application rejected on the deadline date to file an ABS-Mail application, as party affiliation is required on the absentee application in a primary election.

b. In addition to the ABS-VPD, the Division developed a voter secrecy

waiver, which is necessary for all emailed or faxed ballots returned to county officials because those ballots must be remade on a ballot card that can be read by the ballot tabulator used to count the ballots. The Division completed that form—ABS-25—and it was approved for use on January 14, 2022. The Division also added the electronic version of the ABS-25 to SVRS for use by county election administrators when an ABS-VPD form is added to a voter's record.

c. The Division continues its efforts to improve upon the functionality of the process and system.

   i. The Division's SVRS vendor is working to remedy all bugs and defects identified during testing for the online application and modifications to SVRS, including updating parts of the online application to match with the paper-based ABS-VPD and streamlining the system for processing applications by county officials. This will take considerable work by the contractor before a black-out period starts in September, a period during which it is not advisable to push new enhancements to the system to limit risk to the election.

   ii. The Division is training county officials on the new functionality added to SVRS relating to processing the ABS-VPD applications, with the first training date set for June 21, 2022, and training materials being completed before that date.

   iii. The Division's SVRS vendor will train SVRS help-desk personnel

on the new functionality of the system so that they can better assist county administrators with issues that may arise during the election cycle when processing online applications.

iv. The Division is currently soliciting a web accessibility testing vendor to retest indianavoters.com and its documents using the latest Web Content Guidelines (WCAG) standard.

1. On May 23, 2022, the Division, through its contractor (Baker Tilly), distributed the State's web-accessibility testing project overview and vendor questionnaire, with a deadline for interested vendors to respond on June 8, 2022.
2. The scope of the project prioritizes accessibility testing for the Division's fillable PDFs, the ABS-VPD and ABS-25 (the affidavit for voters with print disabilities), the registration website, including the voter portal on indianavoters.com, the mobile website portal, the historical elections results module, and the election night reporting website.
3. The project seeks a testing completion date by August 2022, with a goal of all web accessibility testing and remediation to be complete by September 30, 2022, in advance of the November 2022 general election.

d. Although the Election Division has no role or enforcement authority in the actual production of Election Day or absentee ballots, the Division

intends to develop best practices for creating an absentee ballot that can be used with at-home adaptive technology, such as a screen reader. One option may include following the model used by Pennsylvania in *Drenth v. Boockvar*, No. 1:20-cv-829, 2020 WL 2745729, at *6–7 (M.D. Pa. May 27, 2020), to create a "write in" ballot, where a voter with print disabilities would be presented with a list of candidates for each office and then the voter types in the name of their selected candidate or the party affiliation for their candidate of choice in a separate document using text boxes. This model is similar to the federal write-in absentee ballot (FWAB) process for UOCAVA voters, but it is not identical because UOCAVA voters do not receive a list of candidates and instead have to conduct their own research.

e. The Division has also received feedback from several voting-system vendors regarding the feasibility of creating accessible ballots with the election-management software certified for use with their voting systems or alternative methods to convert the ballot images to be workable with at-home adaptive technology. The majority of counties contract with a vendor known as MicroVote, but others elect to contract with Hart, ES&S, and Unisyn. In response to a VSTOP (voter system technical oversight program) inquiry about the use of adaptive technologies with mailed, faxed, and emailed absentee ballots, the four vendors indicated that they had not performed extensive testing to determine if their ballot cards

were or could be made accessible with adaptive technology, and the Election Division has not independently evaluated or tested the voting systems vendors' capabilities in this regard.

16. Implementing an RAVBM tool to be used in time for the November 2022 general election would be highly improbable if not impossible. Because state law does not require RAVBM, the Election Division and the counties would have to start from scratch.

a. First, the Division would have to select a vendor, and the State's procurement process is very prescribed and would take months to complete, starting with pulling together specifications for a request for proposal, releasing the proposal and receiving bids, evaluating bids and negotiating a best and final offer, and then moving forward with executing a contract that requires the review of other state agencies, including the Indiana Office of Technology and the Attorney General's office.

b. Second, the State would need to engage its SVRS vendor, who also manages the public-facing website indianavoters.com, to build out the website or at least work with the RAVBM vendor to incorporate any "plug-and-play" technology and ensure that the RAVBM technology works with existing state resources, including its cybersecurity tools.

c. Third, because Indiana election officials are unfamiliar with RAVBM tools, the Election Division would need to become minimally proficient in using the tool to then prepare and present to county election officials

training on how to use, monitor, and troubleshoot the system, presumably with the assistance of the RAVBM vendor and Civix.

d. Fourth, the State is focused on improving the ABS-VPD online application to ensure it conforms with all existing state and federal laws and release improvements to the system put on hold to create the ABS-VPD module for the primary election before the black-out period to push enhancements to the system takes effect in mid-September 2022. According to the SVRS project manager, the list of improvements scheduled between now and September 2022 and the hours needed to do so rival what the State does in an entire year, rather than a three-month period of time. It may be impossible to coordinate with the RAVBM vendor to incorporate their tool with the State's existing infrastructure before absentee ballots must be mailed to those voters with approved absentee applications for the November 8, 2022, general election, which is Saturday, September 24, 2022.

e. Fifth, all of this would have to occur while the Election Division and county election officials are in the process of completing recounts and certifying results for the May 2022 primary election, preparing for the November 2022 general election (with a deadline of August 26, 2022 to certify candidates to each county election board so they can begin to put together absentee and Election Day, a deadline of September 19, 2022 for each county election board to have printed or delivered the absentee

and provisional ballots, and a deadline of September 24, 2022 for each county election board to send out absentee ballots by mail to any voter whose application to receive an absentee ballot by mail was approved on or before that date, as well as to fax or email an absentee ballot to any UOCAVA or print-disabled voter whose request for an absentee ballot to be delivered by the method has been approved), and working toward continued implementation of SEA 398.

f. Sixth, the Division lacks the funding to implement an RAVBM tool, with less than $50,000 in its SVRS fund for spending in 2023 and little to no discretionary spending in its other funds, as most are dedicated funds that can be used for certain activities as directed in state law.

g. In view of all of these factors, implementing an RAVBM tool is not feasible until at least the May 2023 municipal primary election, at the earliest.

I DECLARE, UNDER THE PENALTY OF PERJURY, THAT THE FOREGOING IS TRUE AND CORRECT.

June 15, 2022
Date

J. Bradley King
J. Bradley King
Co-director of the Indiana Election Division (Republican Party Affiliation)

6/15/2022
Date

Angela Nussmeyer
Co-director of the Indiana Election Division (Democratic Party Affiliation)

RISK MANAGEMENT FOR ELECTRONIC BALLOT DELIVERY, MARKING, AND RETURN

INTRODUCTION

Some voters face challenges voting in-person and by mail. State and local election officials in many states use email, fax, web portals, and/or web-based applications to facilitate voting remotely for groups like military and overseas voters and voters with specific needs.

The Cybersecurity and Infrastructure Security Agency (CISA), the Election Assistance Commission (EAC), the Federal Bureau of Investigation (FBI), and the National Institute of Standards and Technology (NIST) assess that the risks vary for electronic ballot delivery, marking, and return. While there are effective risk management controls to enable electronic ballot delivery and marking, we recommend paper ballot return as electronic ballot return technologies are high-risk even with controls in place. Recognizing that some election officials are mandated by state law to employ this high-risk process, its use should be limited to voters who have no other means to return their ballot and have it counted. Notably, we assess that electronic delivery of ballots to voters for return by mail is less vulnerable to systemic disruption.

In this document, we identify risks and considerations for election administrators seeking to use electronic ballot delivery, electronic ballot marking, and/or electronic return of marked ballots. The cybersecurity characteristics of these remote voting solutions are further explored in NISTIR 7551: A Threat Analysis on UOCAVA Voting Systems.

RISK OVERVIEW

	ELECTRONIC BALLOT DELIVERY	ELECTRONIC BALLOT MARKING	ELECTRONIC BALLOT RETURN
Technology Overview	Digital copy of blank ballot provided to voter	Making voter selections on digital ballot through the electronic interface	Electronic transmission of voted ballot
Risk Assessment	Low	Moderate	High
Identified Risks	Electronic ballot delivery faces security risks to the integrity and availability of a single voter's unmarked ballot	Electronic ballot marking faces security risks to the integrity and availability of a single voter's ballot	Electronic ballot return faces significant security risks to the confidentiality, integrity, and availability of voted ballots. These risks can ultimately affect the tabulation and results and, can occur at scale

RISK MANAGEMENT FOR ELECTRONIC BALLOT DELIVERY, MARKING, AND RETURN

All states use **electronic ballot delivery** to transmit a digital copy of an unmarked ballot to the intended voter to mark, in compliance with the Military and Overseas Voters Empowerment Act (MOVE). These ballot delivery systems are exposed to typical information security risks of internet-connected systems. The most severe risks to electronic ballot delivery systems are those that would impact the integrity and/or availability of the ballots, such as altering or removing ballot choices. These risks can be reduced and managed through use of appropriate security controls. Additionally, some electronic ballot delivery systems perform functions to verify a voter's identity before presenting them their assigned ballot. The identification process can use personal identifying information, such as name and driver's license number, or biometrics. When this verification is improperly configured, remote electronic ballot delivery systems can present additional privacy risks—like the loss or theft of the voter's personal and/or biometric identity information. These risks may be managed through configuration management and appropriate security controls.

Electronic ballot marking allows voters to mark their ballots outside of a voting center or polling place. Typically, this describes the electronic marking of a digital copy of the blank ballot using the electronic interface. The marked ballot is then returned to the appropriate official. Risks to electronic ballot marking are best managed through the production of an auditable record, meaning the voted ballot is printed and verified by the voter before being routed to the appropriate official. This auditable record is an important compensating control for detecting a compromise of security in remote voting.

Electronic ballot return, the digital return of a voted ballot by the voter, creates significant security risks to the confidentiality of ballot and voter data (e.g., voter privacy and ballot secrecy), integrity of the voted ballot, and availability of the system. We view electronic ballot return as high risk.

Securing the return of voted ballots via the internet while ensuring ballot integrity and maintaining voter privacy is difficult, if not impossible, at this time. As the National Academies of Science, Engineering, and Medicine write in Securing the Vote: Protecting American Democracy (2018), "We do not, at present, have the technology to offer a secure method to support internet voting. It is certainly possible that individuals will be able to vote via the internet in the future, but technical concerns preclude the possibility of doing so securely at present." If election officials choose or are mandated by state law to employ this high-risk process, its use should be limited to voters who have no other means to return their ballot and have it counted. Further, election officials should have a mechanism for voters to check the status of their ballot, as required for provisional ballots and military and overseas voters by the Help America Vote Act and the MOVE Act, respectively.

RISK COMPARISON – ELECTRONIC AND MAILED BALLOT RETURN

Some risks of electronic ballot return have a physical analogue to the return mailing of ballots. However, electronic systems present far greater risk to impact a significant number of ballots in seconds.

- **Scale –** While mailing of ballots could be vulnerable to localized exploitation, electronic return of ballots could be manipulated at scale. For mailed ballots, an adversary could theoretically gain physical access to a mailed ballot, change the contents, and reinsert it into the mail. This physical man-in-the-middle (MITM) attack is limited to low-volume attacks and mitigated by proper chain of custody procedures by election officials. In comparison, an electronic MITM attack could be conducted from anywhere in world, at high volumes, and could compromise ballot confidentiality, ballot integrity, and/or stop ballot availability.
- **Bring Your Own Device –** Unlike traditional voting systems, electronic ballot delivery and return systems require a voter to use their own personal devices such as a cell phone, computer, or tablet to access the ballot. A voter's personal device may not have the necessary safeguards in place. As a result, votes cast through "bring your own device" voting systems may appear intact upon submission despite tampering as a result of an attack on the personal device rather than on the ballot submission application itself. Voters using personal devices increase the potential for an electronic ballot delivery and return system to be exposed to security threats.
- **Voter Privacy –** Electronic ballot return brings significant risk to voter privacy. Unlike traditional vote by mail where there is separation between the voter's information and their ballot, many remote voting systems link the two processes together digitally. This makes it difficult to implement strong controls that preserve the privacy of the voter while keeping the system accessible.

TECHNICAL CONSIDERATIONS FOR ELECTRONIC BALLOT RETURN

Some voters, due to specific needs or remote locations, may not be able to print, sign, and mail in a ballot without significant difficulty. While we assess electronic ballot return to be high risk, some jurisdictions already use electronic ballot return systems, and others may decide to assume the risk.

While risk management activities should lower risk, election officials, network defenders, and the public may all have different perspectives on what level of risk is acceptable for the systems used to administer an election. For those jurisdictions that have accepted the high risk of electronic ballot return, the following guidance identifies cybersecurity best practices for internet- and network-connected election infrastructure. The information provided should be considered a starting point and is not a comprehensive list of defensive cybersecurity actions. Even with these technical security considerations, electronic ballot return remains a high-risk activity. Refer to applicable standards, best practices, and guidance on secure system development, acquisition, and usage.

GENERAL

- All election systems and technology should be completely separated from systems that are not required for the implementation or use of that specific system.
- Any ballots received electronically should be printed or remade as a paper record.
- Election officials should implement processes to separate the ballot from the voter's information in a manner that maintains the secrecy of the ballot.

- If the system attempts to verify the voter's identity through digital signature, biometric capture, or other method, assess whether an attacker could use this to violate ballot secrecy.
- The auditability of the results should not rely solely on the data stored digitally within the system.
- Best practices for securing voter registration data should be used to protect the personal identifying information that is stored in the voter registration database and used to authenticate voters.
- Removable storage media (e.g., USB drives, compact flash cards) used to handle sensitive election data should be obtained from a trusted source and erased before being used. To the extent practical, removable storage media should be new.
- Follow the domain security best practices issued by the Federal Government available at https://home.dotgov.gov/management/security-best-practices/

FAX

Facsimile (fax) machines are often used by local election offices and voters. While this may be a convenient tool for distributing or receiving ballots, policy makers should be aware of the risks and challenges associated with fax. Fax has no security protections unless sent over a secured phone line and is generally not considered suitable for sensitive communications. Faxes may be viewed or intercepted by malicious actors with access to phone lines. Furthermore, multipurpose fax machines with networked communications capability can be leveraged by cyber actors to compromise other machines on the network. We recommend election officials using fax machines implement the following best practices.

- Use a no-frills fax machine; multipurpose fax machines typically have modems for external network communications. If you only have a multipurpose fax machine, turn off the Wi-Fi capability and do not plug it into the network—only connect it to the phone line.
- Check the configuration to make sure that the fax cannot print more pages than anticipated from a single fax or ballot package.
- Use a dedicated fax machine and fax line for the distribution and receipt of ballots. Do not make the phone number publicly available, and only provide it in the electronic ballot package for voters who have been authorized to vote using electronic return.
- Election officials should set up transmission reports when faxing a ballot package to the voter to verify that the ballot package was received by the fax machine it was sent to.
- Use a trusted fax machine that has been under your control. Ensure you have enough fax machines and phone lines to handle the anticipated volume.
- When a public switch telephone line (PSTN) fax machine is not available and internet Protocols are used to fax, treat these systems as internet-connected systems, not as a fax machine using telephone protocols.

EMAIL

Email is a nearly ubiquitous communications medium and is widely used by election offices and voters. While this may be a convenient tool for distributing or receiving ballots, policy makers and election officials should be aware of the risks and challenges associated with email. Email provides limited security protections and is generally not considered suitable for sensitive communications. Email may be viewed or tampered with at multiple places in the transmission

process, and emails can also be forged to appear as if they were sent from a different address. Furthermore, email is often used in cyberattacks on organizations, such as attackers sending messages with malicious links or attachments to infect computers with malware. This malware could spread to other machines on the network if strong network segmentation techniques are not used.

- Use a dedicated computer that is separated from the remainder of the election infrastructure to receive and process these ballots. For very small offices that may not have the resources to use a dedicated computer, a virtual machine should be installed to separate these devices.
- Patch and configure the computer—as well as document viewer software—against known vulnerabilities (e.g., disable active content, including JavaScript and macros.).
- If possible, implement the .gov top-level domain (TLD). The .gov TLD was established to identify U.S.-based government organizations on the internet.
- Use encryption where possible (e.g., implement STARTTLS on your email servers to create a secure connection, encrypt attached files, etc.)
- Implement Domain-based Message Authentication, Reporting and Conformance (DMARC) to help identify phishing emails.
- Implement DMARC, DomainKeys Identified Mail (DKIM), and Sender Policy Framework (SPF) on emails to help authenticate emails sent to voters.
- Utilize anti-malware detection and encourage voters to as well. Make sure to update the anti-malware regularly.
- Implement multi-factor authentication (MFA) on any email system used by election officials.
- Follow best practices for generating and protecting passwords and other authentication credentials.
- Use a dedicated, shared email address for receiving ballots, such as Ballots@County.Gov. Implement naming conventions in subject lines that will help identify emails as legitimate (e.g., 2020 Presidential General). While a dedicated, shared email account is typically not a best practice, in this instance, it segregates potentially malicious attachments from the network.

WEB-BASED PORTALS, FILE SERVERS, AND APPLICATIONS

Websites may provide accessible and user-friendly methods for transmitting ballots and other election data. While web applications support stronger security mechanisms than email, they are still vulnerable to cyberattacks. Software vulnerabilities in web applications could allow attackers to modify, read, or delete sensitive information, or to gain access to other systems in the elections infrastructure. Sites that receive public input, such as web forms or uploaded files, may be particularly vulnerable to such attacks and should be used only after careful consideration of the risks, mitigations, and security/software engineering practices that went into that software.

- Avoid using knowledge-based authentication (e.g., address, driver's license number, social security number). To the extent practical, implement MFA for employees and voters and mandate MFA for all system administrators and other technical staff (including contractors).
- Patch and configure computers as well as document viewer software against known vulnerabilities (i.e., disable active content, including JavaScript and macros.).

- If possible, implement the .gov top-level domain (TLD). The .gov TLD was established to identify US-based government organizations on the internet.
- Use secure coding practices (e.g., sanitized inputs, parameter checking) for web applications.
- Encrypt traffic using Hypertext Transfer Protocol Secure (HTTPS) supporting Transport Layer Security (TLS) version 1.2. If you use a file server, ensure it uses a secure file transfer protocol, such as SFTP or FTPS.
- Ensure you have the bandwidth/capacity to handle the anticipated volume of traffic.
- Obtain outside cybersecurity assessments, such as CISA vulnerability scanning and remote penetration testing.
- Develop a vulnerability management program (VMP). This allows well-meaning cybersecurity researchers to find and disclose vulnerabilities privately to an election official, giving the election official time to implement upgrades and patches before disclosing the information publicly.
- Place the application on a network that is continuously monitored, such as the network with a web application firewall, an Albert sensor, or an intrusion detection and prevention system.
- Carefully vet any third-party companies or contractors obtaining system access to perform security assessments or regular maintenance.
- Inform voters to only download the application from the trusted mobile application store.
- Encourage voters to use a trusted network and not an open Wi-Fi network.

RESOURCES

- CISA services can be located in the CISA Election Infrastructure Security Resource Guide. All services can be requested at cisaservicedesk@cisa.dhs.gov.
- Become an EI-ISAC Member by going to https://www.cisecurity.org/ei-isac/.
- CISA's Binding Operational Directive (BOD)18-01 addresses enhancing email and web security.
- NIST Activities on UOCAVA Voting
- NIST special publication (SP) 800-177 provides recommendations and guidelines for enhancing trust in email.
- NIST SP 800-52r2 provides guidelines for selection, configuration, and use of TLS.
- FBI's Protected Voices initiative provides information and guidance on cybersecurity and foreign influence topics.
- The EAC's Election Security Preparedness webpage collects multiple resources that can assist election administrators.
- For more information about how election jurisdictions in the United States vote remotely, please see Uniformed and Overseas Citizens Absentee Voting Act Registration and Voting Processes.

APPENDIX: DETAILED RISK MAPPING

TECHNOLOGY	ELECTRONIC BALLOT DELIVERY	ELECTRONIC BALLOT MARKING	ELECTRONIC BALLOT RETURN
RISK: Exploitation of software flaws in election infrastructure			
Fax	Low	N/A	N/A
Email	Moderate	Moderate	High
Web	High	High	High
RISK: Unauthorized modification(s) to blank ballots			
Fax	Low	N/A	N/A
Email	Moderate	Moderate	N/A
Web	Low	Moderate	N/A
RISK: Loss of voted ballot integrity			
Fax	N/A	N/A	High
Email	N/A	N/A	High
Web	N/A	N/A	High
Risk: Loss of ballot secrecy			
Fax	N/A	N/A	Moderate
Email	N/A	N/A	High
Web	N/A	N/A	High
RISK: Unauthorized individual participates in voting channel			
Fax	Moderate	N/A	High
Email	Low	Low	High
Web	Low	Moderate	High

TECHNOLOGY	ELECTRONIC BALLOT DELIVERY	ELECTRONIC BALLOT MARKING	ELECTRONIC BALLOT RETURN
Risk: Broken Chain of Custody			
Fax	Low	N/A	Moderate
Email	Moderate	Moderate	High
Web	Low	Moderate	Moderate
RISK: Unable to access system or obtain ballot			
Fax	Low	N/A	Moderate
Email	Moderate	Moderate	High
Web	Moderate	High	High