Election Security Services

CIS and the Elections Infrastructure ISAC have worked collaboratively with election officials and their teams to provide an election-focused cyber defense suite and A Handbook for Elections Infrastructure Security to help both technical and non-technical individuals assess, plan, and execute on practical, actionable best practices to meet their goal of securing elections.

Pairing the Handbook with the Election Infrastructure Assessment Tool can help election offices increase their understanding of the controls they should implement in their environment. To help narrow the search for security implementation tools, this checklist highlights key services recommended in the handbook and available opportunities to implement them.

Key: ☆ CIS Handbook Best Practices ⓘ CIS Controls ? What it is → Where to get it

Whitelist Authorized Applications and IP Addresses

☆ 1, 17 & 61 ⓘ 2

? Application whitelisting allows only authorized software to be installed on a system. IP whitelisting allows only authorized systems to connect to a network. Whitelisting can be implemented using a combination of commercial whitelisting tools, policies or application execution tools that come with anti-virus suites and popular operating systems.

→ GSA Schedule 70 132-44 CDM Tools

Create and Keep an Asset Inventory

☆ 2, 27, 29, 68 & 88 ⓘ 1

? Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

→ CIS CyberMarket, GSA Schedule 70 132-44 CDM Tools

Architect Your Network Securely

☆ 3 & 6 ⓘ 9, 11 & 14

? Manage (track, control, and correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers and segment networks to greatly reduce an intruder's access to other parts of the network.

→ GSA Schedule 70 132-12 Maintenance of Equipment, Repair Services and/or Repair/Spare Parts, GSA Schedule 70 132-33 Perpetual Software License

Monitor Your Network

☆ 7 & 42 ⓘ 12

? Detect, prevent, and correct the flow of information transferring networks of different trust levels with a focus on security-damaging data. Network monitoring should be multi-layered, relying on firewalls, proxies, DMZ perimeter networks, and network-based intrusion detection and intrusion prevention systems (IDS and IPS). It is also critical to filter both inbound and outbound traffic.

→ EI-ISAC, GSA Schedule 70 132-44 CDM Tools

Encrypt Data and Network Connections

☆ 9, 12, 46, 83 & 84 ⓘ 13, 14 & 18

? The adoption of data encryption, both in transit and at rest, provides mitigation against data compromise. The process for generation, use, and destruction of cryptographic keys should be based on proven processes as defined in standards such as NIST SP 800-57.

→ GSA Schedule 70 132-12 Maintenance of Equipment, Repair Services and/or Repair/Spare Parts and Schedule 70 132-32 Term Software License

Maintain and Review Logs

☆ 10, 11, 38, 39 & 49 ⓘ 6

? Collect, manage, and analyze audit logs of events that could help detect, understand, and recover from an attack. Correlation tools can make audit logs far more useful in identifying subtle attacks and for subsequent manual inspection.

→ GSA Schedule 70 132-44 CDM Tools

Continued →

Train, Train, Train

☆ 13, 32 & 57 ⓘ 17

? Develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs. Periodic training for all workforce members should be measured and tested for effectiveness, updated regularly, and be specific, tailored, and focused on the specific behaviors and skills needed by the workforce.

→ EI-ISAC, CIS CyberMarket, FedVTE, GSA Schedule 70 132-50 Training Courses

Identify Vulnerable Systems and Software

☆ 19 ⓘ 3

? Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers. Use vulnerability scanning tools that measure security flaws and map them to vulnerabilities and issues categorized using an industry-recognized classification scheme or language.

→ EI-ISAC, DHS NCATS, GSA Schedule 70 132-44 CDM Tools, GSA Schedule 70 132-45A Penetration Testing, GSA Schedule 70 132-45D Risk and Vulnerability Assessment

Use Multi Factor Authentication

☆ 24 ⓘ 4 & 16

? Multi-factor authentication provides an additional layer of defense beyond a password, which may be compromised in a data breach. It typically consists of something you know (password) along with something you have (mobile phone, physical key, token) or something you are (biometrics).

→ GSA Schedule 70 132-44 CDM Tools

Protect Websites from DDoS Attacks

☆ 31

? A denial of service attack (DoS) is a cyber attack that seeks to disrupt the availability of a system or service. DDoS mitigation services typically filter potentially malicious traffic and utilize the resources of a large organization, such as a network provider, to spread the load of traffic targeting a system across multiple locations

→ Google, Cloudflare, GSA Schedule 70-132-44 CDM Tools

Protect Against Malware

☆ 40 ⓘ 8

? Anti-malware controls the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

→ GSA Schedule 70 132-44 CDM Tools

EI-ISAC™

The Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) is a voluntary and collaborative effort based on the strong partnership between the Center for Internet Security (CIS), the U.S. Department of Homeland Security, and the Election Infrastructure Subsector Government Coordinating Council (EIS-GCC). The EI-ISAC and its 24x7x365 Security Operations Center provide state and local election offices with an election-focused cyber defense suite, including sector-specific threat intelligence products, incident response and remediation, threat and vulnerability monitoring, cybersecurity awareness and training products, and tools for implementing security best practices. For more information visit http://www.cisecurity.org/ei-isac.

DHS Continuous Diagnostics and Mitigation Program (CDM)

The Continuous Diagnostics and Mitigation (CDM) Program fortifies government networks and systems with capabilities and tools. These capabilities and tools identify cybersecurity risks on an ongoing basis; prioritize these risks based on potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. Please reach out to cdm.arm@hq.dhs.gov for further information.

GSA

GSA Cooperative Purchasing Program

With GSA's Cooperative Purchasing Program, state and local governments can get what they need – for less. The Cooperative Purchasing Program provides access to thousands of nationwide, pre-vetted vendors that offer a wide array of commercial information technology (IT) and law enforcement products, services and integrated solutions. For more information visit http://www.gsa.gov/cooperativepurchasing.

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number, {2010-PD-123-000001}. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.