State and Local Election Management Systems

States and local jurisdictions generally have established, persistent Election Management Systems (EMSs) that handle all backend activities for which those officials are responsible. Each state has an EMS, and each local jurisdiction will typically have a separate EMS that may, but will not always, connect to the state's system. The extent to which the two systems are integrated, if at all, varies greatly.

For the most part, a local EMS is used to design or build ballots, program the election database, and report results. A state EMS typically does a wide variety of things including election night reporting and military and overseas ballot tracking.

An EMS will also typically include vote tabulation. For the purposes of this handbook, vote tabulation is broken out into its own section.

EMSs can have a wide variety of inputs and outputs that will depend on the separation of duties between the state and the local jurisdictions and the manner in which each state or local jurisdiction handles particular aspects of the election process.

Risks and threats

While EMSs are typically dedicated software that carries its own risks, that software generally runs on COTS software and hardware. Many risks and threats associated with EMSs are similar to those of other systems running on COTS IT hardware and software, and 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 the dedicated components, whether hardware or software,
- Errors in properly managing authentication and access control for authorized users,
- Difficulty associated with finding, and rolling back, improper changes found after the fact, and
- Infrastructure- and process-related issues associated with backup and auditing.

The consequences of a successful attack in an EMS are significant. These include the inability to properly control election processes and systems or, depending on the functions of the EMS, incorrect assignment of ballots to their respective precincts or other errors. Furthermore, successful manipulation of an EMS could result in cascading effects on other devices that are programmed from the EMS, potentially including voting machines and vote tabulation.

To help manage these risks, most election offices do not have network connections to their EMS, and rarely have internet connections. Instead, they keep the EMS isolated as a standalone machine or on a separate network that has no internet connection and is solely dedicated to the functioning of the EMS. Data transfers to and from the EMS are conducted with removable media only. This is an indirect connection and presents a particular set of risks to mitigate.

How these components connect

The diversity of functions delivered by an EMS makes it difficult to generalize the level of connectedness of any given system, but most will have at least some aspects of a network connected system. A host of factors impact connectedness, such as whether a state or local EMS is network connected, communications with the EMS leverages connections such as a Secure File Transfer Protocol (SFTP), or all data is transferred through removable media.

Connection Types for Election Management Systems

Connectedness	System Type and Additional Information
Network Connected	Unless known definitively to have no network capabilities, treat an EMS as network connected.
Indirectly Connected	If known definitively to have no network capabilities, treat an EMS as indirectly connected.
Not Connected	Not applicable.
Additional Transmission-based Risks	Not applicable.

Previous Pollbooks

Next Vote Capture