Order directing that might exceed the authority of this Court in this matter.

THE COURT: Well, I don't know if it exceeds my authority, but I would say this: I don't have a problem with requiring the Judge of Election to consult with the clerk before declaring the machine inoperable. So that the boss is called and the boss can weight in, if necessary.

MR. SANTEE: That would be agreeable, Your Honor.

JUDGE DALLY: And that it's recorded.

THE COURT: Right. Right. Does that make sense?

THE WITNESS: That makes sense, yes.

THE COURT: Okay. All right.

MR. SANTEE: If she may then be excused, and she will take that directive back.

THE COURT: Okay. Good enough. Thank you, Amy.

THE COURT: Mr. Santee, you want to make a record? You may.

MR. SANTEE: Yes, briefly.

MR. NITCHKEY: Or do you want me to do the Order first?

MR. SANTEE: I was going to text it to

her.

PRESIDENT JUDGE KOURY: Was he typing it as you spoke? I know the court reporter was.

(Off the record discussion.)

PRESIDENT JUDGE KOURY: I'll note for the record -- I want to note for the record that Mr. McClure was laughing as I was asking for additional language in the Order. So it is on the record.

MR. SANTEE: Your Honor --

THE COURT: Yes?

MR. SANTEE: -- I object to the notation on the record. I understand Judge Koury's representation. I object. Look, we were off the record discussing this --

THE COURT: I understand Judge Koury expressed some frustration, but that's not for me. There's nothing I can -- I'm not going to react to Judge Koury's frustration. I'm not going to change anything that happened today.

MR. SANTEE: Your Honor, if I may. Are we back on the record at this point?

THE COURT: Well, I think you were going to make a presentation.

MR. SANTEE: I am, yes. Your Honor, I object to anything that was said or done that was supposed to be off the record.

THE COURT: I don't know if it was on the record. You'll have to ask the court reporter because I wasn't watching if she was taking it down.

MR. SANTEE: I'll object, generally, if there is an issue.

THE COURT: Stacey, is that on the record, what happened?

THE COURT REPORTER: Yes. When Judge Koury asked to put it on the record, I put it on the record.

THE COURT: Okay. Do you want to --

MR. SANTEE: Sure. I object to that being in the record.

THE COURT: And you want me to strike his statement?

MR. SANTEE: I do, Your Honor. I move to strike that statement.

THE COURT: I'll strike his statement.

MR. SANTEE: Your Honor, if I may inquire of Mr. Dertinger.

THE COURT: You may.

CHARLES DERTINGER,

having been duly sworn according to law,

was examined and testified as follows:

DIRECT EXAMINATION

BY MR. SANTEE:

Q Sir, state your full name.

A Charles Dertinger.

Q What is your current job title?

A I'm the Director of Administration.

Q What does your job title entail in terms of --

A I oversee the conduct of elections.

Q Were you present today during the testimony offered by the movants in this case?

A I have been.

Q You heard some of the issues with regard to issues with the voting machines; correct?

A I have.

Q And specifically, in terms of the efforts made to correct those issues, were there some -- what efforts has the County made?

A Once we were made aware that these problems existed, we reached out to -- very specifically, I reached out to the ES&S and directed them to -- with all haste -- to bring people and resources here to deal with these problems. As this was a new voting system, and we had every expectation that it should work as was planned.

All proper L&A testing -- that is to say the logics and analytics testing -- had been done in accordance with the State Department Guidelines. Meaning that each one of the buttons were tested in the environments where they were set up, to ensure that each one of them worked. They were then brought to the polling places and some points of calibration, which is what this has been -- a calibration issue -- has gone out of calibration in the far right corner of the ballot. As what we have seen calls in for.

They had originally had a technician here with a technical analyst to be here to assist us in the rollout. Since then, they have sent -- at our request, sent additional resources here to deal with that.

The very first thing they did was evaluate the problem that we were having. And in some cases, it was a matter of some people pressing too high on the button. Some people pressing too hard. And unfortunately, when something doesn't work, we tend to push harder. So that was causing the problem to be exacerbated.

They have gone out. And at the polling places that we are familiar with that were a problem, they have been dispatched to deal with those. And in many of those locations have remedied the problem.

The issue earlier in the day, when we first found out about it, was being addressed by the technical assistant that we had in the Voter Registration Office. And had been calling those folks to give them advice on how to fix it over the phone. And continued to do so until one such event caused a machine to stop working.

In most of our polling places, we do have multiple machines. And as was expressed earlier, when they do not work, you are supposed to -- as a voter, you are responsible to review the voter verifiable ballot. The reason for this system is to give you an opportunity to look at what you have selected.

The electronic version of this is not the voting component. The voting component of this is only the record, or the printed ballot. When it goes through the scanner, it is not a vote until such time as you say, cast your ballot.

All you're using the iPad, as you were, is to print a ballot. Once you print that ballot, if it's not correct, you have the opportunity and the right to reject that ballot and not cast that ballot. That is the reason these machines were purchased. And one of the reasons for which they were certified by the Department of State.

THE COURT: I wasn't aware -- I voted this morning. I wasn't aware that I was supposed to review the paper ballot.

THE WITNESS: We have --

THE COURT: I wasn't told. No one told me to review the paper ballot. I voted. I pressed the thing. It -- a paper ballot came down. And then I had to press another thing and it got eaten up. But I didn't check the paper ballot against my vote. I assumed it was going to record it correctly. I didn't -- no one told me that that was my obligation to double check the machine.

THE WITNESS: It is the way the -- this new standard has been adopted by the State Department.

THE COURT: Well, how are the voters supposed to know that they're supposed to double check their work when they vote? When I pressed the button, the buttons lit up. I expected my vote to be recorded that way. I had no idea I was supposed to look behind this little glass screen -- because something came down. And I said, do I take that or do you keep that because the Judge was behind me. And she said, no, don't press that button, and it goes into the machine.

THE WITNESS: The instructions on the machine tell you to verify your ballot and then cast your ballot.

THE COURT: Okay. It doesn't say verify your ballot by reading the little piece of paper showing through the screen on the bottom right of the box. That's not what -- I thought when you verified your vote, it was before you press vote. You look and make sure the lights are lit up right, which is what I did. And I pressed that button.

THE WITNESS: The machine goes blank when it tells you to verify your ballot. So the only thing you can look at is the printout. And then it says, cast your ballot.

THE COURT: That's quite a design there. Voters should be told this; when they press vote that it's not really done yet and your vote doesn't count. You have to double check your vote before you -- it counts.

You've got to be kidding me. That's the most ridiculous system I've ever heard of. So you're going to tell me that I was wrong. I voted. I'm fairly educated and my vote might not be right because I failed to double check a piece of paper in the lower right-hand corner of the machine? Come on. Come on. Before you make a record, think.

THE WITNESS: Your Honor, that's why it's called a voter verifiable paper ballot. The State Department, as well as the education and outreach that we've done throughout the county in some 18 locations that we've brought the machine to, as well as kept it here and put signs up everywhere throughout the building that identify it as a voter verifiable ballot, indicate that it's to be verified by the voter.

THE COURT: All right. So I was wrong for not walking through your building and looking for a poster somewhere to read about whether my ballot was properly verified. You've got to be kidding me. All right. I understand what you're saying. I don't even know why you're making that record because that's not even for today.

THE WITNESS: The record was that --

THE COURT: That's for another day. In case they try to invalidate your election. That's what your testimony is for today. So it doesn't really help me today.

MR. NITCHKEY: Can I ask one question on cross, Judge?

THE COURT: No. No. It's not necessary. We don't need to fight about this. The issue is: There's some problems right now and some concern. We've tried to address it as best we can. We'll see what happens. And whether or not the election is questionable is for another day and another record. I'm not going to do that today.

MR. SANTEE: That's fine, Your Honor.

THE COURT: All right. Is there anything else?

MR. NITCHKEY: Well, I really wanted to ask --

THE COURT: I'm not going to do it anyway, probably. It's going to have to be a judge from another county.

MR. NITCHKEY: I just wanted to ask a question.

THE COURT: Knowing how my Court Administrator is, I think he's going to ask for a full-bench recusal.

MR. NITCHKEY: Since we're making a record, Judge, I just wanted to ask one question.

THE COURT: What?

CROSS-EXAMINATION

BY MR. NITCHKEY:

Q Mr. Dertinger -- and please, I don't mean to be a bad guy here, but I want to make sure I understood one thing that you said correctly.

These are new machines; correct?

A They are.

Q And you said they were tested at the facility were they were made, where they were calibrated?

A No. They were tested at our warehouse where they were set up for this election. L&A testing is the logics and analytics testing, so that we go through the trouble of making sure that every button operates at the time we set up the election. So that nothing -- cross votes or --

Q So they were tested in your warehouse?

A They were.

Q Okay. These are electronic machines; correct?

A They are.

Q Okay. And they're calibrated?

A They are.

Q And they were there after -- after they were tested, transported to the polls?

A Yes.

Q Were they tested at the polls?

A They were not tested at the polls.

Q So it's possible that the calibration in the transport could have been thrown completely off?

THE COURT: Listen, anything is possible. Why are we making this record now? This is for another day. This is for another day and another time.

The only thing I can do right now is try to help the voters who haven't voted yet, and that's what I'm trying to do. Mr. Dertinger, whether he wants to criticize the voters as not understanding what their obligation was as a voter or what they did to try to make these machines work properly is for another day. I don't decide any of that right now.

MR. NITCHKEY: Okay.

THE COURT: Okay.

MR. NITCHKEY: We're done.

JUDGE DALLY: Wait. My issue, I think, is important for today. The call log for complaints.

THE COURT: I think we heard -- I think we told --

MR. DALLY: Well, I think this witness was called to testify to that issue; weren't you?

THE COURT: I don't know. I have no idea.

THE WITNESS: There is a -- to be in the elections office, to see what goes on in the elections office -- people called because they don't know where they're voting, they don't know what their polling place is, they've run out of paper, they've run out of stickers, they are -- people are coming in because they think they have an absentee ballot.

The calls that come in there are done constantly on a rollover basis, and the problems that we had with the equipment were relayed directly to ES&S. I will verify with them, but I believe they have a record of all the calls.

THE COURT: Let me try to answer Judge Dally's question. They've never kept a call log before. It's never been necessary and she hasn't done it up until now. But when she was here, she indicated that she would keep a call log going forward for any other complaints. But I think her testimony was: Different people in the office fielded calls, and no one was required to keep a call log.

MR. NITCHKEY: Right. And I think that's an important issue, if you're trying to determine whether the election was properly carried forth.

THE COURT: Well, the only issue is that they don't have a log for -- you're not going to be able to verify what the problem was using a call log from before 5:00 p.m. today because it doesn't exist.

So you're going to have to have individual people come in, whether they're voters or Judges of Election, if you believe there's a problem.

JUDGE DALLY: Right. And that's why I made the request.

THE COURT: I understand. And I think Amy indicated that she would keep record of the calls with regard to the machines. But I think Mr. Dertinger is correct that, historically, we've never had to do that before and that wasn't a policy. And they didn't do that today until just now when we discussed it.

So I mean, it is what it is.

MR. NITCHKEY: Thank you, Your Honor.

THE COURT: Good luck.

MR. NITCHKEY: Thank you, Your Honor.

(The proceedings concluded.)

CERTIFICATION

I.

I hereby certify that the proceedings are contained fully and accurately in the notes taken by me in the above cause, and that this is a correct transcript of the same.

Date: ___________________________, 2019

____

Stacey Jacovinich
Official Court Reporter

II.

The foregoing record of the proceedings in the within matter is directed to be filed.

Date: ___________________________, 2019

____

Stephen G. Baratta, Judge

EXHIBIT 13

PA Post®

Focused on Pennsylvania's public policies, politics and statewide issues

Adam Carbullido, Election Security & Systems Senior Vice-President of Product Development, on Dec. 12 describes why the company's ExpressVote XL gave voters problems at the polls and later incorrectly tallied totals in multiple races in

POLITICS & POLICY

DECEMBER 12, 2019 | 4:48 PM
UPDATED: DECEMBER 12, 2019 | 9:58 PM

Human error and sensitive touchscreens blamed for Northampton Co. election problems

Emily Previti ⊕

EASTON – Incorrect election night vote counts in Northampton County were the result of human error and overly sensitive touchscreen technology, according to representatives from the manufacturer of the county's new voting machines.

The ExpressVote XL voting machines **erroneously tallied votes < https://papost.org/2019/11/06/machine-errors-delay-election-reporting-in-pa-s-northampton-county/>** in cross-filed races — those in which one candidate is running as the nominee for more than one political party. Voters also complained that the machines' touchscreens were overly sensitive and weren't registering their choices correctly.

Officials for the XL's manufacturer, Election Systems & Software, addressed the media and, later, County Council, on Thursday to reveal findings from their investigation into what went wrong on Nov. 5 with the system that the county paid $2.8 million to acquire.

They reported that the touchscreen problem happened because selection boxes for different candidates were too close together. To fix that issue, the boxes have been removed in the latest version of ES&S software, which is scheduled to start Pa.'s certification process in January, according to Adam Carbullido, the company's senior vice-president of product development.

Carbullido said tabulation errors occurred only in cross-filed races on ballots where voters chose the straight-party option, which automatically selects the same party for each race.

In the future, that won't be an issue because Pennsylvania will no longer offer the straight-party option starting with the

2020 primary.

Regardless, Carbullido said, the error should have been caught at two different points: During configuration before the machines were delivered, and during pre-election logic and accuracy testing in Northampton, which company and county officials jointly conducted.

“Had we provided the proper guidance and scrutiny, … it would have been caught,” Carbullido said, referring to ES&S staff who assisted the county. “We told (county election workers) to review the tapes, but not how to review the tapes and to what level of detail they needed to be reviewed.”

The Pennsylvania Department of State will oversee future pre-election testing in Northampton County and start the process earlier.

But the problem originated because of mistakes made by ES&S workers during machine configuration prior to shipping from the company’s warehouse in Omaha. Carbullido said the company will also heighten quality control procedures by double-checking configurations before voting machines are shipped out.

Some Northampton County Council members expressed concern about avoidable gaps in the quality control process of an industry leader like ES&S <

https://www.propublica.org/article/the-market-for-voting-machines-is-broken-this-company-has-thrived-in-it> .

"The largest manufacturer of voting machines in the country had people in their plant that made human errors," said Councilman Robert Werner. "These programs were marketed to us as if they were infallible. I know the votes were counted. But … we don't have any hard solid proof they're going to work."

Emily Previti / PA Post

Northampton County Councilwoman Tara Zrinski, left, watches a presentation from Election Systems & Software representatives including Product Manager Tobey Dingbaum Thursday. (Emily Previti / PA Post)

County Executive Lamont McClure said the problems experienced in the most recent election < **https://www.lehighvalleylive.com/elections/2019/11/no-changes-in-winners-following-northampton-county-vote-canvass.html>** ultimately illustrate that the machines and auditing process function as intended.

"That should give voters confidence that in November of 2020, we will know definitively who wins Northampton

County," McClure said. "That's not to say I wasn't deeply, deeply disappointed and at some points angry with the XL's [performance]."

Carbullido said 30 percent of Northampton's machines were improperly configured. He said the company hasn't heard about similar problems elsewhere with the XL; however, Protect Our Vote Philly co-founder Rich Garella said the same touchscreen issues occurred in Philadelphia last month.

Northampton County won't incur any costs as a result of the investigation. ES&S also will provide funds to augment voter education about how to use the machines, company officials said Thursday.

ES&S still has to present its findings to the county Election Board on Dec. 19.

In the meantime, local political leaders say they'd prefer an independent audit.

The leaders of the county's main political parties — Republican Lee Snover and Democrat Matt Munsey — recently asked Council to bring in University of South Carolina professor Duncan Buell to look at the machines. Council shot them down, citing Buell's links to Jill Stein < **https://www.wfmz.com/news/area/lehighvalley/northampton-county-voting-machine-vendor-to-report-on-problems/article_8b26025a-17da-11ea-b0a3-b3bd924b927e.html>** , the former Green Party presidential candidate whose litigation led to < https://papost.org/2019/12/10/how-pa-s-election-security-lawsuit-settlement-led-to-the-last-minute-challenge-of-the-states-top-selling-touchscreen-voting-machine/> the statewide mandate to upgrade all election systems in time for next year's primary.

"They made the machines, they sell the machines," Munsey said Thursday. "Of course, they're going to give it a clean bill of health. … Even if 10 percent of voters don't trust it, I think that's a problem. And having an independent investigation check on that would help people feel confidence that it's not just a company saying everything's fixed."

LINKS

- **Seven solutions for Pennsylvania's problems at the polls < https://papost.org/2019/11/07/seven-solutions-for-pennsylvanias-problems-at-the-polls/>**

TAGS

election security election systems & software expressvote xl

northampton county voting machines

CATEGORIES

POLITICS & POLICY

EXHIBIT 14

PA
SIGN-UP FOR POLITICSPA PLAYBOOK

Top Stories | Governor | Senate | Congress | Harrisburg | Features

HD190: Special Election Set for February 25

Written by John Cole, Managing Editor

On Monday afternoon, Speaker Mike Turzai announced February 25, 2020 as the special election date to fill the open state House seat vacated by Movita Johnson-Harrell (D-Philadelphia).

Johnson-Harrell resigned from office on Dec. 13 after Attorney General Josh Shapiro announced that she was charged with theft, perjury, tampering with public records along with other crimes in connection to her nonprofit. She represented the 190th District since March 2019 after she won a special election to fill the seat held by state Rep. Vanessa Lowery-Brown (D-Philadelphia), who resigned "under protest" in December 2018 after she was sentenced on a bribery conviction.

Although Turzai selected the special election for February, Philadelphia City Commissioners Chairwoman, Lisa Deeley, sent a letter to Turzai last week urging him to schedule the special election the same day as the Pennsylvania primary.

According to the Philadelphia Tribune, Jabari Jones, president of the West Philadelphia Corridor Collaborative; Ark of Refuge pastor Pam Williams; Amen Brown; and Ray Bailey confirmed their interest in the seat, while Philadelphia Democratic Party Chair Bob Brady said that he knew of "at least two more potential candidates" weighing a run as well.

Poll

Reader Poll: Should PA Pass a 'Fair Pay To Play Act' for College

The parties will pick the candidates to run in the special election.

Athletes?

Yes (53%)

No (42%)

Undecided (4%)

December 17th, 2019 | Posted in Front Page Stories, Harrisburg, Top Stories | 1 Comment

One thought on "HD190: Special Election Set for February 25"

Sean says: **December 19, 2019 at 11:43 am**

This is wild. What a waste of money for Turzai to schedule this not on the actual primary date.

Reply

Archive

- December 2019
- November 2019
- October 2019
- September 2019
- August 2019
- July 2019
- June 2019
- May 2019
- April 2019
- March 2019
- February 2019
- January 2019

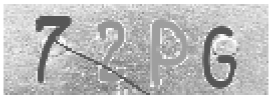
Got Something To Say:

Your email address will not be published. Required fields are marked *

Message:

Name *

Email *



CAPTCHA Code *

Post Comment

RSS Feed

ARCHIVE ABOUT US CONTACT ADVERTISE

EXHIBIT 15

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

JILL STEIN, RANDALL REITZ, ROBIN HOWE, SHANNON KNIGHT, and EMILY COOK,

Plaintiffs,

-against-

No. 16-CV-6287 (PD)

KATHY BOOCKVAR, in her official capacity as Acting Secretary of the Commonwealth; and JONATHAN MARKS, in his official capacity as Commissioner of the Bureau of Commissions, Elections, and Legislation,

Defendants.

DECLARATION OF J. ALEX HALDERMAN IN SUPPORT OF PLAINTIFFS' MOTION TO ENFORCE THE SETTLEMENT AGREEMENT

J. ALEX HALDERMAN declares under penalty of perjury pursuant to 28 U.S.C. § 1746, that the following is true and correct:

1. My name is J. Alex Halderman. I am a professor of computer science and engineering at the University of Michigan. My credentials, qualifications, and areas of expertise are described more fully in my declaration previously filed in this action at Dkt. #8 and Exhibit A thereto.

2. I am familiar with the operation of the voting system manufactured by Election Systems & Software called the ExpressVote XL. I have reviewed publicly available materials describing the system's technical specifications, the Secretary of the Commonwealth's reports certifying it for use in Pennsylvania, and reports certifying it for use in other jurisdictions.

3. From the perspective of election security, there are two central advantages of a voting system that uses paper ballots: (1) it does not place a hackable computer between the voter and the official record of her vote; and (2) the voter's selections are recorded on a physical record that cannot later be changed by hackers. The ExpressVote XL does not share these central advantages of paper balloting systems.

4. Although it records each voter's selections on a piece of paper, the ExpressVote XL works differently than most paper ballot systems. Despite its use of paper, its overall functioning bears more resemblance to a direct-recording electronic voting machine that produces a voter-verifiable paper audit trail (a "DRE with VVPAT" system). DRE with VVPAT systems provide inferior security to systems that use paper ballots.

5. As in a DRE with VVPAT system, the ExpressVote XL prompts the voter to make selections on a computer. It then prints a summary of the voter's selections on a piece of paper that is held behind a transparent window. A prompt on the computer screen asks the voter whether to cast her vote. If the voter accepts the prompt, the paper is fed back through the machine and into a collection container.

6. The paper on which the ExpressVote XL prints the voter's selections passes back through the printer on its way to being deposited in the collection bin. The system's software is designed to lift the printhead to prevent it from making any additional marks on the paper when the paper passes back through the machine. It would be feasible for malware to tamper with this function and cause the printhead to add additional races or selections to the paper after the voter has reviewed it. In this way, an attacker could change the voter's selections after the paper was out of the voter's sight.

7. The ExpressVote XL scans the voter's paper record before, not after, she reviews it. The system's software is designed not to cast the votes until after the voter has accepted the printout. It would be feasible for malware to compromise this function and cause paper records that have been rejected by voters to be tabulated as well as those that have been accepted by voters. Such an attacker would cause the set of voted paper records to differ from voters' intended votes.

8. The paper records printed by the ExpressVote XL contain the names of selected candidates and a set of bar codes that supposedly correspond to those selections. What is scanned and counted by the machine is not the human-readable names but only the non-human-readable bar codes. Voters have no practical way to verify that the bar codes correctly reflect their selections. It would be feasible for malware to cause the machine to print bar codes that corresponded to candidates the voter did not select. The result would be that the tabulated votes did not reflect the voter's choices, but the voter would not be able to detect this.

9. Other ballot marking devices (BMDs) are not designed the same way. Many, if not most, BMDs produce ordinary paper ballots that are handled by the voter and fed into an optical scanner just like paper ballots that are filled out by hand.

10. With a paper ballot system, a robust post-election audit can correct any computer-based error or fraud. This is not possible with the ExpressVote XL, because it would be feasible for malware to cause the paper records to differ from voters' actual votes. If hacking compromises the paper records, a post-election audit will arrive at the same wrong result.

Dated: November 21, 2019

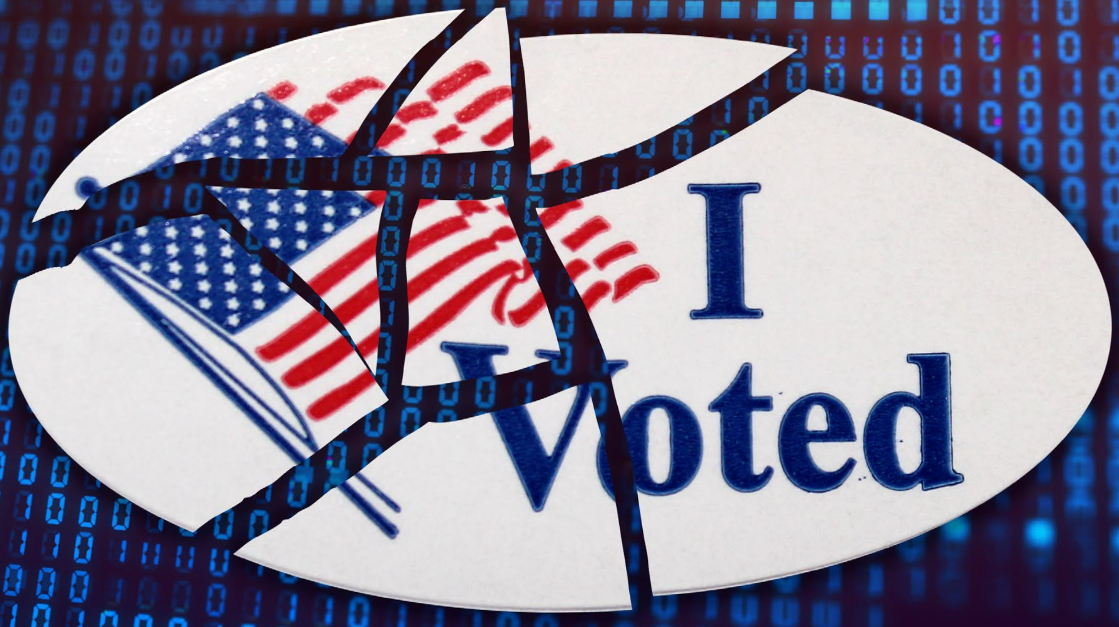
J. ALEX HALDERMAN

EXHIBIT 16

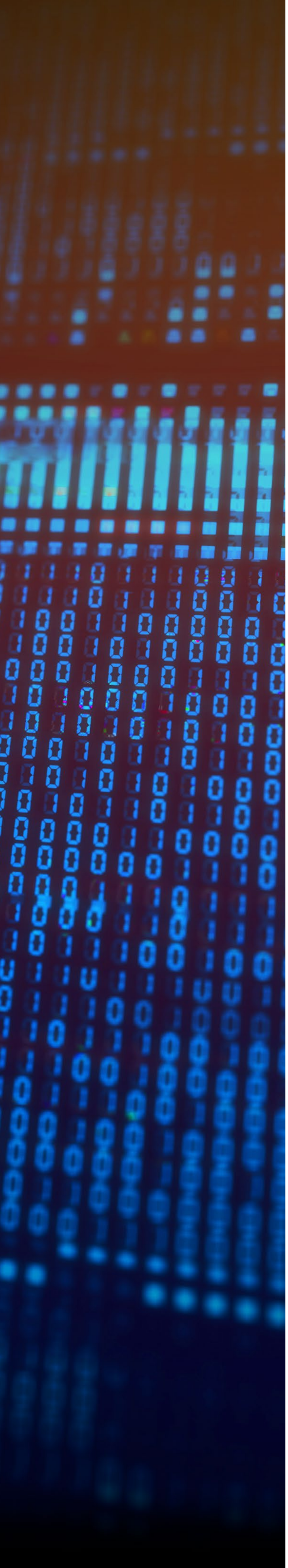
University of Pittsburgh

THE BLUE RIBBON COMMISSION ON PENNSYLVANIA'S ELECTION SECURITY

STUDY AND RECOMMENDATIONS



PITT
CYBER
University of Pittsburgh
Institute for Cyber Law,
Policy, and Security



Contents

Introduction from the Co-Chairs

This report, and the work of the commission in preparing it, offers a thorough review of the cybersecurity of Pennsylvania's election architecture and the challenges we must take on to improve it.

From the colonial era through today, America has prided itself on its democratic ideals. Popular sovereignty—the essential right to choose one's own leaders through the ballot box—is central to this identity. The nation has greatly expanded the franchise over the years through a series of historical movements—often difficult and even violent. Pennsylvania has played an outsize role in that steady march of history, from Quaker meeting houses; to the Continental Congresses and the Constitutional Convention; to the Women's Suffrage, Labor, and Civil Rights movements.

In recent years, however, debates over the nation's elections have been less about the expansion of the franchise than about our capacity to conduct the vote fairly, efficiently, and securely. This should trouble all Americans. The health and success of our democracy depend in large measure on broad public trust in the execution of our representative form of government. Indeed, it is far easier to lose faith in the results of elections than it is to earn it.

Interference by foreign actors threatens this faith. There is a growing understanding that foreign propaganda and disinformation via social media by nation-state actors have introduced another type of threat to the credibility of our elections and, indeed, to our national discourse. No one should doubt these well-documented attempts at interference.

Although there have been dramatic improvements in American election security since 2016, more must be done—at the local, state, and federal levels.

We have little doubt that foreign adversaries will increase their efforts in the lead-up to the presidential election in 2020. The persistence and sophistication of these actors are only increasing.

Pennsylvanians in particular should be concerned about election security. Our state is one of the most vulnerable to election manipulation, in large part because of reliance on older electronic voting systems. As recently as the 2018 election, an estimated 83 percent of Pennsylvanians were voting on machines that offer no auditable paper record. This could thwart Pennsylvania's counties from detecting a successful hack, or even benign error, and it prevents counties from recovering in the instance of an attack.

Of course, it is not just the voting machines and closely linked election management systems that are at risk. There are multiple threat vectors throughout our election architecture, including in our voter registration system, tallying methods, and election-night reporting. The architecture is complex and was not built to withstand threats from nation-states and other sophisticated attackers.

Private election vendors play an outsize role in many Pennsylvania counties' election efforts. For many, unfortunately, we fear that security is far from a top priority.

And, as we are learning every day, even successful defense against attacks on the *outcome* of the vote may not be enough to protect Americans' faith in our elections. Any number of attacks could create chaos or confusion among poll workers and voters, leading to a damaging loss of faith in election results, even where those results are not maliciously altered. A nation-state rival does not need to alter actual votes if Americans do not trust the vote tally.

The litany of threats is long—and exacerbated by a lack of funding and training for election officials, who are suddenly expected to be front-line cyber warriors defending our democracy against sophisticated nation-state actors.

However, we are heartened by an overwhelming consensus of experts about the way forward. From the National Academies of Sciences, Engineering, and Medicine and the U.S. Senate Intelligence Committee to hundreds of cybersecurity experts, the key remedies are clear: Use voting systems with voter-marked paper ballots; improve cybersecurity of election management and voter registration systems; conduct robust post-election audits; and have good contingency planning in place. These recommendations, and more, are detailed in the pages that follow.

The Governor's and Department of State's efforts to require counties to have voting systems with voter-verifiable paper records by the end of 2019 should reassure all Pennsylvanians. We urge the General Assembly to work closely with counties to fund these critical replacements. We must support our local election officials and the critical efforts by the Department of State to improve the Commonwealth's entire election architecture.

We must not pretend that the existing election architecture from an era of flip phones is sufficient to withstand a determined foreign adversary. Improving it will require political will, including funding. And it will require that the Commonwealth and counties be prepared to administer an election even in the face of a cyberattack.

This is not a partisan issue. And there is no question that Pennsylvania can—and must—secure its elections for our citizens.

This report, and the work of the commission in preparing it, offers a thorough review of the cybersecurity of Pennsylvania's election architecture and the challenges we must take on to improve it. We must be better prepared to manage the kinds of cyber threats that have targeted us in the past—and anticipate the threats of the future.

We are confident that this report offers evidence-based, actionable recommendations to secure Pennsylvania's elections. We hope that it might also serve as a model for other states in their own important efforts.

We, as Americans, must address our election security with the urgency the threat deserves.

David J. Hickton
Founding Director,
University of Pittsburgh Institute
for Cyber Law, Policy, and Security

Paul J. McNulty
President,
Grove City College

Acknowledgments

With support from:

The Heinz Endowments
Howard Heinz Endowment
Vira I. Heinz Endowment

The Pittsburgh Foundation

Pitt Cyber
University of Pittsburgh
Institute for Cyber Law,
Policy, and Security

in partnership with:

Verifiedvoting

The University of Pittsburgh Institute for Cyber Law, Policy, and Security (Pitt Cyber) and The Blue Ribbon Commission on Pennsylvania's Election Security gratefully acknowledge the generous support of The Heinz Endowments and The Pittsburgh Foundation's Charles H. Spang Fund to host The Blue Ribbon Commission on Pennsylvania's Election Security.

The commission thanks Christopher Deluzio for his tremendous contribution to this report and throughout this entire effort; Beth Schwanke for her guidance and development of the commission; and the entire staff of Pitt Cyber, including Sarah Barca, Kate Ulreich, and Ray Winstead, for their contributions.

We are also grateful to the exceptional partnership and thoughtful expertise provided by Verified Voting throughout this effort.

Many thanks to Carnegie Mellon University's Software Engineering Institute for providing technical advice. Thanks to Jones Day for pro bono support, especially David Coogan, as well as the many individuals at the University of Pittsburgh and beyond without whom this project could have never occurred.

We are sincerely grateful for all of the cooperation from Kathy Boockvar, senior adviser to the governor on election modernization (and, as of January 4, 2019, slated for nomination as secretary of the commonwealth); Jonathan Marks, commissioner, Bureau of Commissions, Elections, and Legislation, Department of State; Tim Benyo, chair, Association of Eastern Pennsylvania County Election Personnel; Shari Brewer, chair, Western Pennsylvania Election Personnel Association; and Ed Allison, director of voter registration, Lawrence County.

We acknowledge all of the thoughtful contributions we received in public comments and the many organizations and people throughout Pennsylvania and the country who provided us with their expertise and insight. In particular, thanks to those who presented at the commission's meetings, including state and county election personnel; J. Alex Halderman, professor of computer science, University of Michigan; and Elizabeth Howard, counsel, Brennan Center for Justice.

Commission Members*

SENIOR ADVISORS

Charlie Dent: former U.S. congressman, 15th District of Pennsylvania

Paul H. O'Neill: 72nd Secretary of the U.S. Treasury

Dick Thornburgh: Former governor, Pennsylvania; former Attorney General of the United States; former Under-Secretary-General of the United Nations

David Hickton: founding director, Pitt Cyber; former U.S. Attorney for the Western District of Pennsylvania (co-chair)

Paul McNulty: president, Grove City College; former Deputy Attorney General of the United States; former U.S. Attorney for the Eastern District of Virginia (co-chair)

Jim Brown: former chief of staff to U.S. Senator Robert P. Casey Jr.; former chief of staff to Pennsylvania Governor Robert P. Casey

Esther L. Bush: president and CEO, Urban League of Greater Pittsburgh

Mary Ellen Callahan: former chief privacy officer, U.S. Department of Homeland Security

Susan Carty: president, League of Women Voters of Pennsylvania

Nelson A. Diaz: retired judge, Philadelphia Court of Common Pleas

Jane Earll: attorney; former Pennsylvania senator

Douglas E. Hill: executive director, County Commissioners Association of Pennsylvania

Mark A. Holman: partner, Ridge Policy Group; former deputy assistant to the president for Homeland Security; former chief of staff to Pennsylvania Governor Tom Ridge

Ken Lawrence: vice chair, Montgomery County Board of Commissioners

Mark A. Nordenberg: chair of the Institute of Politics, University of Pittsburgh; Chancellor Emeritus of the University; Distinguished Service Professor of Law

Grant Oliphant: president, The Heinz Endowments

Pedro A. Ramos: president and CEO, The Philadelphia Foundation

James C. Roddey: former chief executive, Allegheny County

Marian K. Schneider: president, Verified Voting; former Pennsylvania Deputy Department of State for Elections and Administration

Bobbie Stempfley: director, CERT Division, Software Engineering Institute, Carnegie Mellon University

David Thornburgh: president and CEO, Committee of Seventy

Sharon Werner: former chief of staff to U.S. Attorneys General Eric H. Holder Jr. and Loretta E. Lynch

Dennis Yablonsky: former CEO, Allegheny Conference on Community Development; former Pennsylvania Secretary of Community and Economic Development

* Affiliations are provided for identification purposes. Commissioners are serving in their personal capacities.

Executive Summary[**]

[**] Pennsylvania’s election architecture is in a period of significant change. The commission has strived to provide the most accurate and up-to-date information. For publication purposes, this report reflects information current as of January 4, 2019 (unless otherwise noted).

These threats strike at the heart of democracy in Pennsylvania and throughout the United States. Securing our elections is not a partisan issue—and Pennsylvanians of every political persuasion should embrace the solutions that the commission recommends.

ELECTION INFRASTRUCTURE THROUGHOUT THE COUNTRY IS UNDER THREAT—AND PENNSYLVANIA IS NO EXCEPTION.

In fact, Pennsylvania's elections are worryingly susceptible to hacking for two primary reasons. First, the Commonwealth is a regular battleground state, with tight presidential election results, close congressional elections, and myriad other hotly contested races, making it an appealing target for those wishing to wreak havoc on the United States and its democracy.

Second, the bulk of Pennsylvania's voting machines are vulnerable to hacking and manipulation, something that computer scientists have demonstrated for several years.[1] This vulnerability stems from many counties' use of insecure electronic voting systems that are susceptible to manipulation and offer no paper record—and therefore no way of verifying the tabulation of votes when the veracity of election results is questioned.

Given the clear and present danger that these paperless machines pose, replacing the systems with those that employ voter-marked paper ballots should be the most pressing priority for Pennsylvania officials to secure the Commonwealth's elections.

Yet because even the most secure voting machines are still at some risk for hacking, replacing the vulnerable paperless voting systems would be insufficient if not coupled with robust, post-election audits. Such audits, if conducted properly after every election, can ensure that officials are able to detect machine tabulation errors that might affect the outcomes of elections. Pennsylvania's Election Code does require some post-election tabulation auditing (a flat-rate audit); however, only counties that use paper ballots can meaningfully comply with the Election Code's requirements. Moreover, Pennsylvania officials should improve upon the Election Code by embracing risk-limiting audits, which would offer a more effective and efficient method of verifying election results.

Voter registration databases are also a target for cyberattack. According to federal officials, Russian operatives targeted several states' voter registration databases—including Pennsylvania's—in the lead-up to the 2016 presidential election. Pennsylvania's voter registration system, which is into its second decade of service, has several vulnerabilities that could expose the system to manipulation by hackers seeking to delete, alter, or create registration records.

Fortunately, Pennsylvania officials are poised to embark upon the procurement process to replace this system—a process that will present an opportunity to deploy best practices in selecting and managing election vendors. These private companies also service much of Pennsylvania's election architecture beyond the voter registration system and, if not managed properly, can introduce substantial vulnerabilities through lax cybersecurity practices and opaque supply chains.

Any cyber defense would be incomplete without strong and extensive contingency planning. Such measures—which run the gamut of having adequate backup paper supplies for electronic pollbooks, ensuring poll workers are trained to handle contingencies, and preparing for natural disasters and attacks on the electric grid—ensure that election systems can recover in the face of an attack or technological error. Thus, proper contingency planning can provide a measure of resilience, something that Pennsylvania could improve, particularly while many counties continue to use vulnerable paperless voting systems.

These threats strike at the heart of democracy in Pennsylvania and throughout the United States. Securing our elections is not a partisan issue—and Pennsylvanians of every political persuasion should embrace the solutions that the commission recommends.

It is impossible to eliminate completely the risk of cyberattack on Pennsylvania's election architecture. However, trust in the integrity of our elections hangs in the balance; Pennsylvania officials must work to both reduce the potential for attacks and mitigate the impact in the event of an attack or other technological event. Citizens' faith in democracy demands nothing less.

SUMMARY OF RECOMMENDATIONS

Recommendation 1: Replace Vulnerable Voting Machines with Systems Using Voter-Marked Paper Ballots.

Counties using direct recording electronic (DRE) systems should replace them with systems using voter-marked paper ballots (either by hand or by machine) before 2020 and preferably for the November 2019 election, as directed by the Pennsylvania Department of State.

The Department of State should decertify DRE voting systems following December 31, 2019, if not sooner.

The Department of State should not certify and counties should not procure DRE machines—not even with voter-verifiable paper audit trails—but instead systems that tabulate voter-marked paper ballots, which are retained for recounts and audits.

Recommendation 2: The Pennsylvania General Assembly and the Federal Government Should Help Counties Purchase Secure Voting Systems.

Pennsylvanians, including public officials, must recognize that election security infrastructure requires regular investments and upgrades. Our elections—and Pennsylvanians' faith in them—are not free.

The General Assembly should appropriate funding to help cover the cost of counties' purchase of voting systems that incorporate voter-marked paper ballots (marked either by hand or by ballot-marking device) and other needed improvements to Pennsylvania's election security.

The U.S. Congress should provide additional appropriations for states, like Pennsylvania, which need to replace significant numbers of DREs without voter-verifiable paper audit trails.

Pennsylvanians should support federal legislation that includes assistance for states to replace aging voting systems.

The Governor, General Assembly, and counties should explore creative financing mechanisms (such as a bond issuance) to assist counties with procuring more secure electronic voting systems with voter-marked paper records.

The General Assembly should also consider creating a fund for regular future appropriations as upgrades in security and accessibility technologies merit.

Review and, where not already in place, implement cybersecurity best practices across Pennsylvania's election architecture.

Recommendation 3: Implement Cybersecurity Best Practices throughout Pennsylvania's Election Architecture.

Ensure that vote-tallying systems: (1) are single-use systems; (2) are air-gapped; and (3) follow the one-way, one-use removable media rule. Have redundancies in reporting tallies.

Require counties to compare and reconcile precinct totals with countywide results to ensure that vote totals add up correctly.

The State and counties should be conscious of supply chain vulnerabilities. Any contractors or vendors should be assessed for security risks. Security considerations should be a key selection factor—not reviewed after a procurement decision has been reached.

Implement multifactor authentication before implementing changes to a registration record in SURE.

Add an additional layer of encryption to SURE system data.

Send paper notifications to registered voters after online changes to records.

Require mandatory pre-election testing of e-pollbooks across Pennsylvania (where e-pollbooks are used) to ensure e-pollbooks are in good and proper working order before Election Day.

Recommendation 4: Provide Cybersecurity Awareness Training for State and Local Election Officials.

The Commonwealth should continue to conduct cybersecurity training for state personnel. In addition, the Department of State should continue to work toward rolling out, in consultation with counties, cybersecurity training for local election officials throughout Pennsylvania.

Local officials should support Commonwealth efforts to roll out cybersecurity training and creatively look to leverage existing resources to ensure personnel are adequately prepared to face today's cybersecurity threats.

The Department of State should encourage local election officials to take advantage of federal cybersecurity training resources, such as the Department of Homeland Security's free, online, on-demand cybersecurity training system for governmental personnel and the inter-agency National Institute for Cybersecurity Careers and Studies.

Recommendation 5: Conduct Cybersecurity Assessments at the State and County Levels.

The Pennsylvania Department of State should continue to conduct, and all of Pennsylvania's counties should conduct, comprehensive cybersecurity assessments. Election officials should also conduct regular process audits across the election ecosystem.

Local officials should not only support but also work closely with Commonwealth officials in connection with cybersecurity assessments.

Election officials should avail themselves of the no-cost cybersecurity assessment resources offered by the U.S. Department of Homeland Security.

Pennsylvanians should support federal legislation that strengthens and supports federal cybersecurity resources and provides training and assessment assistance to state and local election officials.

The General Assembly should provide funding support to counties to implement regular, periodic cybersecurity assessments and audits, especially relating to election infrastructure.

Recommendation 6: Follow Vendor Selection Best Practices in SURE Replacement Procurement and Leverage Auditor General's Findings.

In connection with the upcoming procurement process to replace SURE, the Department of State should heed vendor selection best practices applicable to election infrastructure.

Beyond the SURE procurement process, the State and counties should be conscious of supply chain vulnerabilities.

The Department of State should work closely with the Auditor General's office in connection with that office's audit of Pennsylvania's voter registration system. Any relevant audit findings should be taken into account in the upcoming procurement process.

Recommendation 7: Employ Risk-Limiting Audits

Pennsylvania should employ transparent risk-limiting audits after each election.

The Department of State, in partnership with select counties, should pilot risk-limiting audits. The General Assembly should then pass legislation to make this a statewide requirement.

Recommendation 8: Implement Best Practices throughout Pennsylvania's Cyber Incident Response Planning.

Review and, where not already in place, incorporate cybersecurity best practices into Pennsylvania's cyber incident response plans.

All Pennsylvania counties should join the EI-ISAC (Elections Infrastructure-Information Sharing and Analysis Center).

The Pennsylvania Auditor General's audit and the Commonwealth's Inter-Agency Election Preparedness and Security Workgroup should examine cyber incident response plans.

The General Assembly should provide funding support to counties to bolster election-related contingency planning measures as part of a broader appropriation to support improvements to election security across the Commonwealth.

Recommendation 9: Revise the Election Code to Address Suspension or Extension of Elections Due to an Emergency.

The Election Code should provide clear authority for the suspension or extension of elections due to a wide-scale cyber-related attack, natural disaster, or other emergency that disrupts voting. The Election Code should include straightforward procedures governing the declaration of an emergency and the suspension or extension of voting.

Recommendation 10: Bolster Measures Designed to Address Voting Equipment–Related Issues So Voting Can Continue Even in the Event of Equipment Failure.

Ensure that emergency paper ballots sufficient for two to three hours of peak voting are available in every polling place using DRE machines.

Update poll worker training to address procedures for voting equipment failures.

Ensure that procedures are in place to ensure that voters with disabilities will be able to vote in the event of accessible voting equipment failures.

Recommendation 11: Enhance Measures Designed to Address E-pollbook–Related Issues So Voting Can Continue Even in the Event of Equipment Failure.

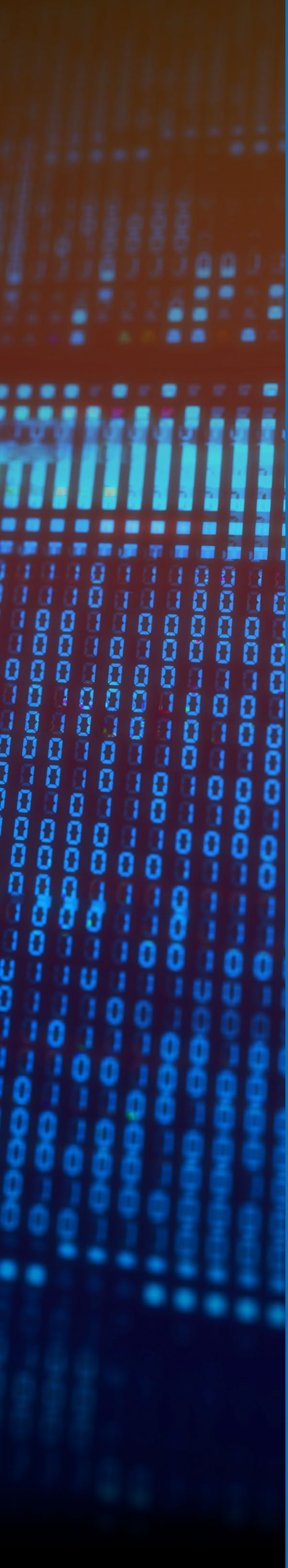
Ensure that provisional ballot materials sufficient for two to three hours of peak voting are available in every polling place using e-pollbooks.

Update poll worker training to address procedures for e-pollbook failures.

Counties using e-pollbooks should review and, where appropriate, implement cybersecurity best practices for e-pollbooks.

TABLE OF RECOMMENDATIONS BY RESPONSIBLE OFFICIAL

	State Officials	Local Officials	Federal Officials
Recommendation 1: Replace Vulnerable Voting Machines with Systems Using Voter-Marked Paper Ballots.	X	X	
Recommendation 2: The Pennsylvania General Assembly and the Federal Government Should Help Counties Purchase Secure Voting Systems.	X	X	X
Recommendation 3: Implement Cybersecurity Best Practices throughout Pennsylvania's Election Architecture.	X	X	
Recommendation 4: Provide Cybersecurity Awareness Training for State and Local Election Officials.	X	X	
Recommendation 5: Conduct Cybersecurity Assessments at the State and County Levels.	X	X	
Recommendation 6: Follow Vendor Selection Best Practices in SURE Replacement Procurement and Leverage Auditor General's Findings.	X	X	
Recommendation 7: Employ Risk-Limiting Audits.	X	X	
Recommendation 8: Implement Best Practices throughout Pennsylvania's Cyber Incident Response Planning.	X	X	X
Recommendation 9: Revise the Election Code to Address Suspension or Extension of Elections Due to an Emergency.	X		
Recommendation 10: Bolster Measures Designed to Address Voting Equipment–Related Issues So Voting Can Continue Even in the Event of Equipment Failure.	X	X	
Recommendation 11: Enhance Measures Designed to Address E-pollbook–Related Issues So Voting Can Continue Even in the Event of Equipment Failure.	X	X	



Voting and Election Management Systems

Overview

It is imperative that officials take steps to address these vulnerabilities before the 2020 election.

Both the insecurity of Pennsylvania's existing paperless voting systems and the lack of auditability make replacing these machines an urgently and immediately necessary step to secure Pennsylvania's elections. Officials can and should replace Pennsylvania's paperless voting machines (DREs), which do not have voter-marked paper ballots. The Department of State has taken important steps toward this end by requiring that counties have voter-verifiable paper-record voting systems selected by the end of 2019. Pennsylvania must ensure its new voting systems meet current best practices and can be put in use without an undue financial burden on counties.

Separate from—but inextricably linked to—voting machines, multiple back-end voting-related functions are also at risk of cyberattack on their specialized election management software.[2] This is true in Pennsylvania, as it is throughout the United States, with varying levels of vulnerabilities. As a U.S. Senate Intelligence Committee interim report noted, "… potentially vulnerable systems include some of the core components of U.S. election infrastructure, including systems affiliated with…vote casting, vote tallying, and unofficial election-night reporting to the general public and the media."[3] These functions (e.g., ballot building, tallying, and reporting) are diverse and vary within Pennsylvania at the county level, both in function and in level of risk.

Security experts agree that voter-marked paper ballots (either by hand or machine) are a necessary component of secure voting machines. Ensuring that voting systems provide a paper record that the voter reviews (a "software-independent record") "provides an important security redundancy that should act as a deterrent to cyber-attacks and should provide voters with more confidence that their votes have been counted accurately."[4] The presence of paper ballots does not *prevent* errors or attacks. Indeed, similar vulnerabilities exist in systems that include voter-marked paper ballots. However, a paper record allows jurisdictions to detect any problems with the tabulation software and recover from it.

A transition to voting machines with voter-marked paper ballots (by hand or device) and implementation of cybersecurity best practices to shore up the security of election management systems (and other elements of the election architecture) should reduce the likelihood of successful cyberattacks. When coupled with robust post-election audits (described elsewhere in this report), these efforts can mitigate the consequences of attacks by ensuring detection and making it possible to recover from any attacks or errors.

Although there is no publicly available evidence to support the conclusion that recent election results (in Pennsylvania or elsewhere) were compromised, the risk nonetheless remains, and it is imperative that officials take steps to address these vulnerabilities before the 2020 election.

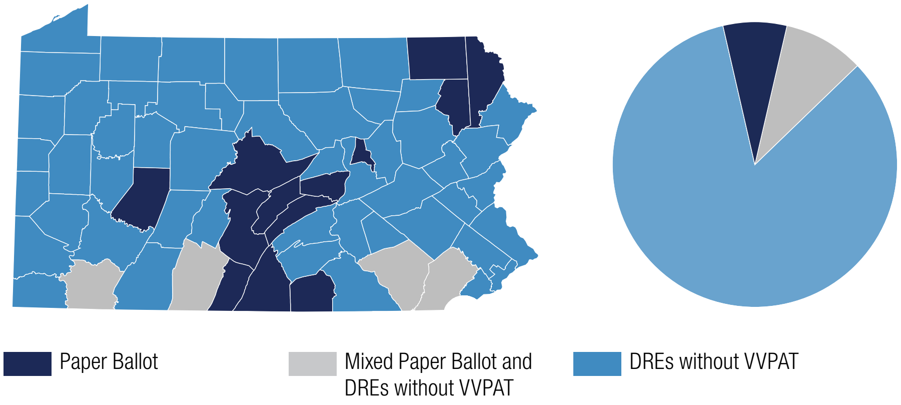
PENNSYLVANIA'S VOTING SYSTEMS AND THEIR VULNERABILITIES

During the 2016 presidential and the 2018 midterm elections, more than 80 percent of Commonwealth voters were registered to vote in precincts using voting systems known as "DREs without VVPAT" (direct-recording electronic systems *without* a voter-verifiable paper audit trail).[5] Unfortunately, however, computer scientists and cybersecurity experts, as well as most election administration officials, agree that these are the country's most insecure voting systems. There is a remarkable consensus of experts regarding the insecurity of these machines.[6] The DRE systems used in Pennsylvania and elsewhere have widely known exploitable vulnerabilities.[7]

As of November 2018, only thirteen of sixty-seven counties in Pennsylvania used optical scan systems as primary polling place equipment,[8] which security experts recommend as best practice in combination with meaningful audits. These counties were Adams, Centre, Franklin, Fulton, Huntingdon, Indiana, Juniata, Lackawanna, Mifflin, Montour, Snyder, Susquehanna, and Wayne counties.

POLLING PLACE EQUIPMENT IN PENNSYLVANIA

NOVEMBER 2018



Source: Verified Voting, The Verifier—Polling Place Equipment in Pennsylvania—November 2018
www.verifiedvoting.org/verifier/#year/2018/state/42

HOW ARE PENNSYLVANIA'S DRE VOTING SYSTEMS VULNERABLE?

There have been several high-profile examples of researchers hacking voting machines like those in use in Pennsylvania. In 2007, a Princeton University computer scientist, Andrew Appel, bought a used Sequoia AVC Advantage voting machine. Appel's then-graduate student, J. Alex Halderman, was quickly able to gain access to the machine's memory and software, altering them in such a way that made modification of vote counts easy and detection difficult.[9] More than a decade later, 574 precincts in Pennsylvania in Montgomery and Northampton counties still use that model.[10] In 2017, at DEF CON's Voting Village, attendees hacked the 25 pieces of election equipment available within three days, including voting machines in use in Pennsylvania (such as the ES&S iVotronic, the AVC Edge, and the AccuVote TSx), albeit under circumstances markedly different from those in polling places.[11] During the 2018 DEF CON Voting Village, attendees again exposed weaknesses in the latter two machines.[12]

The lack of voter-marked paper ballots (either by hand or machine) retained for recounts or audits in the majority of Pennsylvania's voting machines is perhaps most potentially damaging to the legitimacy—and faith therein—of Pennsylvania's vote. If the records are corrupted, whether intentionally by malicious attack or from benign malfunction, there might be no way to know.

The lack of a paper trail prevents Pennsylvania's counties from having the usual means for detecting any hacking or error, then recovering from such an event. In the event of a suspected attack, without a paper record, counties would be unable to verify that voting records on machines were accurate. And if a county cannot credibly prove that the outcome of its vote is accurate,[13] the assertion of a successful hack could be just as damaging as a successful hack. An attack would not have to change the outcome of a vote to impact the public's faith in the reported outcome of the vote.

Nor could officials conduct an effective recount. Meaningful recounts even in the absence of a suspected attack are nearly impossible without a contemporaneous paper record of votes. Thus, Pennsylvania would be unable to undertake robust, manual recounts, which voters have come to expect in races with razor-thin margins of victory.

Threat Scenario

A nation-state adversary could pursue an aggressive disinformation campaign across social media, falsely claiming to the public that vulnerable machines were hacked. The adversary could point to several potential vulnerabilities.

Because Pennsylvania's paperless DRE systems do not have a paper trail, officials would be unable to conduct the kind of post-election audit or recount that could assuage the public that results should be trusted. As a result, officials might lack the necessary means to rebut the disinformation campaign.

The U.S. Department of Homeland Security Secretary testified before the U.S. Senate Select Intelligence Committee that the inability to audit election results in states such as Pennsylvania poses a threat to national security.[14]

Testifying before Congress, University of Pennsylvania computer scientist Matt Blaze outlined the cybersecurity risks on existing DRE voting systems used in Pennsylvania and elsewhere:

> "DRE-based systems introduce several avenues for attack that are generally not present (or as security-critical) in other voting technologies. Successful exploitation of any one of these attack vectors can compromise elections in ways from which it may not be possible to recover:
>
> - Alteration or deletion of vote tallies stored in internal memory or removable media,
> - Alteration or deletion of ballot definition parameters displayed to voters,
> - Alteration or deletion of electronic log files used for post-election audits and detecting unauthorized tampering."

He went on to note that "[t]hese attacks might be carried out in any of several ways, each of which must be reliably defended against by the DRE hardware and software:

- Direct tampering with data files stored on memory cards or accessible through external interface ports,
- Unauthorized replacement of the certified software running on the machine with a maliciously altered version,
- Exploitation of a pre-existing vulnerability in the certified software."[15]