Center for Internet Security (CIS)

- **CIS is a community-driven nonprofit**
  - Mission is to make the connected world a safer place
  - Develops security best practices
    - CIS Critical Controls and CIS Benchmarks
  - Home to the MS-ISAC and EI-ISAC

- **The CISA, CIS, and the EI-ISAC relationship**
  - Voluntary and collaborative effort based on a strong partnership

---

**CISA** focuses on the cybersecurity of all critical infrastructure within the United States (including election offices).

**MS-ISAC** is a trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial (SLTT) government entities.

**EI-ISAC** supports the rapidly changing cybersecurity needs of U.S. SLTT election offices.

CIS is home to the MS-ISAC and the EI-ISAC.
What is the EI-ISAC?

- **Elections Infrastructure – Information Sharing and Analysis Center**
  - Created in 2018
  - Mission to improve the cybersecurity posture of SLTT election offices
  - Provides cybersecurity solutions at no cost
Who We Serve

+3,539 Members

- 50 State Election Offices
- +3,400 Local Election Offices
- 6 Territorial Election Offices
- 12 Election Associations
- 48 Supporting Members
- 2 Tribes
How to Increase Your Cybersecurity Posture
Defense-in-Depth Approach to Cybersecurity

**Community**
Share access to threat data and connect with organizations that have similar risk profiles.

**Best Practices**
Implement security best practices to protect organizations from cyber threats.

**Risk Management**
Continuous risk identification and management.

**Network**
Defend against intrusions from malicious actors.

**Device**
Protect workstations and servers against cyber-attacks.

**Data**
Protect sensitive data and intellectual property from malicious threats.

**BEST PRACTICE DEVELOPMENT**
- CIS Benchmarks Community
- CIS Critical Security Controls Community

**INFORMATION SHARING AND ANALYSIS**
- MS-ISAC Membership
- EI-ISAC Membership
- ISAC Working Groups

**SECURITY BEST PRACTICES**
- CIS Benchmarks
- CIS Critical Security Controls

**CIS SECURESUITE MEMBERSHIP**
- CIS-CAT Pro
- CIS CSAT Pro
- CIS Build Kits

**CLOUD SECURITY**
- CIS Hardened Images

**VULNERABILITY MANAGEMENT PROGRAM**
- Phishing Engagements
- Penetration Testing
- Vulnerability Scanning

**Risk Assessment Method**
- CIS RAM

**Cybersecurity Training**
- Vulnerability Disclosure Program

**ENDPOINT SECURITY SERVICES**
- Managed Endpoint Detection and Response
- NGAV
- Asset Management and Control

**CIS CyberMarket**

---

24x7x365 Security Operations Center
Threat Intelligence, Detection, and Response

---

EI-ISAC
Vulnerability Disclosure Program

Vulnerability Disclosure Program (VDP)

The Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) has created a Vulnerability Disclosure Program (VDP) that gives permission for security researchers to ethically find and report vulnerabilities in an election office's systems.

What is a VDP?

A VDP is a formalized process to receive, validate, remediate, and communicate vulnerability information identified by security researchers on specific technology systems. VDPs have proven successful in many industries, from the largest tech companies to small governments. They can be an effective and efficient way for an organization to improve its security posture.

Why Consider a VDP?

• Many election organizations simply don't have skilled cybersecurity professionals on staff.

• Formalized process to receive, validate, remediate, and communicate vulnerability information identified by security researchers on specific technology systems.

• South Carolina and Idaho are initial pilot states

Confidential & Proprietary  7

TLP: CLEAR
Albert Sensors

- Intrusion detection system
- The Albert program began in 2011. CISA has funded 200+ Albert sensors, deployed to every state in the U.S.
- More than 800 other Albert sensors have been purchased by and deployed
- The MS/EI-ISAC has the most comprehensive view of cyber threats and attacks against U.S. SLTTs.
- The rapid updating of Albert sensors to look for emerging threats, as well as activity by known threat actors, significantly increases the cyber defenses of our members
Malicious Domain Blocking and Reporting (MDBR)

Security Focused DNS service:
Blocks malicious domain requests before a connection is even established!

Simple Implementation:
No new hardware or software required

Helps limit infections related to:
- Known Malware
- Ransomware
- Phishing
- Other cyber threats
Endpoint Detection and Response (EDR)

- Program began in March 2020
- **Program has been extended**
- Partnered with CrowdStrike to deliver endpoint protection services
- EDR quickly identifies and limits the spread of malicious activity
- SOC monitors 24x7x365
- Added functionality for additional protection
Virtual Service Review

Meet with the EI-ISAC team to review your organization’s current status

Review Services

Update Contacts

New Membership Offerings

Contact us at: elections@cisecurity.org
Who Do I Contact?

- **EI-ISAC Team:**
  - elections@cisecurity.org

- **EI-ISAC Registration**
  - https://learn.cisecurity.org/ei-isac-registration
Thank You!

Headquarters
518-880-0699
elections@cisecurity.org

Marci Andino
518-516-3132
Marci.andino@cisecurity.org