Encrypt Data in Transit

Any data that is being actively transferred, termed “data in transit,” can present substantial risks for election offices. One of the biggest risks to election integrity occurs when transferring ballot definition files, ballot PDFs, and other such data between otherwise well-protected devices.

For the purposes of this guide, data in transit may refer to data sent over a network. Data stored on physical media being moved from one physical location to another are addressed in the removable media best practice. Data stored on other storage devices, like local storage on a computer or network storage are addressed in the encrypt data at rest.

An election office will often move data between its own systems and between its systems and those of vendors or other partners. An important example is transferring ballot PDFs to a commercial printer that produces the paper ballots for an upcoming eleciton.

The most important thing to know about encrypting data in transit is that the common ways you transfer data are typically easily distinguished between encrypted and unencrypted, or secure and insecure, implementations. These different implementations are called protocols. For instance, you should never transfer, exchange, or submit important data (election data, user credentials, or the like) via a website that starts with HTTP; it should always start with HTTPS.

Encrypted data transfer protocols are ubiquitous; you just need to make sure you and whomever you’re exchanging data with use them.

Goals

1. Use encrypted protocols when transferring all important data (Level 1 maturity)
2. Ensure vendors and other partners encrypt data in transit (Level 1 maturity)

Actions

For Encrypt Data in Transit, the necessary actions are the same for all maturity levels.

1. Use encrypted data transfer protocols for all sensitive data.
   - Use HTTPS, not HTTP
   - Use FTPS, SFTP, SCP, or WebDAV over HTTPS, not FTP or RCP
   - Use SSH2, not Telnet
   - Use RDP, not VNC
2. Use an up-to-date version of these protocols compatible with your systems, for instance TLS v1.2 or 1.3, not TLS 1.1 or 1.0.
3. Set defaults for these protocols and versions wherever possible throughout your systems.
4. Impose the same encryption requiremens on vendors and other partners as you use yourselves.
   - You can use the managing vendors best practices to help implement appropriate best practices across all of your vendors.

Cost-Effective Tools

- Appropriate encryption capabilities are very likely built into the tools and services you are already using. For most, the proper configuration – turning them on and setting them to use the version you want – is all that is necessary.

Mapping to CIS Controls and Safeguards

- 3.10: Encrypt Sensitive Data in Transit
- 12.6 Use of Secure Network Management and Communication Protocols
- 15.4: Ensure Service Provider Contracts Include Security Requirements

Mapping to CIS Handbook Best Practices

- 8, 12, 84