Managing Vendors

In nearly all election jurisdictions, many of the hardware, software, and services that underpin our elections—from voter registration and election management systems to pollbooks and vote capture devices—are procured from private vendors.

Even simple public-facing websites may be procured and their security—or lack thereof—may have consequences on elections. The industry partners from which IT is procured play a critical role in managing the security risks inherent in elections.

Understanding and properly managing security expectations in the procurement process can have a substantial impact on the success of the election process.

Goals

1. Understand how to use procurements to achieve security goals (Level 1 maturity)

Actions

For Managing Vendors, the necessary actions are the same for all maturity levels.

1. Use CIS's A Guide for Ensuring Security in Election Technology Procurements to guide your procurements.

Cost-Effective Tools

- CIS's A Guide for Ensuring Security in Election Technology Procurements: Provides model procurement language that election officials can use to communicate their security priorities, better understand vendor security procedures, and facilitate a more precise cybersecurity dialogue with the private sector.

Mapping to CIS Controls and Safeguards

- 15.1: Establish and Maintain an Inventory of Service Providers (Level 1 maturity)
- 15.2: Establish and Maintain a Service Provider Management Policy (Level 2 maturity)
- 15.3: Classify Service Providers (Level 2 maturity)
- 15.4: Ensure Service Provider Contracts Include Security Requirements (Level 2 maturity)
- 15.5: Assess Service Providers (Level 3 maturity)
- 15.6: Monitor Service Providers (Level 3 maturity)
- 15.7: Securely Decommission Service Providers (Level 3 maturity)

Mapping to CIS Handbook Best Practices

- 18, 20, 34, 37, 62, 73

Previous
Managing Inaccurate Election Information

Next
Defense-in-Depth