About the Essential Guide to Election Security

When The Handbook for Election Infrastructure Security was published in 2018, election officials had much less guidance to rely on. Today, they often have the opposite problem: an enormous amount of guidance to navigate. With so much guidance and so many tools and approaches available, it's difficult for any given election official to know what will best work for them.

This Guide aims to solve that problem and aid the process of building a program designed to meet the individual needs and abilities of any given election office.

Why does this Guide look like a webpage? (Or does it??)

You might be reading this online. Or you might be reading a PDF. If the latter, it's because your PDF was built from an online version. Here's why we're keeping all of the content for the Guide online:

CIS published The Handbook for Election Infrastructure Security in early 2018, just before the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) launch.

In 2021, the EI-ISAC began working with the election community to update that Handbook. A common item of feedback we received was that the static nature of the Handbook meant it didn't include any of new and evolving the best practices that weren't already in place in early 2018.

Creating an updated version of that Handbook would've left us in the same position: the pace of new best practices and services available to secure election infrastructure is too rapid to rely on a static model for communicating them to election officials.

Instead, we decided to create this dynamic, always up-to-date online Guide. It can still be exported as one big PDF, but when you do so, you will get the best practices current as of the moment you hit the button to create the PDF.

We can also embed and link to more engaging content like videos and examples. When best practices change, officials face new risks, or different resources become available, we can quickly update the Guide to reflect the new state of the world.

What's Changed

Election offices operate in an environment heavy on information technology (IT). The teams administering elections have been protecting these environments for decades. Still, as the threats evolve and the measures for mitigating IT risk increase in complexity, their task becomes ever more difficult.

In early 2018, CIS, with significant contributions from the election community, published its Handbook for Election Infrastructure Security, a guide to assist election offices in defending their IT systems from cybersecurity threat actors. It consisted of 88 best practices to mitigate risk across all types of election equipment.

The EI-ISAC received positive feedback from the election community on the Handbook's value. In the four years since then, several significant changes have occurred:

1. The CIS Controls, on which many of the 88 best practices are based, underwent a major revision.
2. The Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) has greatly increased the number of freely available tools and services for election offices across the country.
3. Since releasing the Handbook, the EI-ISAC has developed a series of best practice guides and other information. Other organizations have also contributed to the body of knowledge for security election infrastructure and related activities, including:
   - A wide array of guidance and tools available from the Cybersecurity and Infrastructure Security Agency (CISA) and other government agencies; and
   - A body of work for other academic and nonprofit organizations such as the *Global Cyber Alliance <https://gcatoolkit.org/elections/>*, Harvard University's Belfer Center, the Brennan Center for Justice, and others.
4. Election officials have made significant strides in meeting today's threats, but uneven and insufficient funding has caused a wide array of differences in cybersecurity postures.
5. The nature of threats has changed. In 2016, nation-state actors posed most of the apparent risks. Today we have more information on real-world attacks. We know that they come various sources and come from both virtual and real-life sources.
6. Managing inaccurate information about election administration has become one of the thorniest and most pervasive threats to democracy and election officials need guidance on mitigating misinformation and threats and harassment of election officials.

How is this version different?

These changes to the election ecosystem warrant a rethinking of the original Handbook. Developed in collaboration with federal partners, state and local election officials, and election technology providers, this update takes several major steps to address this continual evolution of the election space:

1. We've developed a more rigorous maturity model. The original Handbook simply listed high, medium and low priorities for each of the 88 best practices. This gave a rough order in which to implement best practices, but didn't account for a given jurisdiction's resources or capabilities. We now have three maturities and a decision tree for finding an organization's fit. For any best practice, the approach to implementation addresses whether, for instance, the office has limited technical expertise or well-trained teams of IT security specialists. These are described in detail in the Maturities section.
2. We've incorporated new best practices that cover the many threats and opportunities that have emerged, like around managing inaccurate information about election administration, understanding artificial intelligence in elections, and how to access free services. We'll continue adding and evolving guidance as necessary.
3. For each best practice, we've provided more information on what actions to take and how to get the job done, so even readers with the least technical knowledge know how to get started.
4. We've added a substantial listing of available resources and additional direction throughout the best practices.
5. We've moved from the original Handbook—a static paper or PDF document—to a more dynamic web-based experience. As described earlier, this allows continually updated online tools, videos, and resources as threats evolve and new opportunities emerge.
6. We're developing a "peer support" tool to enable election teams to communicate with each other, creatively solve problems, share best practices, and rapidly and collaboratively respond to emerging issues. Expect to see this later in 2022.

In addition to these, there are many minor updates we hope improve the usability of this Guide, allowing it to serve as an effective tool for every election office regardless of size, resources, or technical sophistication.

We Love Feedback

We'll take feedback at any time. Provide feedback 1 of 2 ways:

1. Send any feedback to essentialguide@cisecurity.org. You can export a PDF (hover over "v:latest" in the bottom left and hit "PDF") and comments directly in it. You can also put feedback directly in the email.
2. If you're familiar with GitHub, we'd love to get feedback through issues and pull requests. You can get to the repo through the menu in the bottom left of any Read The Docs page (hover over "v:latest" and hit "view" under "On Github"). Feel free to fork the repo and create a PR when you're ready, or directly add issues to the repo with the tag "community review."

Thank you!