Protect Democracy

August 22, 2019

Via E-mail
Damon Circosta
Chair, North Carolina State Board of Elections
430 N. Salisbury St.
Raleigh, NC 27603

Re: Proposed Modifications to NCSBE's Election Systems Certification Program

Dear Chair Circosta:

We write to respectfully request that the North Carolina State Board of Elections ("NCSBE" or "the Board") approve Secretary Anderson's proposed modification to the Board's Elections Systems Certification Program[1] at its public meeting on Friday, August 23, 2019, and encourage counties to use ballot-marking devices only when their assistive technology is needed.

Decisions on whether to certify new election equipment are among the most important that the Board makes. A state's choice of voting technology has the power to shape who can vote, how accurately their votes will be counted, and whether voters will have confidence in the results of elections. In choosing how North Carolina voters will cast their ballots, likely for the next decade or more, the Board should carefully weigh the impact that its choice will have on voters' practical ability to cast a ballot and have that ballot counted. The Board should certify a voting system only if it is confident that the system assures voters' ability to cast an effective ballot.

Ballot-marking devices (BMDs), and barcode-based BMDs in particular, raise serious questions about voter access, election accuracy, and voter confidence. Whereas hand-marked paper ballots are well-understood in North Carolina, the newest generation of BMDs are uncharted territory. As we have learned more about older generations of election technology (including the iVotronic machines currently in use in some North Carolina counties), experts have identified risks that were unforeseen when the machines were first purchased. North Carolina doesn't need an unnecessarily complicated voting system and the risks that would come with that.

[1] *See Proposed Modification to State Board of Elections' Election Systems Certification Program*, North Carolina State Board of Elections (Aug. 20, 2019), https://s3.amazonaws.com/dl.ncsbe.gov/State_Board_Meeting_Docs/2019-08-23/Certification/ProposedModification_CertificationProgram.pdf. As you know, the proposed modification would require ballots produced by ballot-marking devices to be identical to hand-marked paper ballots, and would require all certified voting systems to include a hand-marked paper ballot option.

Hand-Marked Paper Ballots are the Right Choice for Most Voters

Two-thirds of North Carolina voters already cast ballots on what experts believe to be the gold standard for election technology: hand-marked paper ballots, scanned by an electronic tabulator, and verified by post-election hand-to-eye audits.

The advantages of a hand-marked paper ballot system are numerous. First, it is relatively easy to accommodate higher-than-expected turnout at a polling place by erecting more voting stations. In contrast, jurisdictions that use ballot-marking devices are unable to procure new machines on Election Day to handle a high turnout. This can lead to long lines, which are exacerbated when equipment malfunctions, and voters may be disenfranchised. Second, it's very secure — the voter directly verifies his or her selections by marking them on the ballot, and that ballot can be preserved throughout the vote-counting process. Third, a hand-marked ballot can easily be audited; this ensures that a malfunctioning tabulator does not compromise the election results. Finally, a system in which most voters cast hand-marked paper ballots is significantly less expensive for counties than an all-BMD system.

An election system based primarily on hand-marked paper ballots must also offer a voting method that is accessible to voters who are unable to complete a paper ballot by hand. BMDs that produce a human-readable ballot are a good solution for these voters. In the North Carolina counties that currently use hand-marked paper ballots, polling places are equipped with ES&S AutoMARK ballot-marking devices. These machines produce a ballot that is identical to the ballots used by voters completing ballots by hand, protecting ballot secrecy for voters who use these machines.

In light of the many benefits afforded by North Carolina's existing hand-marked paper-based voting system, the Board should decline to certify new systems that would introduce unnecessary complications to the voting process, either by requiring all voters to use a ballot-marking device or by introducing non-verifiable barcodes to the ballot.

The ES&S ExpressVote System is a Particularly Risky Choice for North Carolina

The ExpressVote system manufactured by Election Systems and Software (ES&S), which is the only barcode-based system currently under consideration by the Board, would be a particularly risky choice for North Carolina.

First, all barcode-based BMDs, including the ExpressVote, raise security and operational concerns.[2] Like all BMDs — indeed, all computers — barcode-based BMDs bear some risk of hacking or malfunction.[3] The central improvement BMDs offer compared to paperless voting

[2] Indeed, as we explained in our letter of July 26, 2019, the use of any BMD when not required for accessibility introduces unnecessary risk into the voting process. But that problem is particularly acute for barcode-based systems.

[3] Election equipment vendors often boast that their equipment is secure because it is "never connected to the Internet." But a direct Internet connection is not the only way that malware can enter a voting system. Voting machines must be programmed before each election to display the correct ballot for every voter. Usually, that is done by creating ballot-definition files on another

machines like the iVotronic is that BMDs generate a paper ballot that a voter can review. But because people cannot read barcodes, when the BMDs generate a barcode rather than human-readable text, the voter cannot actually verify whether their ballot has been cast as intended.[4]

Second, the ExpressVote runs an outdated version of Windows, which will soon be vulnerable to attack. Last month, the Associated Press reported that ES&S still uses Windows 7 for its voting systems because it still has not received federal accreditation for upgrading its systems to Windows 10.[5] Windows 7 was released in 2009 and reaches its end of life on January 14, 2020, meaning that Microsoft will generally stop providing technical support and fixing software vulnerabilities.[6]

These and other problems with the ExpressVote system have disrupted efforts by other jurisdictions to replace their old voting machines. Indeed, three organizations recently petitioned Pennsylvania's Department of State to re-examine its recent certification of ES&S's ExpressVote XL voting system on ten separate grounds.[7] The most alarming concern raised is that security researchers have now discovered that the ExpressVote XL could either malfunction or be manipulated so as to add, modify, or invalidate votes *after a voter has viewed, confirmed, and cast their ballot*.[8] As the Pennsylvania petitioners note, "[i]t is common sense that a voting machine should not have the ability to change votes after the voter has confirmed and cast her ballot."[9]

In Georgia, where the state recently adopted a different barcode-based BMD system produced by Dominion, the new system is already subject to legal challenge.[10] The plaintiffs allege that the use of Dominion's barcode-based BMD system violates voters' constitutional right to cast an effective ballot because (1) the barcodes themselves are not voter-verified, (2) the BMDs are vulnerable to intentional hacking and other manipulations, and (3) voters do not

computer, transferring it to a memory card, and then using that memory card to program the voting machine. Unless all of that equipment is rigorously isolated from any Internet-connected device, it will be possible for malware to enter the voting system.

[4] Jennifer Cohn, *What Is the Latest Threat to Democracy? Bar-Codes and Ballot Marking Devices A.K.A. "Electronic Pencils"*, Medium (Mar. 6, 2018), https://medium.com/@jennycohn1/what-is-the-latest-threat-to-democracy-ballot-marking-devices-a-k-a-electronic-pencils-16bb44917edd.

[5] Tami Abdollah, *AP Exclusive: New Election Systems Use Vulnerable Software*, Associated Press (July 13, 2019), https://www.apnews.com/e5e070c31f3c497fa9e6875f426ccde1.

[6] *Id.* While extended support may be available at additional cost to counties, it is not as comprehensive and provides only a temporary solution.

[7] Letter from Ronald A. Fein, Legal Director of Free Speech for the People, *et al.* to Kathy Boockvar, Acting Secretary of the Commonwealth (July 16, 2019), https://freespeechforpeople.org/wp-content/uploads/2019/07/petition_for_rexamination_of_expressvote_xl.pdf.

[8] *See id.* at PDF page 3 (Petition page 1) n.1 (collecting sources).

[9] *Id.* at 4.

[10] Third Amended Complaint, *Curling v. Raffensberger*, No. 1:17-CV-2989-AT (N.D. Ga. Aug. 16, 2019), ECF No. 581-1.

routinely check the accuracy of BMD-produced ballots before they are submitted.[11] The ES&S ExpressVote shares many of the characteristics identified by the Georgia plaintiffs as giving rise to constitutional violations.

Moreover, past history demonstrates that the Board should expect to learn of more security vulnerabilities in the ExpressVote system over the coming years. Within six years of North Carolina's adopting the iVotronic voting system, researchers hired by the Ohio Secretary of State identified major vulnerabilities in that system. Taken together, these vulnerabilities created a risk that malware, once introduced into a single voting machine, could "propagate virally" through the voting system, with the possibility of compromising an entire election.[12] Those findings were confirmed by subsequent research by Florida State University researchers.[13] Similar deficiencies have been found in other computerized voting systems,[14] and, over time, are likely to be found in the ExpressVote system as well.

Recent news reports have also called into questions key claims by ES&S about the security of its voting systems. ES&S has long claimed that its voting systems can never be connected to the Internet, and therefore are insulated from hacking attempts. But just this month, election security experts revealed that at least some of ES&S's backend systems have been connected to the Internet for years, without appropriate security precautions.[15] Similarly, the company asserted that it never equipped its machines with remote-access software that would allow the machines to be controlled via a network. But earlier this year, in a letter to Senator Ron Wyden, ES&S admitted that it *had* installed remote-access software on some of its equipment.[16] These revelations must cast substantial doubt on ES&S's assertions about the security of the ExpressVote, and underscore the need for truly voter-verified paper ballots.

If and when vulnerabilities are discovered in the ExpressVote in the future, the counties could be required — by litigation or legislation — to replace relatively new voting systems well before they reach end-of-life. This would be an unnecessary expense for cash-strapped counties,

[11] *Id.* at 21-28.

[12] Patrick McDaniel, *et al.*, EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing 49, 98 (Dec. 7, 2007), https://www.eac.gov/documents/2017/03/21/everest-report-state-voting-systems-voting-technology/.

[13] *See* Alex Yasinsac, *et al.*, *Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware* (Jan. 23, 2007), https://people.eecs.berkeley.edu/~daw/papers/sarasota07.pdf.

[14] *See* EVEREST, *supra* n.12, at 101-270; Ariel J. Feldman, *et al.*, *Security Analysis of the Diebold AccuVote-TS Voting Machine* (Sept. 13, 2006), https://jhalderm.com/pub/papers/ts-evt07.pdf.

[15] *See* Kim Zetter, *Exclusive: Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials*, Vice (Aug. 8, 2019), https://www.vice.com/en_us/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials.

[16] *See* Kim Zetter, *Top Voting Machine Vendor Admits It Installed Remote-Access Software on Systems Sold to States*, Vice (July 17, 2018), https://www.vice.com/en_us/article/mb4ezy/top-voting-machine-vendor-admits-it-installed-remote-access-software-on-systems-sold-to-states.

and one that the Board can avoid now by declining to certify unnecessarily risky barcode-based machines.

Conclusion

North Carolina knows how to run secure elections: with hand-marked paper ballots and appropriate accessibility accommodations. Secretary Anderson's proposed modification to the Elections Systems Certification Program is consistent with the Board's mandate to certify only equipment that is safe to use in North Carolina's elections. There is no reason for the state to take unnecessary risks with its elections by certifying technology whose security cannot be guaranteed.

Sincerely,

Jessica Marsden
Counsel, Protect Democracy