Securing the Vote

Nevaeh, Wallace

Department of Cybersecurity, Old Dominion University

CYSE495 Cyber Election Security

Professor Malik Gladden

9 August 2025

Ballot marking devices (BMDs), which allow voters to cast votes in an easy-to-use and accessible way while producing a verifiable paper record, have become a popular tool as election systems continue to modernize. Notwithstanding their advantages, BMD security is still a major worry since, like all computerized technologies, these systems are prone to procedural flaws as well as technological ones that might erode public trust in election results. The main elements and operational procedures of BMDs will be identified and explained in this article, along with any possible cybersecurity risks they may encounter. Useful enhancements and policy suggestions will also be suggested in order to increase the security and reliability of these devices. This research attempts to encourage the ongoing use of these technologies in a way that preserves the openness, accessibility, and integrity of the democratic process by addressing both the technological and procedural elements of BMD protection.

The most noticeable element is the user interface (UI), which is usually a touchscreen display. However, accessible controls like Braille keypads, audio ballots, and sip-and-puff devices may also be included. The ballot definition software that this interface interfaces to has pre-programmed election configuration files that list candidates, contests, and ballot types specific to the jurisdiction. To reduce the possibility of manipulation, the vote capture module digitally captures the voter's choices throughout the session in a secure setting.

After voting is complete, the printer module creates a paper ballot that displays the voter's selections in both human-readable text and, in certain systems,

machine-readable format like a barcode or QR code. Before casting their ballots, voters may check and verify the integrity of their choices thanks to this paper record, sometimes referred to as the Voter-Verifiable Paper Audit Trail (VVPAT). Additional security measures are put in place to guard against cyber attack and unwanted access, including secure boot procedures, cryptographic software signature, tamper-evident seals, physical locks, and air-gapping from the internet.

Voter authentication is the first step in the BMD voting process, during which election authorities confirm eligibility and provide a ballot activation card, token, or code associated with the relevant ballot type. The voter then makes options, navigates contests, and reviews choices before making a final decision using the interface. The paper ballot is produced by the BMD's printer module upon validation.

Voter verification is the following phase, where the voter checks the printed ballot to make sure their intended choices are reflected correctly. The voter has the option to request a fresh ballot and go through the procedure again if a mistake is found. After it has been validated, the ballot is tabulated by inserting it into an optical scanner or a safe ballot box. Last but not least, post-election audits, like risk-limiting audits, employ paper ballots as the official record to confirm that computerized counts are accurate.

Ballot marking devices are still vulnerable to cybersecurity risks, even though they increase accessibility and decrease some voter mistakes. Software flaws provide a serious concern because malicious code might change how ballots are printed, how selections are recorded, or how candidate names are displayed. Modified barcodes or QR codes might distort votes even with correct human-readable text since most voters are unable to validate these machine-readable forms. Other dangers include supply chain

breaches prior to devices reaching election authorities, insider threats from those with authorized system access, and physical access assaults during setup, storage, or transportation.

A combination of legal, procedural, and technical safeguards is needed to secure BMDs. In theory, every system ought to generate paper ballots that can be verified by voters and undergo risk-reduction audits following each election. In addition to rigorous air-gapping, cryptographic signatures, and secure boot procedures, devices should also be subjected to logic and accuracy testing before and after elections.

As far as procedure goes, jurisdictions should use tamper-evident seals, enforce chain-of-custody documents, and guarantee bipartisan oversight throughout testing and setup. To avoid unintentional misconfigurations and insider threats, poll workers must get training. Transparent communication of protections and voter education initiatives that promote careful ballot analysis can strengthen public trust. Lastly, electoral infrastructure must be maintained and enhanced with ongoing federal and state financing as cyber threats change.

Though their security cannot be taken for granted, ballot marking devices offer a useful way to increase accessibility and reduce some voter mistakes. Comprehending their elements and procedures reveals both their advantages and their drawbacks, ranging from insufficient voter verification to software manipulation. Through the implementation of stringent procedural restrictions, powerful public communication, and strong technology protections, election authorities may greatly improve the security and credibility of BMDs. This will contribute to the continued availability and security of these devices as a part of the democratic process.

References

Appel, A. W., DeMillo, R. A., & Stark, P. B. (2020). *Ballot-marking devices (BMDs) cannot assure the will of the voters*. Election Law Journal. Retrieved from https://www.cs.princeton.edu/~appel/papers/bmd-insecure.pdf

Cybersecurity and Infrastructure Security Agency (CISA). (2020). *Election security*. U.S. Department of Homeland Security. https://www.cisa.gov/election-security

National Institute of Standards and Technology (NIST). (2022). *Security considerations for remote electronic voting*. U.S. Department of Commerce. https://www.nist.gov/itl/voting

Verified Voting. (2023). *Ballot marking device security*. Verified Voting Foundation. https://verifiedvoting.org