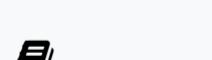


INTRODUCTION[The Essential Guide to Election Security](#)**MATURITY**[Maturities](#)[Determining Your Maturity Level](#)[Prioritizing Best Practices for the Level 1 maturity](#)[Prioritizing Best Practices for the Level 2 and Level 3 maturities](#)**BEST PRACTICES**[Index of Best Practices](#)[Addressing Physical Threats](#)[Join the EI-ISAC](#)[Asset Management](#)[Encrypt Data at Rest](#)[Encrypt Data in Transit](#)[Managing Infrastructure with Secure Configurations](#)[User Management](#)[Backups](#)[Incident Response Planning](#)[Building and Managing Staff](#)[Patching and Vulnerability Management](#)[Remediate Penetration Test Findings](#)[Perform Internal Penetration Test](#)

v: latest

Managing Removable Media



ON THIS PAGE

Goals

Actions

Level 1 Maturity

Level 2 and Level 3 Maturity

Cost-Effective Tools

Mapping to CIS Controls and Safeguards

Mapping to CIS Handbook Best Practices

While removable media such as [USB](#) drives and [PCMCIA](#) cards are going extinct in most IT environments, they are still an important tool for environments in which some machines are not network connected.

In the election environment, the election management system and voting systems typically have no network connections and are not on the internet, so removable media remains a part of everyday life.

While keeping hardware and software off of networks can eliminate certain threats, others can be introduced by exchanging data with removable media. Election offices need to be sure to properly source and sanitize anything used to physically transfer data between machines.

Goals

1. Employ appropriate media sanitization (Level 1 maturity)
2. Effectively use removable media in the election environment (Level 1 maturity)

Actions

For Managing Removable Media, the necessary actions vary by maturity, as detailed below.

Level 1 Maturity

1. Wherever possible, use removable media only once. This could mean using a [CD-R](#), [DVD-R](#), or other once-write media, but that can be difficult with today's machines.
2. Instead, use [USB](#) sticks or other removable media like flash cards.
 - o If your budget can sustain it, use them once. If not, follow a media sanitization guide to reduce the risk of introducing [malware](#) into your non-networked machines.
3. Source your removable media from trusted sources or, if you can't, the consumer market, like a big box store where there's enough volume that it would be difficult to target you as an election office.
 - o CIS's [cybermarket](#) offers USB sticks and other products from vetted vendors.
4. Regardless of all other guidance, be sure to follow the guidance and directives of their chief election official and voting system vendor.

Level 2 and Level 3 Maturity

Organizations operating at a Level 2 or Level 3 maturity should take additional actions, including:

1. Make removable media sanitization a part of your larger media sanitization program. NIST [SP 800-88](#) is the gold standard for such a program.

Cost-Effective Tools

- CIS's [cybermarket](#): A buying guide for EI-ISAC members, providing products from trusted vendors at discounted rates.

Mapping to CIS Controls and Safeguards

- 3.9: Encrypt Data on Removable Media (Level 1 maturity)
- 10.3: Disable Autorun and Autoplay for Removable Media (Level 1 maturity)
- 10.4: Configure Automatic Anti-Malware Scanning of Removable Media (Level 2 maturity)

Mapping to CIS Handbook Best Practices

- 4, 22, 55, 63

[Previous
Website Security](#)[Next
Exercising Plans](#)