Vote Capture

ON THIS PAGE

Types of vote capture processes

Risks and threats

How these components connect

Vote capture devices are the means by which actual votes are cast and recorded. Approaches vary greatly both across and within jurisdictions. Any given jurisdiction, and even a single polling place, is likely to have multiple methods for vote capture to accommodate both administrative decisions and different needs of voters.

For instance, on election day, a polling place may give voters the choice of electronic ballot marking devices or paper ballots. Additionally, voters with language needs or voters with disabilities may necessitate the use of additional components or a separate device.

Because of this diversity in vote capture approaches, providing specific recommendations around vote capture security is a detailed task. The EAC, in coordination with other federal partners, state and local governments, vendors, and others in the elections community, maintain standards and a certification program for vote capture devices. We will not try to replicate or alter those recommendations here, but we will provide a set of threats, risks, and categorizations to help guide officials toward best practices for vote capture devices.

Vote capture devices are often top of mind when thinking of election security-—and for good reason. Vote capture devices are where democracy happens: the voices of the people are heard via the ballots they cast. But they are a single part of a larger ecosystem for which a holistic security approach is necessary. Much attention has been paid to vote capture devices, and these efforts should continue; ensuring the security of vote capture devices, like any aspect of security, is a continuous process.

The primary inputs to vote capture devices are the ballot definition file, which describes to the device how to display the ballot, an activation key (for some electronic machines), and the ballot itself for scanning of a paper ballot. The primary output is the cast vote record.

In cybersecurity, we often talk about non-repudiation: the inability to deny having taken an action. Our democracy is founded in the opposite principle: your ballot is secret; no one should be able to prove who or what you voted for or against in the voting booth. This presents an inherent difficulty in maintaining the security of the voting process. We intentionally create voter anonymity through a breakpoint between the fact that an individual voted and what votes they actually cast. We never want to enable the ability to look at a marked ballot and track it back to a specific voter.

Instead, we must carefully protect the integrity and secrecy of the vote cast through the capture process and into the process of tabulation. To do this, best practices call for applying a series of controls to mitigate the risk that a vote capture device is functioning improperly, to identify problems if they occur, and to recover without any loss of integrity.

Types of vote capture processes

Vote capture generally occurs in one of six ways:

1. *Voter marked and hand counted paper balloting.* Ballots are typically pre-printed or printed on demand, given to voters who fill them out by hand, collected, and counted by hand. Hand counting represents a relatively small share of total votes. This category usually covers some mail-in ballots.
2. *Voter marked paper balloting with scanning.* Ballots are typically pre-printed or printed on demand, given to voters who fill them out by hand, and collected. Votes are tabulated by scanning the paper ballot with an optical or digital scanner, either individually or in batches. This category covers some mail-in ballots. These scanners have several flavors, with the most common being: precinct count optical scanners (PCOS), central count optical scanner (CCOS), and simply optical scanners (OS).
3. *Electronic marking with paper ballot output.* Rather than handing out a paper ballot, the voter is directed to a machine that displays the ballot. The voter casts votes, and the machine prints a marked ballot. These types of machines are referred to as ballot marking devices (BMD). These printed ballots are tabulated either individually or in batches. Votes are usually tabulated by scanning the paper ballot with an optical or digital scanner, though are sometimes counted by hand. The vote capture device does not store a record of the vote selections. This type of vote capture device is commonly referred to as a ballot marking device.
4. *Electronic voting with paper record.* The voter is directed to a machine that displays the ballot. The vote is captured on the machine and either transmitted digitally to a central machine for tabulation, or removable media is extracted from the machine at a later time to transmit a batch of captured votes. At the time the vote is captured, the machine creates a printed record of the vote selections that the voter can verify. That record remains with the machine. This type of vote capture device is commonly referred to as a direct record electronic (DRE) device with voter verifiable paper audit trail (VVPAT).
5. *Electronic voting with no paper record.* The same as electronic voting with paper record, but the machine does not print a record of the captured vote. Captured votes are only maintained digitally, typically in multiple physical locations on the device and, sometimes, on a centrally managed device at the polling location. This type of vote capture device is commonly referred to as just a DRE.
6. *Electronic receipt and delivery of ballots conducted remotely.* The majority of ballots received by voters using this method are voters covered by the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA). Though most UOCAVA votes involve paper ballots, there is a sub-set of this population that submits their marked ballot in a digitally-connected method such as email or fax. Once received digitally, the voter's vote selections are transcribed so that the vote selections are integrated into the vote tabulation and results reporting systems; these systems do not have network connections to the voting system. Voting methods commonly called internet voting or mobile voting fall under this process.

Risks and threats

The consequences of a successful attack in a vote capture device are significant: the intentions of a voter are not properly reflected in the election results. The vast majority of vote capture devices are not network connected systems. This helps limit the attack paths and therefore the risks to which they are subject—in cybersecurity parlance, a non-networked approach substantially reduces the attack surface. Therefore, to change a large number of votes typically requires access to the vote capture machine hardware or software, or the ability to introduce errors through the devices that program the vote capture device or download results from the vote capture device. Moreover, most vote capture devices are tested and certified against criteria defined by the EAC, a state or local entity, or both, though evolving threats can change the risk profile of a device even if it has previously been certified.

The last type of vote capture described above, *'electronic receipt and delivery of ballots conducted remotely'* can take on a large number of flavors. In terms of cybersecurity-related risks, for activities like emailing marked ballots, election officials must consider especially risks involved in the transmission of the ballot. If the transmission of the marked ballot is done via digital means, it is subject to the risks of that transmission mode.

Regardless of approach, risks exist, and they mostly stem from the transfer of data to or from vote capture machines. Specifically, they include:

- If ever networked, risks associated with established (whether persistent or intermittent) network connectivity,
- Risks associated with the corruption of removable media or temporary physical connections to systems that are networked,
- Security weaknesses in the underlying COTS products, whether hardware or software,
- Security weaknesses in proprietary products, whether hardware or software,
- Errors in properly managing authentication and access control for authorized users, and
- Difficulty associated with finding, and rolling back, improper changes found after the fact, especially in the context of ballot secrecy.

How these components connect

Each type of vote capture process should have risks evaluated individually based on its type of connectivity.

The numbering in the right column below align with the types of vote capture processes above.

Connection Types for Vote Capture

Connectedness	System Type and Additional Information
Network Connected	If a vote capture machine transmits data for any reason—or even if the functionality is enabled regardless of whether it is used—it should be considered network connected. Although many jurisdictions program the vote capture devices with the ballot definition using indirectly connected methods, some use methods to load the ballot definition files to the vote capture device by transmitting the data over a closed-local area network. Also, many central count scanners, used for Voter marked paper balloting with scanning in batches (usually vote by mail ballots) are similarly networked on a closed-LAN. Some electronic vote capture machines also directly transmit data for election night reporting.
Indirectly Connected	Type 2: *Voter marked paper balloting with scanning.* Paper ballots do not include an electronic component. While scanners are not typically network connected devices, they must be programmed to understand the ballot format and must transmit captured vote data to another, usually network connected, device. Type 3: *Electronic voting with paper ballot output.* In addition to the role of the scanners, the vote capture machines are typically not network connected, but must be programmed to display the ballot and print the ballot in the correct format. Type 4: *Electronic voting with paper record.* The vote capture machines are typically not network connected but must be programmed to understand the ballot format and must transmit captured vote data to another, usually network connected, device. Type 5: *Electronic voting with no paper record.* The vote capture machines are typically not network connected but must be programmed to understand the ballot format and must transmit captured vote data to another, usually network connected, device. Note: If a vote capture machine transmits data for any reason—or even if the functionality is enabled regardless of whether it is used—it should be considered network connected.
Not Connected	Type 1: *Voter marked and hand counted paper balloting.* Out of scope in this handbook as the vote capture process does not include a digital component.
Additional Transmission-based Risks	Type 6: *Electronic voting conducted remotely.* These methods vary greatly and must be addressed on a case-by-case basis. At minimum, when web-based, email, or fax transmission is used in either direction, it leverages a digital component and should incorporate the relevant transmission-based mitigations.