Online Voting: An Equity Balance for the 2020 Election

August 13, 2020

Authors: Jack Cable, Sydney Frankenberg, Adriana Stephan, Pierce Lowary, Alex Zaheer, Matthew Isaac Frank, and Tom Westphal

Table of Contents

Executive Summary

This memo evaluates the risks of providing online voting to mitigate the risk of transmitting COVID-19 while conducting the November 2020 general election. We provide a brief history of online voting, evaluate recent attempts to implement online voting, highlight the potential benefits and risks, and ultimately discourage the use of online voting in this election.

We begin by illustrating the path that online voting has taken to reach its current form. Internet voting in the United States began as early 2000 and has been used as recently as this year's primaries in West Virginia. We additionally outline the major funding sources for recent online voting pilots.

Although we recommend against the adoption of online voting for the 2020 presidential election, we nonetheless evaluate the rationales offered by its defenders. Traditionally, proponents argue online voting can make the ballot more accessible to those with disabilities and members of the military and other overseas voters. In normal circumstances, supporters claim that online voting increases turnout by removing barriers to voting such as inaccessibility and inconvenience. Recent studies sponsored by online voting supporters have suggested that online voting has a significant effect on electoral participation. During a pandemic, online voting offers an attractive alternative to in-person voting. There are, however, persistent concerns over the negative effects that online voting may have on the electorate, such as potentially reduced trust in the accuracy of electoral counts and a demographic divide in who can effectively use the technologies.

Despite hope in certain quarters, the broad consensus in the security community remains the same: online voting is simply not ready for large-scale implementation. Platforms will have to resolve several issues before they are ready for mass adoption. These include the difficulty of authenticating voters, the potential presence of malware on the voter's device, and the impossibility of preventing online voting servers from compromise. In addition to these fundamental security concerns, the strained relationship between online voting vendors and the security community casts a pall on the effort to certify the integrity of online voting systems.

Finally, we give an overall recommendation that considers both the security risks and the demand for an alternative voting method given the current health crisis, suggesting that online voting should not be implemented in favor of other systems that can offer both accessibility and security, such as Remote Accessible Vote By Mail (RAVBM). In the case that online voting is employed by a jurisdiction in the November election, we provide suggested techniques and frameworks to mitigate security threats and maximize integrity.

I. Online Voting: A Brief History

As the COVID-19 pandemic continues to sweep the United States, some election officials are considering a turn to online voting to ensure voters' safety while guaranteeing access to the franchise. To evaluate the merits of this proposal, we must first understand the significance of voters using the Internet to cast their ballots. In the long history of elections, the use of technology to aid in remote voting has been around for a relatively long time. The Department of Defense (DoD) authorized ballots by fax to aid service members during Operation Desert Storm. Two decades later, in 2006, 6 states legalized the use of vote by phone systems to cast ballots.

Many modern electronic voting systems were developed after President Ronald Reagan signed the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) into law. UOCAVA granted the federal government a way to provide U.S. citizens overseas a means to register and vote in federal elections from abroad. In 1988, President Reagan designated the Secretary of Defense as responsible for administering UOCAVA in EO 12642, consequently, multiple Secretaries of Defense have delegated the responsibilities for the Federal Voting Assistance Program (FVAP) to an FVAP Director within the DoD. In 2000, FVAP began experimenting with a project called "Voting Over the Internet" (VOI) to enable overseas members of the military to vote online in the Presidential election. This marked the first time any U.S. citizens used internet voting in a U.S. election and is the most significant federally-backed internet voting experiment in the US. Though only 84 votes were cast over the system, the election proved that the concept of Internet voting for overseas military personnel was viable. After the trial, DoD sought Congressional authority to try a larger test.

In 2002, Congress gave the FVAP their desired approval, and in Section 1604 of the 2002 National Defense Authorization Act which directed the Secretary of Defense to expand the VOI project. This expansion was conducted by the FVAP and known as the Secure Electronic Registration and Voting Experiment (SERVE). SERVE included fifty-five counties from seven states. FVAP brought in private companies to assist the project, including Accenture and VeriSign (who had both helped with the successful 2000 Arizona elections). To aid in assessing security risks, the FVAP established a SERVE Security Peer Review Group (SPRG) with 10 members from academia and industry, some of whom were known critics of internet voting. Four of these members were so passionate about the potentials for security risks that they wrote their own report separate from the suggested FVAP report and published an article in the New York Times that railed against the $22 million system. The project was widely considered to have failed to address security vulnerabilities, and DoD canceled the SERVE project prior to the November 2004 general election.

Problems continued to persist with the state-run technologies designed to enable those overseas to receive and cast their ballots, leading President Obama to sign the Military Overseas Voter Empowerment Act (MOVE) in 2009 which required states to provide absentee ballots to overseas military voters at least 45 days before elections were held. MOVE allowed online registration, online ballot request, and online ballot marking but required all ballots to be printed or sent by fax or mail or copied and pasted into an email format.

Innovation continued at the state and local levels as well. In 2008, soon-to-be West Virginia Secretary of State Natalie Tennant persuaded the state legislature to approve a true internet voting trial that brought in private companies Scytl and Everyone Counts. The companies offered their support for free and constructed a program similar to SERVE that made online voting available for overseas military voters in the 2010 primaries. Several public elections in 2009 used online voting, including a 2009 Board of Supervisors online voting project in King Conservation District in Washington State. In 2010, the Washington, D.C. Board of Elections and Ethics experimented with an internet voting system with an inexperienced nonprofit group and invited anyone to test the system. A professor and a group of graduate students from the University of Michigan took on the challenge and were able to take complete control of the system within 48 hours. This exercise reinforced the inherent insecurity of internet voting.

Many internet voting systems receive state funding, but others are private ventures. In 2017, Tusk/Montgomery Philanthropies (TMP), a nonprofit run by venture capitalist Bradley Tusk, launched an initiative to draw attention to what they considered the need for citizens and elected officials to have access to mobile voting systems. TMP has helped fund almost all modern internet voting systems. Tusk told NPR that "he hopes to fund between 35 and 50 mobile-voting pilots over the coming five years and then campaign for even wider use based on the data compiled from those programs." In 2018, TMP partnered with blockchain voting vendor Voatz to run a pilot in two counties in West Virginia, designed to allow active duty service members, their spouses, and their dependents to vote in the May 2018 primary elections.

When Voatz was used in the West Virginia primary in 2018, it had not been certified by the Election Assistance Commission. By 2018, more than 70,000 voters had used Voatz in elections ranging from labor union and university elections to state party conventions and town meetings. Voatz uses a third party vendor for voter identification and verification. It claims to use a permissioned blockchain to ensure security, though the consensus of security experts is that this alone does not solve the fundamental risks of online voting. As of July 2020, Voatz still has not been certified by the EAC, and recently the EAC issued a press release stating that it does not certify online voting systems.

Recently, issues were discovered with the Voatz mobile app previously used in West Virginia. After a number of problems were discovered with Voatz, West Virginia dropped the online voting vendor.

Another online voting system backed by TMP is Democracy Live, a Seattle-based company that administers voting technology. While the company disputes whether its technology really is "internet voting," their software still transmits votes online. In January 2020, King County became the first county in the United States where every voter could cast a ballot using their smartphone in a minor election. The new technology was used for a board of supervisors election, an election that typically draws in around 1% of the eligible voting population, and was in part funded by TMP. Turnout nearly doubled at the election, though only to 2% and concerns remain over the ability to audit results.

In March, amidst the ongoing coronavirus pandemic, Congress's stimulus package included $400 million in federal grants to help states safely conduct the 2020 election. The law states the grants are intended to assist states in mitigating the effects of the coronavirus for the 2020 Federal election cycle. The Acting Executive Director of the EAC has clarified that states may use these funds for internet voting.

COVID-19 is forcing many states to seek out new forms of remote voting. This has largely meant states will increase and bolster their existing infrastructures for vote-by-mail. These same impulses, however, may lead some to consider the viability of internet voting. This brief history and the security details to follow aim to convince readers that there are crucial differences between these two approaches. Moreover, internet voting remains insecure and lacks the requisite paper trail necessary for ballot verification and overall election transparency.

II. Arguments For Online Voting Adoption

Election administrators considering online voting systems must balance conflicting equities. On the one hand, online voting might increase voters' access to their ballots at a time when in-person voting has been made much more difficult. On the other, there is an overwhelming consensus among experts that this technology is not ready for widespread use due to security concerns. To reconcile these tradeoffs, we evaluate the purported positives of online voting in the section below.

A. Online voting might improve access for vulnerable groups

Independent of the COVID-19 pandemic, online voting advocates have argued that it enfranchises two disadvantaged groups of voters: (1) voters with disabilities, and (2) U.S. military members and other overseas citizens. Both groups have difficulty accessing in-person and postal voting options (albeit for different reasons), and both are granted special voter protections by federal statute. We briefly examine these groups in turn.

Voters with disabilities are often the primary audience for jurisdictions considering online voting, because many find either in-person polling and voting by mail difficult. Federal law requires states to take measures to ensure voters with physical disabilities can access polling spaces and mandates special voting machines are made available to accommodate voters with certain disabilities. Despite those accommodations, some voters with physical disabilities are simply unable to cast their ballot in person. They may prefer to vote from home.

But for voters with some types of disabilities, vote-by-mail paper ballots may be equally disenfranchising. Such voters often find it difficult to mark paper ballots without assistance and rely on the technology and assistance offered by in-person voting options. This segment of the disability community is often at the forefront of efforts to preserve robust in-person voting options. However, voting options such as Remote Accessible Vote-by-Mail (RAVBM) offer a viable alternative by allowing voters with specific disabilities to fill out their ballots remotely, by allowing voters with disabilities to access their ballot in a screen-readable format using either visual or other dexterity-aiding tools to allow them the ability to fill out their ballot, and then print and mail it in. This combines the convenience of computers to aid in filling out ballots with the security of maintaining a paper trail for individual ballots. Of course, RAVBM is not without equity and accessibility concerns (voters must still print and mail ballots) or security concerns (attacks could distribute incorrect ballots or deny voters from accessing their ballots) though the method offers a viable middle ground of maintaining accessibility while preserving reasonable security.

Online voting may be seen as a way to simultaneously serve a diverse array of voters with disabilities. Online voting systems can offer easy physical access to the ballot while providing similar accessibility options present during in-person voting systems. With jurisdictions restricting in-person voting options due to public health concerns, this argument may have increased salience in the Coronavirus era.

Other jurisdictions may be interested in online voting to help U.S. military and overseas citizen voters. These voters are protected by UOCAVA, but they face many challenges, most importantly the

long transmission times associated with traditional postal absentee voting. These voters must request and return ballots well in advance of Election Day or risk having their ballot arrive too late to be counted. If voting were instantaneously accessible from anywhere with an internet connection, UOCAVA voters could be guaranteed the same access to absentee voting as other voters.

B. Online voting may increase turnout

While internet voting remains a relatively unexplored way to reduce the transaction costs associated with voting by improving convenience, it is unclear if providing an internet voting option actually improves turnout. There are very limited case studies of online voting in the United States, as internet voting has rarely been implemented in major U.S. elections. U.S. government-sponsored internet voting projects have largely focused on absentee voting for members of the Uniformed Services stationed abroad.

The Arizona Democratic Party became the first U.S. election administration office to implement online voting during the 2000 Democratic presidential primary. Registered Democratic voters received personal identification numbers in the mail. To cast their ballot, voters logged on to one of two websites, run by the Democratic Party and Election.com, which required entering the PIN, and answering two personal questions. Once verified, the ballot appeared and the voters were free to cast their vote. When given the option to vote online, the highest percentage of ballots cast were cast using remote internet voting (41%), followed by vote-by-mail and in-person voting. While overall voter turnout remained quite low, this could be due to the fact that the Democratic presidential race was already decided by the time Arizona Democrats voted.

West Virginia became the first U.S. state to implement mobile voting by allowing it for overseas voters in the 2018 primaries. Following pilots in two counties for the primary election, West Virginia partnered with Voatz to allow counties to opt into offering a mobile voting option for the November State Senate election. 24 of the state's 55 counties allowed mobile voting for overseas citizens. Voters were required to submit a Federal Post Card Application under UOCAVA. Following approval, voters were given the option of submitting ballots via mail, fax, scan, email, or (if the voter resided in one of the 24 participating counties) to download the Voatz mobile app and submit their ballot online using the app. A recent study of online voting in the 2018 West Virginia federal election, funded by Tusk Philanthropies and the Chicago Harris Cyber Policy Initiative, suggests that mobile voting increased turnout among UOCAVA-eligible voters by 4%. The results also suggest that almost half the individuals using the app were induced to vote because of mobile voting.

The two U.S. case studies highlight two potential drawbacks of implementing online voting on a wider scale: security concerns may dissuade voters from taking advantage of online voting, and the digital divide may affect voter turnout in ways that yield disparities in demographic representation. According to a 2018 U.S. public opinion poll of voting-age Americans, in comparing online to other voting technologies, respondents reported being least confident that votes cast online would be counted correctly and least likely to utilize online voting. Following the implementation of online voting in the Arizona Presidential Primary, one study showed that those on the wrong side of the digital divide (women, the elderly, racial minorities, the unemployed, and rural residents) were less likely to engage in internet voting.

C. Voting online may be cheaper

Due to the complexity of administering elections and the multiple levels of government from which funding is derived, it is difficult to know precisely how much it costs to run elections in the United States. Even the most basic facts about the cost of finance of elections are unavailable. A recent MIT Election Data and Science Lab study estimates the cost of election administration from 26 states is $8.10 per voter. According to a National Conference of State Legislatures report, the technological and security needs of new voting equipment are driving increased costs of election administration.

Advocates of online voting argue it could stem the tide of rising costs. These claims, however, remain largely untested. No studies yet address the cost-effectiveness of online voting in the United States, as the instances of online voting are very rare. In the United States, government-sponsored internet voting projects have predominantly focused on absentee voting. Estonia, however, is leading the development of e-government and internet-based voting tools. Estonian elections allow for a comparative cost framework of voting methodologies that could be useful in understanding how online voting might affect voting costs in the U.S. context. A study of local elections in Estonia in 2017 found internet voting to be the most cost-effective and cheapest (in terms of cost per voter) voting channel when compared to other voting options (advance voting in county centers or polling stations, early voting in county centers, election day voting in county centers, and election day voting in county centers or polling stations). The costs per voter, estimated to be €2.32 per vote, was based on two factors: the resources consumed and the number of people opting to use the voting channel. Notably, vote-by-mail was only available to overseas voters and a cost comparison of vote-by-mail and internet voting was not possible.

The Brennan Center for Justice estimates the total cost of guaranteeing vote-by-mail is available to all U.S. voters in the 2020 general election at $982 million-$1.4 billion. This would include ballot printing, postage costs, drop boxes for absentee ballots and appropriate security, secure

electronic absentee ballot request technology, ballot tracking, improvements to absentee ballot processing, and additional facilities and staff. The lack of data on the costs of online voting systems makes estimating the potential input costs of implementing online voting during the general election difficult. Analysis must cover the cost of providing digital signatures or biometric authentication, designing new systems, pen-testing systems, technical support, and the implementation of a new audit system. Other costs might include a public education campaign on how online voting would work during the general election and the cost of an emergency response team to detect and mitigate attacks, similar to that of Estonia.

D. COVID-19 presents serious accessibility concerns

Election officials are facing unprecedented challenges in the administration of the 2020 general election. As a result of concerns arising from COVID-19, seventeen states postponed primary elections. Voters are concerned about the safety of voting in-person, and many states are searching for alternatives to in-person voting. State contingency plans address considerations, such as poll worker shortages, communications between state and local officials, and public education as to changes of the voting process, such as polling place consolidations and reassignments. If the primaries are any indication, more than half of Americans could vote by mail in the 2020 general election.

Several states are using election security funds allocated in the CARES Act to cover unanticipated costs resulting from COVID-19. In spite of federal guidelines outlining the risks of electronic ballot return, some states turned to internet voting options in the midst of the crisis. West Virginia, Delaware, and New Jersey allowed voters with disabilities and overseas and military voters to submit their votes online via Democracy Live's online voting system. Both Delaware and New Jersey have since withdrawn plans to utilize Democracy Live's system for the 2020 general election, citing security concerns.

III. Security Concerns

A. Security Community Reactions

The reaction of the electronic security community to proposals to broaden the usage of online voting has been quite negative. From the American Association for the Advancement of Science (AAAS) and the National Academies of Science, Engineering, and Medicine (NAS) to Verified Voting and Common Cause, elections and cybersecurity experts have strongly advocated against internet

voting, specifically electronic ballot return. Whatever online voting's benefits may be, it incurs unacceptably high risks to the confidentiality and trustworthiness of voters' data and their ballots.

Security experts detail multiple concerns, from malware to the need to authenticate voters and audit results, that jeopardize the security of elections. The difficulty in meeting these concerns — which Common Cause describes as "insoluble" issues "inherent" with online voting — is compounded by the fact that at present, every layer of the system of systems comprising internet voting needs to be verifiably secure and unaltered. Such a complex system of systems will inevitably present a massive attack surface and innate vulnerabilities, due to flaws in design, human oversight, and the supply chains and dependencies relied upon by the hardware and software involved. But even as these major risks are present, the National Academies assert that "no technical mechanism" exists at present to verify the security of every layer of the system. Therefore, there is currently no technical mechanism that can ensure that the results of internet voting are accurate.

As the NAS Report emphasizes, malicious actors may undermine the integrity of elections in myriad ways, from compromising the process of recording and tallying ballots to making it impossible to adequately verify results. Additionally, given that small changes in vote totals can swing election outcomes, the lack of a voter-verified paper audit trail could make it impossible to know such changes even took place. Implementing an audit trail would be effectively equivalent to sending an ordinary mail ballot, largely nullifying the advantages of online voting. As Verified Voting reiterates, online voting does not fulfill the stringent security, privacy, and transparency requirements of elections.

For these reasons and others, the National Academies' report, which the AAAS labeled the "most definitive and comprehensive report on the scientific evidence behind voting security in the U.S.," stated that internet voting "should not be used" now or in the future "until and unless very robust guarantees of security and verifiability are developed and in place." Similarly, the Cybersecurity and Infrastructure Security Agency, itself referencing the NAS report, stated electronic ballot return is "high-risk even with controls in place." Given all the risks inherent in online voting, the National Academies Report unsurprisingly recommends against its deployment at any time in the near future..

B. Technical Concerns

Unlike other areas of daily life that can be conducted with reasonable expectations of security online, internet voting must satisfy two conflicting requirements. Elections must be secret, such that voters' choices cannot be tied to them, yet verifiable, such that any errors or tampering can be detected and resolved. In contrast, banking—an activity that can be conducted online with reasonable expectations of security—has no such anonymity requirements. Hence, banks may deploy advanced

systems to detect compromise and fraud based on transaction information. The banking system is verifiable: individuals can detect when compromise occurs and report it to their bank. And if large-scale compromise occurs, the bank can accept the risk, factoring the loss into their bottom line. In an online election, the public is left to accept the unacceptably high risk of compromise, which could mean erroneous selection of a candidate to the sought-after office despite his or her opponent actually winning.

There are several technical barriers that computer scientists must address for internet voting to be feasible. The first is authentication, verifying that voters are indeed who they claim to be. Unlike Estonia's online voting system, which utilizes a national ID card system to digitally verify voters, the United States has no such public key infrastructure. Existing online voting systems are instead left to piece together authentication, such as relying on a voter's name, birthdate, and signature, or a third-party identity verification provider. In the first case, given that voter registration lists are publicly available, an attacker could fraudulently submit a ballot for any registered voter. In the latter, a third-party service is inherently unaccountable and may itself be the target of attacks. Furthermore, given controversy regarding voter ID laws in the United States, any method of authenticating voters must also not institute prohibitive barriers that exclude legitimate voters from participating. Thus, any current internet voting system cannot prevent adversaries from casting fraudulent ballots while simultaneously allowing all voters to participate.

Second, unlike in-person or mail-in balloting, online voting does not leave a voter-verified paper trail. Such a paper trail is necessary in order to audit election results when software cannot be trusted. As a result, compromise of voter devices or the servers hosting voting systems could lead to changes in outcomes for which no amount of auditing can detect. Malware present on a voter's device can covertly hijack the voting flow such that a voter's cast ballot differs from their intended selection. Even anti-malware software intended to detect compromise can be subverted, meaning that voting vendors and election officials have no method of knowing if interference has occurred. Malware need not exploit novel vulnerabilities in order to be harmful: malicious applications masquerading as others, such as desktop applications or browser extensions, could offer a route to changing a citizen's vote.

Likewise, compromise at the server level could allow changing the results of an election at scale. No amount of testing can eliminate all flaws from a system. As seen with the Voatz system, despite promises that votes were immutably stored via a blockchain, server compromise before the blockchain would allow an attacker to modify or reveal any voter's ballot. Blockchain cannot address the fundamental difficulties associated with internet voting, and may even introduce additional areas for attackers to target.

In order to overcome the difficulty of securing software, academic experts have introduced the concept of *end-to-end verifiability* (E2E-V), which requires that elections are verifiable even when the software and hardware used to conduct them are untrusted. In election literature, E2E-V is viewed as a prerequisite for any internet voting system that is to be deployed. Unfortunately, decades of research also conclude that no end-to-end verifiable online voting system is robust enough to be widely deployed. As it stands, the expert consensus is that voter-verified paper ballots are the only robust method to achieve E2E-V.

C. Vendor-Specific Concerns

Voatz, the blockchain-based mobile voting vendor, garnered attention in October 2019 when a University of Michigan student was referred to the FBI for an alleged hacking attempt of its infrastructure. Despite the student allegedly operating within terms of Voatz's bug bounty program, Voatz aimed to frame this act of security research as an attempted intrusion. Being receptive to security research is crucial to ensure the integrity of any software system, even more so for a critical voting system. Voatz would later become the first company to be removed from the platform HackerOne for its actions against security researchers.

Little was known about Voatz's security practices prior to an MIT paper released in February 2020. In the study, the authors systematically dispute many of Voatz's security claims. They point out that a blockchain alone cannot ensure the integrity of internet-submitted votes, client-side malware remains a real threat, and that even a passive attacker may infer a voter's selection. Voatz disputed this research, releasing a blog post entitled "Voatz Response to Researchers' Flawed Report" in which Voatz denounced the researchers' "bad faith" report. A report by the security firm Trail of Bits, commissioned by Voatz and Tusk Philanthropies, would later confirm the MIT researchers' findings in addition to discovering 79 additional vulnerabilities.

A second vendor, Democracy Live, has garnered attention following the exposure of Voatz's poor security. Analysts lack information about Democracy Live's systems and security: To date, no commissioned, white-box security assessment of Democracy Live's systems has been published. A report by researchers from MIT and the University of Michigan is the first public analysis of Democracy Live's OmniBallot system, which scrutinizes the system based on the publicly-available voter interface. The report concludes that, as with any internet voting system, Democracy Live cannot prevent malware on a voter's device from modifying votes, and notes the large amount of voter data collected by the company. Furthermore, the authors identify a flaw where votes cast offline, intended to be printed, would still be sent to Democracy Live's servers.

Perhaps due to criticisms of online voting and the scientific consensus that no online voting system is auditable, Democracy Live claims that its platform "is not an online voting system." This statement has been repeated by Democracy Live's customers in the past, with the Delaware election commissioner stating Democracy Live "is not internet or online voting." Democracy Live's reasoning is that ballots are printed by the election administrator after voting occurs and then tabulated. Despite this, however, as stated by the MIT and University of Michigan report, "when ballots are returned over the Internet using OmniBallot, there is no way for voters to confirm that their votes have been transmitted without modification." Although the company points to AWS's Object Lock to ensure immutable storage of ballots, an adversary may still change ballots by compromising voter devices or targeting flaws in Democracy Live's servers before ballots reach storage.

IV. Mitigation

Due to significant security concerns, as well as the paucity of open research that validates vendors' security claims, voters in 2020 cannot vote online using available systems and be confident their vote will be cast and counted as intended. Given the state of the available products for this election and the seemingly non-addressable points of insecurity in the available online voting systems, these systems cannot be considered secure in time for November.

Additionally, while these systems might help enfranchise populations such as the disabled and deployed military communities, these communities can also be served effectively by vote-by-mail albeit with some accommodation. Vendors may position this technology as the only solution to ensuring all citizens can vote, but these claims must be rigorously investigated, and alternatives must be strongly considered.

Despite the above concerns, election officials may still employ online voting systems in the 2020 election. Below, we outline three actions that, if adopted, would attempt to mitigate the risks associated with this technology.

A. Limit Availability

In the jurisdictions in which they are used, online voting systems should be available in only limited capacities in the 2020 general election. Their usage should be no greater than what has been tested in previous trials. First, so far, online voting systems have been available to only small subsets of the population, and mostly in lower-profile contests where they could be monitored heavily. Second, as identified above, few public audits of the vulnerability of these systems are available to election officials,

making well-informed risk calculations impossible for this election. Given these points, the high-profile nature of this election, and the compounding logistical challenges due to COVID-19, election officials should avoid pushing online voting systems beyond what has been publicly tested. They therefore should grant access to this form of voting only when absolutely necessary.

B. Implement Remote Accessible Vote-by-Mail (RAVBM)

If insecurities in online voting lie in ballot delivery, a partially virtual ballot system could serve as a safer compromise. Remote Accessible Vote-by-Mail (RAVBM) may bridge the gap between accessibility and security. RAVBM, widely implemented in several states for registered voters with a disability, is a hybrid system that combines online voting access with mail-in or physical ballot transmission. The system was designed to allow voters with vision or dexterity disabilities to be able to vote from home. Many voters with disabilities have mechanisms on their home computers that assist them in reading and filling out forms. RAVB allows these voters to use these same tools and apply them to filling out their ballots. Through RAVBM, voters mark their ballot on their computer (such as via a PDF or web interface) and then print and mail the ballot or bring it to a polling center to drop off.

RAVBM combines the convenience of receiving a ballot online, eliminating the tedious and expensive step of having states pay third parties to print and mail out individual ballots, with the back-end security of mail-in or in-person voting. While some security concerns are still present, the risk is much lower, as a paper trail exists and the paper ballot can be verified before mailing. This system is not a panacea for accessibility concerns—voters still must be able to print and mail their ballot or be able to get to a polling center to drop off their ballot—but the system offers much greater integrity while aiding accessibility. As of January 2020, the California Secretary of State had conditionally approved three RAVBM voting systems for the upcoming elections, Democracy Live Secure Select 1.2.2 (the same company that makes online voting systems), Five Cedars Group Alternate Format Ballot (AFB) v5.2.1 and Dominion ImageCast Remote 5.2. Recently, Michigan's Secretary of State has made moves to implement RAVBM for voters with specific disabilities state-wide. The state has been rapidly working to find vendors able to create the web interfaces fast enough to use in their August 2020 elections, and they have encountered some pushback as some citizens do not think the state is working fast enough to accommodate blind voters.

We believe the three RAVBM voting systems approved by California could be implemented in other states. Though online voting remains insecure, RAVBM faces far fewer security threats. We strongly urge states to consider strengthening their existing RAVBM infrastructure for voters with disabilities instead of using an online voting system.

C. Require Open and Independent Security Audits Before Use

Lastly, election officials should require public audits of internet voting technologies conducted by reputable third-party security firms. Rather than a simple "seal of approval," such assessments should include critical scrutiny of the voting system and full information of vulnerabilities discovered. Officials should also pay close attention to the type of assessment that occurred. Both Voatz and Democracy Live, for instance, have engaged audits by the National Cybersecurity Center and Shiftstate security, the former of which provides a non-security, functionality-only audit, and the latter which only appears to assess network-level security (as opposed to that of the voting application itself). The Trail of Bits Voatz assessment is perhaps the only public white-box assessment that has been conducted of online voting technology in use in the United States and should serve as a model for future reports moving forward. Of course, no amount of testing can address the fundamental insecurities of online voting described above, though having untested technology deployed in live elections only risks worse outcomes.