Vote Tabulation

ON THIS PAGE

Risks and threats

How these components connect

Vote tabulation is the aggregation of votes (e.g., cast vote records and vote summaries) for the purpose of generating totals and results report files. Many distinguish between vote tabulation and vote aggregation. Most commonly, the former is totalling of votes from various machines by a precint, and the latter totalling of votes from precincts by the jurisdiction. For the purposes of this section, we treat them synonymously.

This section on vote tabulation is considered separately from both the EMS of which tabulation is usually a part, and vote capture machines that also tabulate (or aggregate). Here, vote tabulation is focused on tabulation occurring across precincts, counties, etc., and covers both official and unofficial vote tabulation.

Risks and threats

Similar to vote capture devices, attacks on vote tabulation would seek to alter the counting of cast votes. This impact would be felt through the determination of the election outcome as well as the potential for confusion if initially reported outcomes did not agree with later certified results.

Vote tabulation typically involves either dedicated software or COTS software running on COTS hardware and operating systems, though some dedicated hardware is also in use. Vote capture devices most often transmit the vote data (e.g., results, cast vote records) to the vote tabulation system using removable media, though sometimes that data is transmitted across a network. Vote data is most often transferred across jurisdictions and to the state through uploads via direct connections such as a virtual private network, local network connections, faxes, or even phone calls.

The primary risks to vote tabulation are similar to those of other COTS-based systems: a compromise of the integrity or availability of aggregated votes totals could reduce confidence in an election, if not alter the outcome. Though the vote data is likely loaded to these systems via removable media, most risks stem from vulnerabilities in these networked systems themselves. Such risks and threats include:

- Network connections with other internal systems, some of which may be owned or operated by other organizations or authorities,
- 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,
- Lack of confidentiality and integrity protection for transmitted results,
- Difficulty associated with finding, and rolling back, improper changes found after the fact, and
- Infrastructure- and process-related issues associated with backup and auditing.

These primary risks must be managed to ensure proper management of vote tabulation systems. Because they are risks and threats shared among users of COTS products, there is a well-established set of controls to mitigate risk and thwart threats.

How these components connect

Depending on the implementation, these systems should be considered network connected or indirectly connected. They may interface with the internet, and, even if they do not, almost certainly interface with a system that is connected to a network.

Connection Types for Vote Tabulation

Connectedness	System Type and Additional Information
Network Connected	In some cases, vote tabulation equipment will be network connected, whether through a wired or wireless connection.
Indirectly Connected	If vote tabulation equipment is not network connected, it is indirectly connected through removable media.
Not Connected	Not applicable.
Additional transmission-based risks	Not applicable.