



Public Meeting—August 30, 2019

Beth Schwanke
Executive Director
University of Pittsburgh Institute for Cyber Law, Policy, and Security

Members of the Board of Elections, thank you for the opportunity to submit remarks at this Public Meeting about Allegheny County's selection of a new voting system.

I am honored to represent the University of Pittsburgh Institute for Cyber Law, Policy, and Security (Pitt Cyber), where I serve as executive director.

Pitt Cyber hosted The Blue Ribbon Commission on Pennsylvania's Election Security—an independent, bipartisan effort, supported by The Heinz Endowments and The Pittsburgh Foundation. During the course of that work, the commission and staff conducted extensive research, solicited comments from the public, received presentations from state and local officials and other experts in the field, attended demonstrations of new voting systems available in Pennsylvania, and issued interim recommendations on voting systems. The Commission issued a full report in January 2019.¹

As my colleague, Chris Deluzio, testified before the Board of Elections previously, the most secure and least expensive method of voting is hand-marked paper ballots counted by optical scan machines with ballot-marking devices (or BMDs) available for voters who are unable to hand mark paper ballots.

In fact, Pitt Cyber, in partnership with Citizens for Better Elections, recently released a study finding that of the 37 Pennsylvania counties in our analysis that have selected new voting systems, those that have selected exclusively BMDs are paying nearly twice as much as those that select a hand-marked paper ballot plus BMD configuration—or an average of \$24.60 per voter as opposed to \$12.37 per voter. This finding is consistent with an independent analysis that examined the expected costs of BMDs and hand-marked paper ballot systems over a ten-year period in Georgia, finding substantial savings for hand-marked paper ballot systems.²

I am here today to discuss the use of barcodes by some ballot-marking devices that the State has certified.

The Blue Ribbon Commission on Pennsylvania's Election Security recommends Pennsylvania counties do not procure voting systems that use barcodes or QR codes.³

¹ Study and Recommendations," The Blue Ribbon Commission on Pennsylvania's Election Security, https://www.cyber.pitt.edu/sites/default/files/FINAL%20FULL%20PittCyber_PAs_Election_Security_Report.pdf.

² "Georgia State Election Technology Acquisition: A Reality Check," OSET Institute, March 2019, https://trustthevote.org/wp-content/uploads/2019/03/06Mar19-OSETBriefing_GeorgiaSystemsCostAnalysis.pdf.

³ Study and Recommendations," The Blue Ribbon Commission on Pennsylvania's Election Security, https://www.cyber.pitt.edu/sites/default/files/FINAL%20FULL%20PittCyber_PAs_Election_Security_Report.pdf, pp. 49, 62.

Barcodes provide yet another attack vector for adversaries wishing to tamper with our election results.

As you know, ballot-marking devices are electronic touchscreen computers that voters can use to make their selections; the machine prints a paper record of those selections. Typically, jurisdictions then use optical scanners to tabulate paper ballots, whether they are hand-marked or marked by a BMD.

Depending on the vendor's system, the optical scanner "reads" those ballots⁴ marked by the BMD in two possible ways. Some systems scan the position of the bubble the ballot-marking device has filled in to identify the voter's selections, just like they would for a hand-marked paper ballot. Other systems scan a barcode printed on the paper ballot to identify the voter's selections.

Barcodes, however, are not human readable. A voter is therefore unable to verify if a ballot reflects her intent. In other words, because a voter cannot read a barcode; there is no way for a voter to know that the barcode printed and subsequently scanned reflects her voting choices. What the voter verifies⁵ is not what is being tabulated for the vote count.

A discussion document by the US National Institute of Standards and Technology (NIST) outlines one example of a potential attack related to barcodes,

[A] vote capture device may display the voter selecting one contest when they are actually selecting another (a.k.a. clickjacking). Additionally, malicious or faulty production of a barcode may cause a vote capture device to present the voter with different ballot selections than what will be interpreted by the voting machine. If barcodes are used for tabulation of cast ballots, any modification of a voter's ballot selections may go undetected and impact the election results. Another concern is how discrepancies can be detected and how to handle issues of mismatching information.⁶

Professors Andrew Appel, Richard DeMillo, and Philip Stark also outline a potential attack via barcode, wherein "[i]f an attacker were able to compromise a BMD, the barcodes are an attack vector for the attacker to take over an optical scanner."⁷

⁴ I use the term "ballots" for simplification. When a BMD generates barcode paper records for tabulation, those paper records are more precisely termed "cast vote records," not ballots, because they contain only the voter's selections in each race, rather than the entirety of the ballot with all candidates and ballot questions included. In essence, the cast vote record is a receipt showing a summary of the voter's selections, which are embedded in barcodes for tabulation accompanied by plain text.

⁵ Research suggests that "most voters do not review paper ballots printed by BMDs, even when clearly instructed to check for errors," and even those "voters who do review their ballots do not check carefully enough to notice errors that would change how their votes were counted." Andrew W. Appel, Richard A. Demillo, Philip B. Stark, "Ballot-Marking Devices (BMDs) Cannot Assure the Will of the Voters," pp. 1-2, April 21, 2019, <https://ssrn.com/abstract=3375755>.

⁶ NIST discussion paper, <https://collaborate.nist.gov/voting/pub/Voting/CyberSecurity/BarcodesEncodingPaper-June14-2019.pdf>, June 14, 2019.

⁷ Andrew W. Appel, Richard A. Demillo, Philip B. Stark, "Ballot-Marking Devices (BMDs) Cannot Assure the Will of the Voters," p. 17, April 21, 2019, <https://ssrn.com/abstract=3375755>.

Barcodes also make it difficult to perform a sound audit, because research shows that voters do not adequately verify their selections for BMD-generated ballots.⁸ This means that identifying a malicious attack that changed votes via audit would be significantly less likely.

For these reasons, many computer scientists and election security experts recommend that jurisdictions do not use ballot-marking devices with barcodes.⁹ In the seminal election security publication released last year by The National Academies of Sciences, Engineering and Medicine, the authors stated that barcode-based devices “raise security and verifiability concerns.”¹⁰

I understand that given Allegheny County’s ballot design with extensive candidate positions, there is a concern that only one vendor may be able to meet the County’s needs; and that vendor uses barcodes on paper ballots generated by its BMDs.

Given the voter verification and security concerns posed by the use of barcodes, this makes it all the more essential that the Board of Elections select a configuration that would rely primarily on hand-marked paper ballots and use ballot-marking devices only for those voters who need them; and use only the human-readable portion of the ballot for recounts and audits.

Thank you.

⁸ Risk-Limiting Audits “do not protect against problems that cause BMDs to print something other than what was shown to the voter on the screen,” Andrew W. Appel, Richard A. Demillo, Philip B. Stark, “Ballot-Marking Devices (BMDs) Cannot Assure the Will of the Voters,” p. 8, April 21, 2019, <https://ssrn.com/abstract=3375755>.

⁹ See, e.g., Hursti, Harri. [Presentation to the Presidential Advisory Commission on Election Integrity](#), September 12, 2017; Andrew W. Appel, Richard A. Demillo, Philip B. Stark, “Ballot-Marking Devices (BMDs) Cannot Assure the Will of the Voters,” pp. 16-17, April 21, 2019, <https://ssrn.com/abstract=3375755>.

¹⁰ “Securing the Vote: Protecting American Democracy,” National Academies of Sciences, Engineering, and Medicine, p. 80, <https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy>.