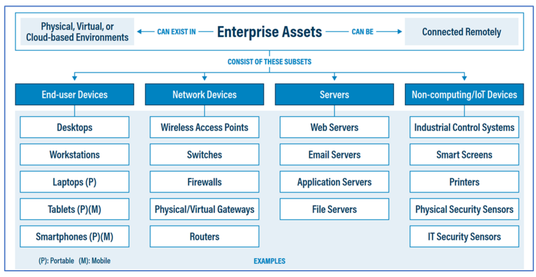
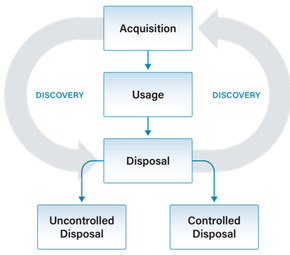
Asset Management

Without a clear understanding of what computers and other technology you must protect, you'll have a hard time ensuring everything you own is properly secured. Assets can take many forms, with varying complexity and value to the organizations.



There are many free tools that can help automate the job of inventorying and managing physical devices, and for many organizations simple tools like spreadsheets are good enough. All assets have a lifecycle and need that lifecycle managed.



You should also know how to dispose of assets. Various types of hardware and software have specific disposal procedures based on the criticality and sensitivity of the equipment and the data it contains.

Goals

1. Maintain proper records of all assets (hardware, software, cloud platforms) throughout their lifecycle (Level 1 maturity)
2. Always know the physical location of hardware (Level 1 maturity)
3. Conduct maintenance and protecting assets from loss, theft, and tampering (Level 1 maturity)
4. Properly dispose of assets (Level 1 maturity)

Actions

For Asset Management, the necessary actions vary by maturity as detailed below.

Level 1 Maturity

For those organizations operating at a Level 1 maturity, keep it simple. You need to know what physical assets you have, where they are, how they're used, how they're protected, and how they're maintained. Understanding this information will help you properly defend your network and other IT assets.

1. Create an inventory of all state and county technology owned and operated in support of election activities. This includes hardware assets, software, and cloud service providers such as laptops, software suites (e.g., Adobe), and email providers.
   - If you have a fewer than a couple dozen of assets to track, it's probably easiest to do so with a table or spreadsheet. You can do this on paper, though if you use paper, you should also maintain a digital records that you can backup. You can use the Level 1 maturity IT Inventory Worksheets as a template or the CIS Enterprise Asset Inventory Worksheet.
   - Even if your county maintains these records, it's best to do so yourself, as you're ultimately accountable for what happens in your environment.
   - Contractor systems should be included in your inventory.
   - This inventory will contain sensitive security information that should not be shared with untrusted parties.
2. Investigate unknown assets discovered during the inventory process. Remove assets that should not be attached to the network. This includes both hardware and software assets.
3. Properly dispose of assets, including shredding paper assets, wiping software assets, and decommissioning hardware assets. Follow all relevant laws for retaining and disposing of all assets.
   - Both NIST and the EAC have extensive guidance on IT asset sanitation and disposal.

Level 2 and Level 3 Maturities

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

1. Maintaining digital inventory records.
2. Applying asset tags.
3. Implementing software tools to discover physical devices on your networks.
4. Allowlist authorized software to prevent unwanted software installation.

Enterprise tools exist to automate this process and if you are at a higher maturity, you should be implementing one of them.

Ensure the inventory records the network address (if static), hardware address, machine name, data asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, mobile device management (MDM) tools can support this process, where appropriate.

This inventory should include assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under the control of your organization. Review and update the inventory of all enterprise assets bi-annually, or more frequently.

Cost-Effective Tools

- CIS Enterprise Asset Inventory Worksheet: An excel workbook suitable for small operations with a limited number of assets
- GCA Cybersecurity Toolkit for Elections: Know What You Have: A toolbox with links to free tools relevant to this best practice
- Nmap: Famous multipurpose network scanner used by system administrators and hackers across the world to identify which devices are connected to your network
- ZenMap: Easy-to-use graphic user interface for Nmap
- Spiceworks: Free IT inventory and asset management software to identify devices and software on your network

Mapping to CIS Controls and Safeguards

- 1.1: Establish and Maintain Detailed Enterprise Asset Inventory (Level 1 maturity)
- 1.2: Address Unauthorized Assets (Level 1 maturity)
- 2.3: Address Unauthorized Software (Level 1 maturity)
- 1.3: Utilize an Active Discovery Tool (Level 2 maturity)
- 2.5: Allowlist Authorized Software (Level 2 maturity)
- 1.4: Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory (Level 3 maturity)

Mapping to CIS Handbook Best Practices

- 23, 27, 28, 30, 45, 55, 65, 67, 68, 69, 79, 86, 88