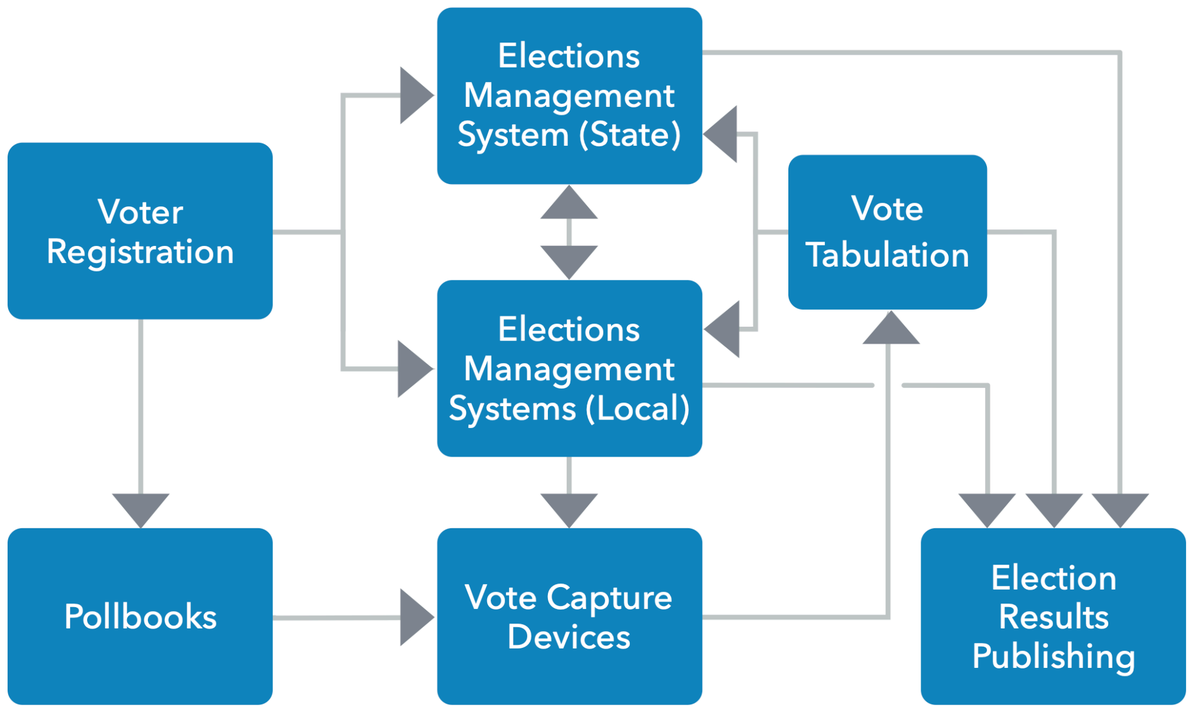
This section draws from the Handbook for Election Infrastructure Security. It is an informative section to help understand and conceptualize how the various election technology components work and interact. While this Essential Guide to Election Security is our recommended go-to for best practices, you can still download the Handbook.

A Primer on Election Infrastructure Security

There are many flavors of elections infrastructure, both from a technology and a process perspective. This is true far beyond just the different types of vote capture and vote tabulation devices. Poll worker management systems, results publishing, and many other systems all have to come together, often requiring a careful orchestration of many systems provided by many vendors. As the joke goes, "there's no easy way to describe an election process in a single graphic without leaving someone out or making somebody unhappy."

That said, many experts have studied the election processes at length, and there are several fundamental components common to nearly all elections systems in the United States.

In some jurisdictions, the owner of various aspects of the architecture may differ, but the fundamentals of the types of systems used to perform the task are generally the same. For that reason, many of the best practices associated with those systems will closely follow IT security best practices, though there are often additional business processes and practices that help mitigate risk.



Many of the components in elections infrastructure are built on general purpose computing machines, such as traditional web servers and database platforms. While this means they are often subject to the same attacks as those in other sectors, it also means experts have identified best practices to mitigate many of the risks.

Each of these components may exist at the state level, at the local level, or both, and some will not be applicable in certain jurisdictions. Even where there is a substantial amount of legacy infrastructure—-old systems that are difficult or impossible to update—-much can be done to mitigate risks. These systems are described below and appropriate best practices and actions are provided throughout this Guide.

The next section describes the connectedness of election systems, to help understand and conceptualize how various types of election technology are (or are not) connected to each other, the internet, and other networks.

The remainder of the sections give background on the architecture of election systems, the role information technology, the risks and threats for each, and how they connect in the context of cybersecurity risk management. Importantly, this primer gives information about protecting the infrastructure. There are many process-oriented risk mitigations employed throughout election administration that are not addressed here.

Previous
Mapping to the Handbook for Election Infrastructure Security

Next
Election Systems and Their Network Connections