Pollbooks

Pollbooks assist election officials by providing voter registration information to workers at each polling location. Historically, these were binders that contained voter information and could be used to mark off voters when they arrived to vote. While paper pollbooks remain in use today and are common as a backup strategy, many pollbooks are electronic and aim to facilitate the check-in and verification process at in-person polling places. While this section focuses primarily on electronic pollbooks (epollbooks), it also recognizes that, depending on the implementation, producing paper pollbooks can carry transmission-based risks.

These epollbooks play a critical role in the voting process. They are necessary to ensure voters are registered and are appearing at the correct polling place, and their efficient use is necessary to ensure sufficient throughput to limit voters' wait times. These epollbooks are most often dedicated software built on COTS hardware (usually a tablet) and riding on COTS operating systems, like Android or iPadOS, though laptops with Windows or MacOS are still in use as well.

The primary input to epollbooks is the appropriate portion of the registration database. The primary output is the record of a voter having received a ballot, and in some cases providing a token to activate the vote capture device. In some cases, for instance where same-day registration is permitted, epollbooks may require additional inputs and outputs to allow for election day changes. A proper record of a voter voting is critical, both auditing and properly giving "credit" to the voter; some states remove voters from the rolls if they go too long without having cast a ballot.

Paper pollbooks are produced from digital records, including digital registration databases. Having taken appropriate measures to mitigate risk for voter registration components, secure transmission of voter information to a printer—whether at the state or local level, or via commercial printing services—protects the integrity of the information in printed pollbooks.

Risks and threats

Attacks on epollbooks would generally serve to disrupt the election day process by one of these three situations:

1. Attacking the integrity of the data on the pollbook by altering the information displayed from voter rolls,
2. Disrupting the availability of the epollbooks themselves, or
3. In some cases, causing issues with the vote capture device by altering an activation token.

Any of these situations could result in confusion at the polling locations and likely a loss of confidence in the integrity of election results. A successful attack of the first variety would more likely occur in voter registration systems by deleting voters from rolls or subtly modifying information in a way that causes delays in their casting a ballot or forces them to use the provisional ballot process, but could also occur in the epollbooks themselves and during the transmission of data to the epollbook.

An epollbook may or may not be connected to a network. If they are network connected, they must be treated as having the risks of a network connected device, even if the functionality is not used. While threats are continually evolving, appropriate measures can be taken to address this largely known set of risks.

The primary cybersecurity-related risks to paper pollbooks come from the transmission of pollbook data to formatting and printing services. Data will typically be loaded onto an epollbook through a wired connection, a wireless network, or removable media such as a USB stick. To that end, risks and threats include:

- Risks associated with established (whether persistent or intermittent) internet connectivity,
- Network connections with other internal systems, some of which may be owned or operated by other organizations or authorities, including private networks for epollbooks,
- Security weaknesses in the underlying COTS products, whether hardware or software,
- Security weaknesses in the dedicated components, whether hardware or software,
- Errors in properly managing authentication and access control for authorized users, including permissions for connecting to networks and attaching removable media, and
- Difficulty associated with finding, and rolling back, improper changes found after the fact.

These risks must be managed to ensure proper management of pollbooks. Because most are risks and threats shared among users of COTS products more broadly than in elections, there is a well-established set of controls to mitigate risk and thwart threats.

How these components connect

Managing risks associated with epollbooks will generally fall into one of two classifications based on the way they can connect to load data and, if applicable, transmit data.

Connection Types for Pollbooks

Connectedness	System Type and Additional Information
Network Connected	Pollbook connects via a wired or wireless network
Indirectly Connected	Pollbook connects via a physical media connection or removable media (e.g., USB sticks and other flash media that are physically connected and disconnected to other devices).
Not Connected	Paper-based pollbooks.
Additional Transmission-based Risks	Transmission of data for paper-based pollbooks for formatting or printing.