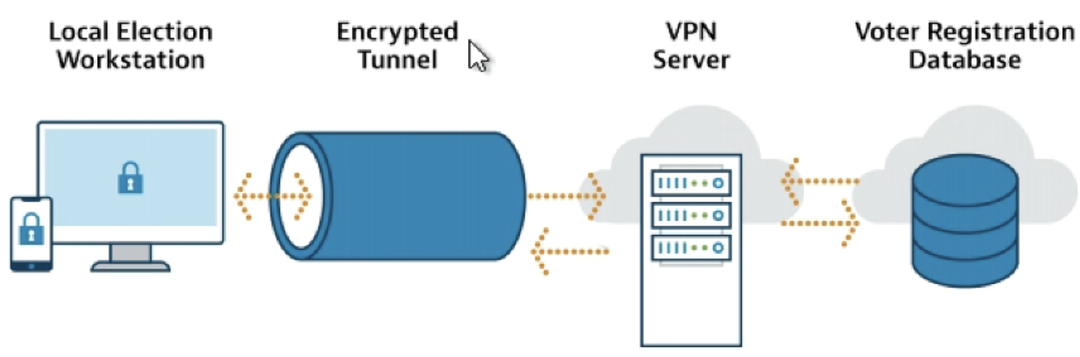
Managing Remote Connections

Remote or traveling employees often require access to enterprise data while physically outside of the workplace. This can be accomplished via a Virtual Private Network (VPN). Other common uses include securely connecting on public Wi-Fi, user anonymity, and circumventing government censorship.

VPNs encrypt and transmit data, allowing a user to securely connect to the internet or access a remote network on an untrusted connection. This ensures that all transmitted data remains confidential. Organizations need to authenticate the device or user attempting to establish a VPN connection before allowing them access. VPNs can also be used to establish secure connections between two organizations on separate networks.

Many cybersecurity firms offer ready-made hardware and software solutions to deploy a VPN. Well-resourced organizations can also develop their own solutions, such as setting up a VPN router to manage secure connections.

Employees can connect to VPNs via laptops, desktops, or even mobile devices such as smartphones and tablets. When an employee connects to a VPN, it will appear as if they are connecting to the internet from the organization's network, instead of their remote location. Below is a diagram showing how VPNs may be used in an election system.



Election offices can use a VPN to:

- Protect employee data if a remote or offsite employee must connect to an office network, or transmit sensitive data (e.g., employee or election data).
- Securely connect local election officials' workstations to a state voter registration database.
- Securely transmit information to an external partner, such as an election vendor or non-profit organization.

Goals

1. Understand VPN technology and its role in election environments (Level 1 maturity)
2. Properly implement a VPN service with your environment (Level 1 maturity)

Actions

For Managing Remote Connections, the necessary actions vary by maturity as detailed below.

Level 1 Maturity

At the Level 1 maturity, organizations should use a VPN for all remote connections. To do so:

1. Recognize situations where a VPN would be useful and appropriate.
2. Implement multi-factor authentication on all VPN connections.
3. Review CIS's Telework and Small Office Network Security Guide for tips on securing a remote work environment.
4. If a trusted third party, like a vendor, provides the VPN used to connect to your network, confirm they are following the same security principles as your organization.

Level 2 and Level 3 Maturities

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

1. Update the hardware and software used by VPNs and implement a patch management program to prevent malicious actors from exploiting known vulnerabilities. There have been reports of cyber threat actors targeting VPNs by exploiting known vulnerabilities in hardware/software systems.
    - For example, see examples of Common Vulnerabilities and Exposures (CVE) here and here, that led to this joint advisory.
2. Review CISA's Enterprise VPN Security Alert
3. Review NIST's Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security

Cost-Effective Tools

- CIS's Telework and Small Office Network Security Guide: Assists individuals and organizations in securing commodity routers, modems, and other network devices. Securing these devices is important as there are serious cybersecurity considerations surrounding the usage of network devices.

Learn More

- For more tips on working with vendors, review CIS's "A Guide for Ensuring Security in Election Technology Procurements."

Mapping to CIS Controls and Safeguards

- 3.10: Encrypt Sensitive Data in Transit (Level 1 maturity)
- 6.3: Require MFA for Externally-Exposed Applications (Level 1 maturity)
- 6.4: Require MFA for Remote Network Access (Level 1 maturity)
- 12.6: Use of Secure Network Management and Communication Protocols (Level 1 maturity)
- 12.7: Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure (Level 2 maturity)

Mapping to CIS Handbook Best Practices

- 44, 46, 83