The Essential Guide to Election Security

Want to skip straight to the action?

- Determine your maturity level
- See the Level 1 maturity best practices and the Level 2 and Level 3 maturities best practices
- For a true beginner, read our primer on election infrastructure security for an introduction into the types of systems used in election administration and the risks and threats associated with them.

To first learn more, read on...

A Best Practices Resource for Election Professionals

The Center for Internet Security (CIS) has developed this Essential Guide to Election Security to serve as a first-stop resource for election officials to learn about best practices in election security. This can aid the process of building a program designed to meet individual needs and abilities of any given election office.

This Guide considers the wide range of technical capabilities and resource availability among the many thousands of election offices in the United States. While providing guidance for all organizational maturities, it emphasizes guidance for small jurisdictions without extensive cybersecurity resources available to them. The most important practices are included for those jurisdictions, with opportunities to ramp up as they mature.

It's an online guide and is continually updated, though readers can easily export it as a PDF. Read more about this Guide and how it came to be in our about this guide appendix.

Who should use this Guide?

This Guide helps election officials and their staffs understand their organizational cybersecurity readiness and take steps to improve. It is for jurisdictions of all of sizes and types, though which best practices apply to you will depend on several factors, including, but not limited to:

- The type of jurisdiction (state vs. county vs. municipality),
- The structure of election administration in a given state (top-down vs. bottom-up),
- The types of election equipment owned, and
- How IT responsibilities are shared with other functions in the jurisdiction, such as when IT is shared with the rest of the county.

Election technology providers and other stakeholders will also find much of the information useful as they consider how their work impacts outcomes in election administration and security.

Structure of this Guide

The Guide is organized into several sections:

1. An introduction.
2. A description of maturities and how they are used in the document.
   - Maturities are used to reflect an organization's capabilities in managing cybersecurity risk
   - Best practices and actions are prioritized based on maturity, so knowing your maturity is important to chart your path through the rest of the Guide.
3. A set of best practices for organizations to implement.
   - Each best practice has an introduction to the topic as well as goals and actions for each maturity level.
   - There are also lists of cost-effective tools, additional resources, and mappings to the CIS Controls.
   - There is a mapping to best practices from the Handbook for Election Infrastructure Security, the predecessor to this Guide. Find a full mapping here.
   - There is also a set of worksheets you can download if you are at the Level 1 maturity and need to complete the baseline priority best practices.
   - The best practices are ordered as follows:
     1. Addressing physical threats: First, be safe. Then be cybersecure.
     2. Join the EI-ISAC: Becoming a member gives you free access to many of the tools in the rest of the best practices.
     3. Baseline priority best practices for the Level 1 maturity: most of the actions within these best practices are supported with the worksheets described above. See the Level 1 maturity the baseline priority best practices.
     4. Priority based on CIS's Community Defense Model 2.0. See the top priority safeguards mapped to the best practices.
4. Additional references, tools, and related information in appendices.
5. A glossary and set of acronyms.

You can create a PDF by hovering over the "v:latest" in the bottom left, at the bottom of the navigation panel. The box that pops up will have a "PDF" link. Hit that link and you'll get a PDF based on the current version of the Guide.

Find more detailed information on this Guide and how to use it in our how to.

Identifying Your Organization's Security Lead

Regardless of the size of your office, one of the most effective steps to increasing your security posture is identifying someone who you'll hold accountable for making progress in examining your current maturity status, maintaining existing security processes, implementing best practices, and taking additional steps towards increasing your security posture.

This individual should own and maintain the process of improving your cybersecurity posture, whether you use this Guide to do so or any other resource. Accountability matters!

A Little Encouragement Before You Start

Many elections officials may not consider themselves security or IT professionals. This Guide takes this into consideration. In addition to implementing the best practices for your maturity, we encourage you to read through the entire Guide. It can provide you an understanding of the types of actions you may want to take as you continually improve your cybersecurity posture.

This guide in a continual development process, and CIS is interested in feedback from all readers. Ideas for content and usability improvements are most welcome, as are any questions if you find yourself with a question or needing more help. Always feel free to reach out to the EI-ISAC elections team at elections@cisecurity.org. We also encourage you to use trusted partners and peers at the federal, state, and local levels for guidance and support.

This Guide was made possible through support from the Democracy Fund. The content of this Guide is the sole responsibility of CIS and may not reflect the views of its funders.