FROM: Twenty election cybersecurity experts

DATE: March 7, 2024

TO: Honorable Cris Dush*, Chair of the State Government Committee of the Senate*
Honorable Amanda M. Cappelletti, *Minority Chair of the State Government Committee of the Senate*
Honorable Carol Hill-Evans, *Chair of the State Government Committee of the House of Representatives*
Honorable Brad Roae, *Minority Chair of the State Government Committee of the House of Representatives*

We, the undersigned, representing a community of computer scientists, election integrity specialists, and data security analysts who wish to see enhanced data privacy, cybersecurity, and election integrity standards adopted by the Pennsylvania Legislature, are writing to express our concerns about the current use of certain voting machines in Pennsylvania, and to recommend best practices for your consideration.

Like much of society, election operations have become reliant on computers such as optical-scan voting machines, touchscreen ballot-marking devices, e-pollbooks, and election-management software. These devices carry advantages and disadvantages whose tradeoffs must be assessed and balanced by legislators.

This letter assesses the advantages and risks of electronic voting technology from a computing science perspective that balances the tremendous power of computers against the risks of cyber threats as these competing concepts relate to elections. Here, we focus on vote tabulators and ballot-marking devices. Our goal is to help inform and advise state legislators who are making legislative decisions about best practices in selecting technology for use in elections.

Our concerns demonstrably predate and transcend the concerns of any one political party or candidate. We represent a variety of political and social views, and therefore believe our recommendations represent a truly nonpartisan scientific perspective.

Suggested Principles for State Statutes Regarding Ballot Marking and Vote Tabulation

Executive Summary

We believe that the goal of laws, regulations and directives relating to elections must be focused on fairness, security, transparency, and accessibility. Each state should strive to approach the gold standard in every category, so that no reasonable candidate or party may have grounds to object that the process was unfair, insecure, or compromised. The process must be transparent, so the public may be assured the winners won and the losers lost.

We believe that no system is perfect, with each having trade-offs. Hand-marked and hand-counted ballots remove the uncertainty introduced by use of electronic machinery and the ability of bad actors to exploit electronic vulnerabilities to remotely alter the results. However, some portion of voters mistakenly mark paper ballots in a manner that will not be counted in the way the voter intended, or which even voids the ballot. Hand-counts delay timely reporting of results, and introduce the possibility for human error, bias, or misinterpretation.

Technology introduces the means of efficient tabulation, but also introduces a manifold increase in complexity and sophistication of the process. This places the understanding of the process beyond the average person's understanding, which can foster distrust. It also opens the door to human or machine error, as well as exploitation by sophisticated and malicious actors.

Rather than assert that each component of the process can be made perfectly secure on its own, we believe the goal of each component of the elections process is to validate every other component.

Consequently, we believe that the hallmarks of a reliable and optimal election process are ***hand-marked paper ballots***, which are ***optically scanned***, ***separately and securely stored***, and ***rigorously audited*** after the election but before certification. We recommend state legislators adopt policies consistent with these guiding principles, which are further developed below.

Introduction

As computers and software play an increasingly central role in election technology, challenges to election results have sometimes arisen from concerns about the trustworthiness of complex computer technology. As election technology experts, we have seen no conclusive evidence that voting machines or other election technology have ever been maliciously used to alter votes or election results in the United States. We oppose efforts to reject election results based on speculative claims that vulnerabilities have been exploited. However, while we have not identified evidence sufficient to justify overturning of prior elections, neither can we rule out the possibility that malicious and sophisticated actors exploited voting machine vulnerabilities with sufficient skill as to conceal their tampering. Therefore, existing vulnerabilities in current voting systems urgently need to be addressed. States must act to reduce those vulnerabilities, both to provide higher assurance of accurate elections and to minimize controversies in the future.

This letter suggests principles that are accepted by many election technology experts for maximizing the credibility of elections. We suggest these as guidelines for legislation or regulatory action.

The overriding principle is that elections must produce reliable evidence that their outcomes—who gets elected, which ballot questions pass—reflect the will of the voters.

This goal must be achieved subject to the following *unavoidable* technological limitations:

1. Computers (including voting machines) *are* capable of being hacked or misprogrammed (software bugs).
2. No cybersecurity fixes can effectively and totally prevent this with high confidence.
3. Hacked (or misprogrammed) voting machines can deliberately (or mistakenly) miscount or misrecord votes.
4. When not hacked or misprogrammed, computers can be accurate and efficient tools for counting votes.
5. No audit process can reliably detect or correct faults that make their way into the final paper ballot pool.
6. In U.S. elections where there are many contests or questions on the ballot, humans counting votes by hand can itself be a source of inaccuracy or create opportunities for fraud.

Therefore, in our opinion, the most reliable way to ensure accurate elections (when there are several contests on the ballot) is for voters to mark paper ballots by hand in a local polling place; for optical-scan voting machines to count those ballots; and for an audit to check the outcomes before certification of results. The audit should include a manual examination of statistically appropriate samples of paper ballots cast.

Voting methods that depart from this model tend to compromise the security of the ballot pool or the privacy of the ballot.

Weaknesses of Electronic Voting Machines

It is impossible to ensure, with current technology, that voting machine software is free of errors or tampering. Even with the best present-day cybersecurity practices, it is impossible to absolutely prevent "hacks" that cause voting computers to run unauthorized software. *(See: Securing the Vote, p.90)* Even with the best present-day software development practices, it is impossible to guarantee that large software packages do not have flaws that have been undetected in testing and that might affect the output.

The consequences of such unauthorized software can include the deliberate and systematic misrecording or mis-tabulation of votes, with the possibility of altering election outcomes. Even when authorized software is used, errors in configuration (or intentional misconfiguration) of ballot files can cause substantial and systematic errors in tabulation, with the possibility of altering election outcomes. *(For example: Antrim County MI, 2020)*

Ballot Marking Devices

Some counties utilize ballot marking devices (BMDs), where the voter uses an electronic touch screen to mark a blank ballot. The BMD then prints a marked ballot card containing both barcodes and human-readable text for the voter to review. This ballot card is then inserted into an optical scanner which is sometimes integrated into the marking device.

These devices have inherent properties that particularly limit their trustworthiness and auditability when used by all voters to mark ballots.

Like all electronic voting machines, BMDs are not reliable against the danger of hacking or misprogramming. BMDs are different from (for example) optical-scan vote counters, which are used to scan paper ballots. If optical scanners are hacked, then an audit of the paper ballots can detect the hack and a recount can correct it.

Neither of these tools are possible with hacked BMDs, because BMDs are the means used to produce the marked ballot. Because a BMD attack could alter the votes recorded on the paper ballots with votes that the voters did not intend, audits or recounts cannot detect or correct some known hacking/attacks on BMDs.

Ballots marked by computerized BMD devices are subject to the serious problem that, if hacked or accidentally misconfigured, they can systematically print votes onto the ballot paper that were not the ones indicated by the voter. *(see: Ballot Marking Devices Cannot Assure the Will of the Voters)*

With diligence a voter might possibly be able to catch such errors. However, extensive observation and experimentation have shown that the vast majority of voters do not carefully check every vote printed on a ballot printed by a BMD. Thus, if a BMD were systematically misprinting votes onto the ballot paper, the majority of voters likely would not notice and would deposit such ballots for tabulation. Because the vote printed on the paper is not the vote indicated by the voter and these maliciously altered ballots would pollute the ballot pool, no subsequent recount or audit could detect, much less correct, this error. *(Tennessee voters reviewed their BMD-printed ballots for 2 seconds, on average; 93% of Michigan voters did not detect a* *fraudulent vote printed onto their BMD ballot; 81% of Georgia voters reviewed their BMD-printed ballot for less than 5 seconds.)*

If a BMD is hacked or accidentally misconfigured to print an incorrect ballot, the only remedy available to any voter who might notice is to request a second opportunity to vote, with the incorrect ballot voided. There is no remedy available that will correct mismarked ballots of voters who don't detect a problem. *(See: Ballot Marking Devices Cannot Assure the Will of the Voters)*

If some voters report that the BMD printed votes onto the ballot different from what they selected on the screen, it is difficult to tell whether the BMD is intermittently changing votes (because hacked) or whether the voters are mistaken in their recollections. (This is different from the case where the BMD *always* prints a wrong vote, which has happened from time to time, and which is easier to diagnose.)

Additionally, certain BMDs (such as the ExpressVoteXL) which print a ballot for review, and then deposit the ballot once approved by the voter, pass the cast ballot beneath the same printer heads which marked the paper ballot. Voting machines that can count ballots (such as optical scan vote counters) must not be *physically* capable (even if their software is hacked) of printing votes onto paper ballots (as BMDs do). The reason for this is that the main purpose of a paper ballot is for the vote indicated by the human voter, and seen by the human voter with their own eyes, to be identical to the vote that will be counted. If the vote-counting scanner is capable (when hacked) of printing new votes onto the ballot after the last time the voter has had an opportunity to see the ballot, then this most important purpose of a paper ballot is lost.

This rules out all-in-one voting machines that combine the function of BMDs and optical-scan vote counters. *(See: Serious design flaw in ESS ExpressVote touchscreen: "permission to cheat"; Reexamination of an all-in-one voting machine; ExpressVote XL "fix" doesn't fix anything)*

Therefore, we recommend that BMDs are not used in any precinct as the primary voting mechanism, but should be reserved for voters who require or request BMDs to assist with marking a paper ballot.

Votes Encoded in Barcodes

Of particular concern is the use of printed barcodes to scan and tally an elector's intent. Certain machines (such as the *ExpressVoteXL*) create a machine-printed ballot containing both human-readable text, and a barcode which is supposed to represent the same information in a digitally readable format. An elector is asked to review the human-readable portion to confirm his or her choices, but the machine ultimately scans the barcode. The standard optical-scan vote-counters for many BMDs count only the barcode, not the human readable vote. *(ES&S ExpressVote, ExpressVoteXL,* and some configurations of *Dominion ICX.)*

In cases where the barcode and human-readable portion disagree (as occurred in the November 2023 election in Northampton County), state statutes generally do not specify which is the official vote of record.[1] Moreover, it has already been the observed practice of some states to conduct recounts by rescanning the barcodes.

This produces a serious paradox: If the *human-readable* portion comprises the official vote of record, then machines are not utilizing it when tabulating official results. If the *barcode* comprises the official vote of record, then no voter can meaningfully review his or her vote of record. If there is more than one representation of the vote (for example, both a barcode and a human-readable text), a hacked or misconfigured BMD could print conflicting votes. This happened in a real election as recently as 2023. *(see: Election Problems in Northampton County, PA in November 2023*.)

In observed instances where a BMD produced a barcode corresponding to the voter's indication, and a human-readable vote different from the voter's indication, voters in that election were advised, while voting, to disregard the human-readable vote printed on their ballot by the BMD.

The principal purpose of the paper ballot is to provide a trustworthy record of the selections the voter indicated, in a way that can be seen by voters and human recounters or auditors. Therefore, to avoid these unacceptable situations, we recommend the vote should be marked on paper in human-readable form, and *only* in human-readable form, not barcodes or QR codes. (BMDs that meet this requirement have been available since 2006.)

Note: While barcodes should not be used to encode votes, in our opinion it is acceptable for them to be utilized for encoding ballot styles. Hand-markable optical-scan ballots sometimes contain a "ballot-style code" that indicates which election district the ballot is for, or which set of contests and candidates are on the ballot. These codes should be indicated both in human-readable and machine-readable form, such as a barcode. This is acceptable since such barcodes do not encode votes, but only the candidate-contest options on the ballot. (see: East Windsor Township ballot, annotated).

[1] One of the very few states that specifies explicitly whether the barcode or the human-readable text is the "real" vote is Georgia. By statute OCGA 21-2-300(a)(2), the tabulation of the QR code is what controls; on the other hand, there is a regulation that provides that if there's a discrepancy, the human readable portion controls. That's Rule 183-1-15-.02(2)(j). But other statutes and regulations severely limit the number and frequency of situations where one would even look for a discrepancy, and thus cause the human-readable portion to become the "vote of record" that is counted and tabulated. Thus, voters can have little confidence that what they can read on their own paper ballot is a vote that will actually be counted.

Internet Connectivity

Many electronic voting machines utilize off-the-shelf circuit boards that contain technology capable of connecting to the internet.

Some voting machines (whether optical scanners or ballot-marking devices) contain internal wireless radios, chips, modems, or hardware capable of wireless networking. We recommend against using voting machines with wireless radio components, even when such connectivity is supposedly disabled.

We strongly believe that permitting internet connectivity in voting machine hardware will inevitably lead to inappropriate usage. The mere presence of wireless capability introduces the risk of unintentional activation through misconfigurations, software updates, or technical errors. Moreover, even if wireless features are disabled, the networking hardware may remain enabled, creating a persistent vulnerability. As demonstrated in past instances such as the decertification of the WINVote voting machine by the Virginia Department of Elections due to its susceptibility to remote manipulation via wireless capability, relying on procedures and processes to prevent activation is naive and insufficient. Despite claims of cost advantages and convenience associated with using COTS devices with wireless networking capability, we assert that the security risks outweigh any perceived benefits.

Therefore, given the significantly increased risks of remote cyber-attacks on election-critical infrastructure, we recommend against the practice of permitting internal internet connectivity in any electronic machines used in the tabulation and storage of election results.

Hand-Marked Paper Ballots

Hand-marked paper ballots are the most trustworthy voting technology for recording voter intent.[2] While not immune to fraud or errors, paper cannot be hacked, and makes it harder for bad actors to tamper with elections, particularly from afar.

However, for efficiency and the reduction of human error in counting, computerized tabulation machines (if not themselves hacked or misconfigured) are generally accurate in counting votes, and not prone to the same biases or mistakes that humans may make in tabulating votes. The added benefit of computerized optical scanning followed by a hand audit or recount is that, in order to cheat without detection, a fraudster would have to hack the computer consistently with alterations to the pool of paper ballots.

[2] Hand-marked does not necessarily imply hand-counted. Hand-marked paper ballots can be counted by optical-scan computer or by hand. In elections where there are many contests or questions on the ballot, humans counting votes by hand can itself be a source of inaccuracy or create opportunities for fraud.

Therefore, the best practice in conducting elections is for voters to mark paper ballots by hand in their local polling place; for those paper ballots to be counted by optical-scan voting machines; and for those paper ballots to be used for rigorous post-election ballot audits, such as Risk Limiting Audits. *(See: Evidence-Based Elections: Create a Meaningful Paper Trail, then Audit)*

Election administrators should also follow best practices for ballot design that makes it easy for voters to express their choices. Ballots, whether hand-marked or viewed on a touchscreen, should be laid out in a way that avoids confusion. Studies have shown that certain bad practices in ballot design can cause a substantial fraction of voters to inadvertently fail to vote in some contests. Jurisdictions should follow the best practices in ballot design published by the U.S. Election Assistance Commission in "Effective Designs for the Administration of Federal Elections", June 2007. *(See: Florida is the Florida of ballot-design mistakes)*

Separate vote-marking from vote-counting

Vote-marking and vote-counting must be done separately from each other, else a hacked voting machine may be able to print fraudulent votes onto the ballot. It is then essential that the pool of voted ballots be kept demonstrably secure and well organized so that they remain a trustworthy record of voters' expressed preferences throughout the election and any subsequent audits. This requires a rigorous chain of custody and physical security throughout the voting process.
A thorough canvass, including ballot accounting, pollbook reconciliation, and eligibility verification, contributes to the trustworthiness of the collection of voted ballots. *(See: Evidence-Based Elections: Create a Meaningful Paper Trail, then Audit*)

Audits

Rather than assume that optical-scan voting machines (or even human teams of hand counters) have tabulated ballots perfectly accurately, elections should be subject to post-election, pre-certification audits. Risk-Limiting Audits are one statistical method by which an election outcome can be sampled to verify the recorded outcome corresponds to what's marked on the counted paper ballots.

When paper ballots are counted by computers (such as optical-scan voting machines), it is a good practice to conduct a risk-limiting audit or a by-hand recount before certifying results. Because by-hand recounts can be very labor-intensive, especially in larger jurisdictions, risk-limiting audits (RLA) may be preferable because they can achieve a higher level of confidence more efficiently. *(*See*: Principles and Best Practices for Post-Election Tabulation Audits)*

However, note that RLAs are not effective in detecting or correcting errors or attacks that pollute the ballot pool, such as BMD ballot errors or malicious attacks on the counted paper ballots.

Disability Accommodation

While we strongly support each of the preceding recommendations, we also recognize (and urge legislators to recognize) that some voters have disabilities that hinder them from marking a ballot by hand.

Such voters must be offered the use of an assistive technology in voting consistent with Federal law. While ballot-marking devices have inherent security vulnerabilities, they can often still serve a purpose as assistive technology for voters with vision or dexterity impairments that prevent them from independently marking a ballot by hand. *(*See*: Accommodating voters with disabilities)*

In such cases, where voters with disabilities are thus accommodated, we recommend protecting the privacy of such voters by requiring that their ballots are (as much as possible) indistinguishable from ballots marked by hand, especially if there are only a few BMD-marked ballots in a given election district. Therefore, BMDs that are provided for voters with disabilities should print all voted ballots in the same format as ballots marked by hand, to be counted by the same optical-scan voting machines or humans. Several vendors sell BMDs that mimic hand marked ballots.

Although BMDs may meaningfully accommodate those with disabilities who cannot express their intent with a pen and paper, we do not believe these devices should be the primary or exclusive means by which votes are recorded by voters who are able to mark a paper ballot by hand.

Conclusion

In summary, while technology provides efficiency and convenience, there are inherent risks of hacks, misprogramming, and miscounting of votes. Robust cybersecurity measures encoded into statute can help mitigate these risks. Ballot Marking Devices, especially all-in-one devices, present unique and inherent departures from best practices for electronic voting machines, and their use should be confined to accommodating those who are unable to mark their ballots by hand.

BMDs that print both human-readable text and barcodes pose a conflict for voters. No machine deployed in the future should be permitted to encode the official vote in barcodes. On printed ballots produced by BMDs, each vote must be indicated only once, and only in a form that is both human-readable and machine-scannable (not, for example, once as a barcode and once as printed text).

No voting machine should be physically capable (even in the presence of software error or malicious replacement of its software) of both scanning (tallying) votes and printing votes onto a paper ballot. Likewise, no voting machine should be physically capable of connecting to the internet, nor should any devices (such as USB or flash drives) be inserted into voting machines if they have previously been inserted into an internet-accessible device. Any voting machines capable of accessing the internet should be discontinued from use.

Hand-marked paper ballots should be the primary means of recording votes. Each polling-place voter, except those who request to use a BMD because they have difficulty marking a paper ballot by hand, should vote by marking by hand an optically scannable paper ballot. Ballot Marking Devices used as assistive devices should print a paper ballot identical in size and format to hand-marked paper ballots.

Paper ballots should be securely preserved and maintained through secure chain of custody measures. The vulnerabilities inherent in technology should be counterbalanced by incorporating non-technological verification methods, such as subjecting outcomes to statistically probative audits of the paper ballots.

While no system is perfect, and no system can guarantee an election will remain free from hacking, bias, or errors, these principles help strengthen confidence in elections, and mitigate known risks.

Signed,

(affiliations listed for identification purposes only and do not indicate institutional endorsement)

Andrew W. Appel, *Eugene Higgins Professor of Computer Science, Princeton University*

Matt Blaze, *Robert L. McDevitt, KSG, KCHS and Catherine H. McDevitt, LCHS Chair of Computer Science and Law, Georgetown University*

Duncan Buell, *Chair Emeritus – NCR Chair in Computer Science & Engineering, University of South Carolina*

Richard DeMillo, *Charlotte B & Roger C Warren Chair of Computing, Georgia Institute of Technology*

David L. Dill, *Donald E. Knuth Professor Emeritus in the School of Engineering, Stanford University*

J. Alex Halderman, *Bredt Family Professor of Computer Science & Engineering, Univ. of Michigan*

David R. Jefferson, *Lawrence Livermore National Laboratory (retired)*

Douglas W. Jones, *Associate Professor Emeritus, University of Iowa*

Douglas A. Kellner, *Kellner Herlihy Getty & Friedman LLP; former co-chair, N.Y. State Board of Elections*

Wenke Lee, *Professor and John P. Imlay Chair of Computer Science, Georgia Institute of Technology*

Daniel Lopresti, *Professor of Computer Science and Engineering, Lehigh University*

Ronald L. Rivest, *Institute Professor, MIT*

Bruce Schneier, *Lecturer and Fellow, Harvard Kennedy School*

Barbara Simons, *IBM Research (retired)*

Kevin Skoglund, *President and Chief Technologist, Citizens for Better Elections*

Michael A. Specter, *Assistant Professor, Computer Science, Cybersecurity & Privacy, Georgia Institute of Technology*

Drew Springall, *Assistant Professor of Computer Science and Software Engineering, Auburn University*

Philip B. Stark, *Distinguished Professor of Statistics, University of California, Berkeley*

G. Gary Tan, *Professor of Computer Science, Pennsylvania State University*

Alec Yasinsac, *Professor of Computer Science (ret.), University of South Alabama; Lt. Col. (ret.), USMC*