

State of Maryland

Maryland's Voting System – Security Features and Practices

Voting System Information

- All voters in Maryland vote on paper ballots. This means that voted ballots can be re-tabulated if there is a need to do so.
- Maryland's voting system has ballot scanners, devices for voters with disabilities to mark ballots privately and independently, and a dedicated computer network at each local board of elections.
 - Each ballot scanner has a removable USB memory drive. This memory drive stores individual and accumulated results and digital images of all voted ballots¹.
 - The ballot marking device does **not** store or count votes. It simply marks the ballot.
 - The network adds the results from the memory drives and generates official results.
- Maryland's voting system has been rigorously tested by a federally accredited testing laboratory and certified by the U.S. Election Assistance Commission. The certification program tests a voting system against federal performance and security standards.
- No part of the certified voting system is connected to the Internet.
 - Ballot scanners are **never** connected to the Internet.
 - Ballot marking devices are **never** connected to the Internet.
 - Election results are **never** sent via modem over telephone lines.
 - The system's certified network is **never** connected to the Internet or the State Board of Elections' (SBE) network.
 - A local election official puts the results onto a memory device and takes the memory device to a computer with access to a primary and secondary secure server. Data are transferred via a virtual private network. This data is encrypted.
- Results released election night are not official election results. The day after the election, all USB memory drives are re-uploaded. This process starts the official election results process.

Duties and Responsibilities of Election Officials

- Election officials test each ballot scanner before each election. They scan pre-marked ballots and compare the results against expected results. If the results match, the unit can be used.
- After testing, election officials seal each ballot scanner and store it in a secure location until it is securely moved to a voting location. Each scanner is sealed until it is ready to use.
- SBE and the local boards of elections have contingency plans if the ballot scanner cannot be used. Each ballot scanner has a locked and secure place to store voted ballots that cannot be scanned because the ballot scanner is not working.
- Election officials audit the voting system results in two ways. SBE uses independent audit software to re-tabulate digital images of **all** voted ballots, and local election officials manually re-tabulate a small number of paper ballots. The audit results are compared against the voting system results.

Security Best Practices

- All State and local election officials receive regular security training.
- Only those election officials that need network access have access.
- Election officials only have the access they need to do their jobs.
- All employees with network access have had background checks.
- All administrative functions in the network and ballot scanners are logged.
- Data stored on the memory device are encrypted.
- Memory devices are assigned to a specific ballot scanner. If the ballot scanner detects a different memory device, the ballot scanner will not accept ballots.
- Before the voting system was first used in Maryland, a third party performed a security review on the election night results network. SBE implemented the recommendations.

¹ As each voted ballot is scanned, the ballot scanner captures a digital image of both sides of the ballot. This digital image can be retrieved and reviewed later.