Elections Infrastructure ISAC®

Are You Ready for the Next Election?

Marci Andino
Sr. Director of the EI-ISAC

July 8, 2022

Center for Internet Security (CIS)

- Community-driven non profit
  - More than 300 employees
- Responsible for CIS Controls and CIS Benchmarks
- Home to the MS-ISAC and EI-ISAC
- "*Making the connected world a safer place*"

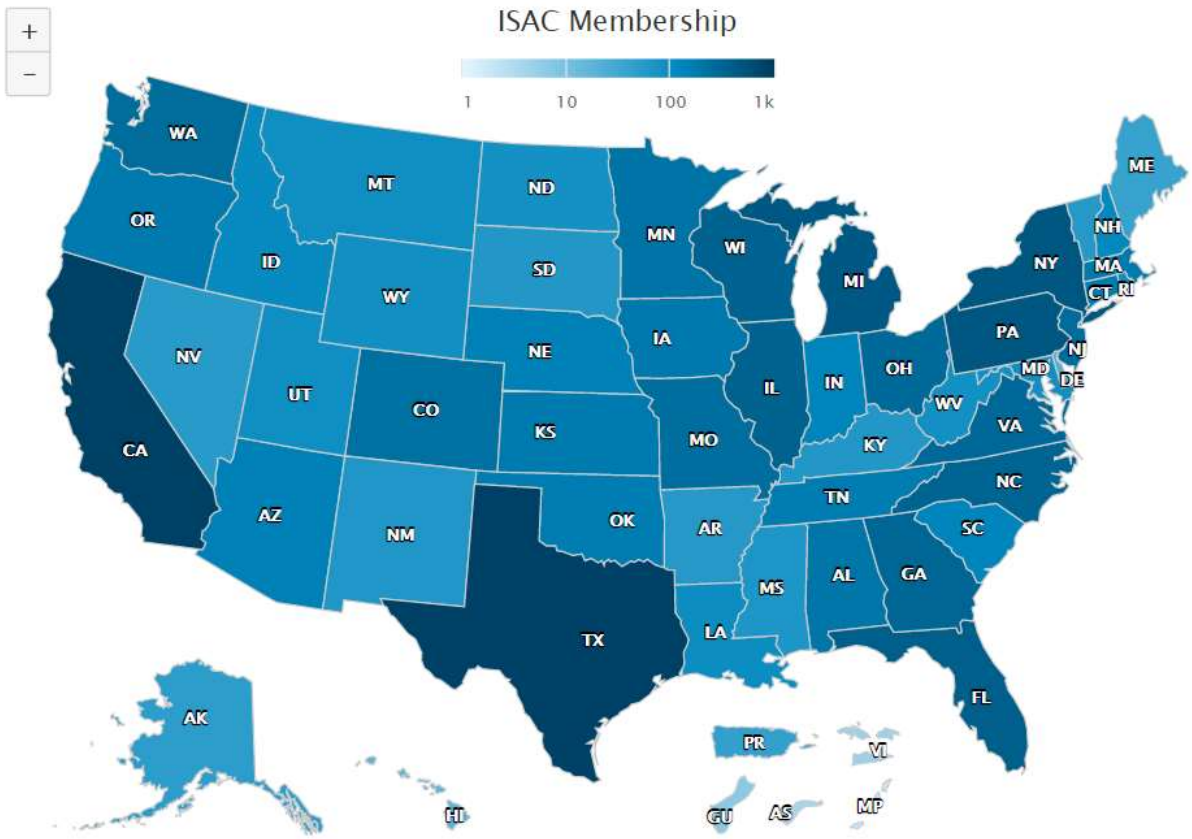
What is the EI-ISAC?

- Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
- A voluntary and collaborative effort based on a strong partnership between the Center for Internet Security (CIS) and the U.S. Department of Homeland Security (DHS)

Who We Serve

+3,387 Members

- 50 State Election Offices
- +2,950 Local Election Offices
- 5 Territorial Election Offices
- 9 Election Associations
- 42 Supporting Members
- 1 Tribe



What is the Mission of the MS-ISAC?

To improve the overall cybersecurity posture of U.S, State, Local, Tribal and Territorial (SLTT) government organizations through coordination, collaboration, cooperation and increased communication.

What is the Mission of the EI-ISAC?

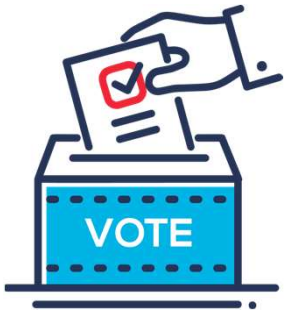
To improve the overall cybersecurity posture of SLTT election offices, through collaboration and information sharing among members, the U.S. Department of Homeland Security (DHS) and other federal partners, and private sector partners are the keys to success.

Initiatives and Resources

- Spotlight
- Alerts
- Endpoint Detection and Response (EDR)
- Malicious Domain Blocking and Reporting (MDBR)
- Security Operations Center (SOC)
- Cyber Incident Response Team (CIRT)
- Malicious Code Analysis Platform (MCAP)
- Vulnerability Disclosure Program (VDP)
- Tabletop Exercises (TTX)

Communication for Election Officials

Content that put elections security topics into context for election officials



EI-ISAC

Election Security Spotlight

TLP: White - Share widely

April 8, 2022

Purpose of Document: Educational resource for administrators.

Spotlights provide election officials with an overview of common cybersecurity topics, and how they relate to election infrastructure security.

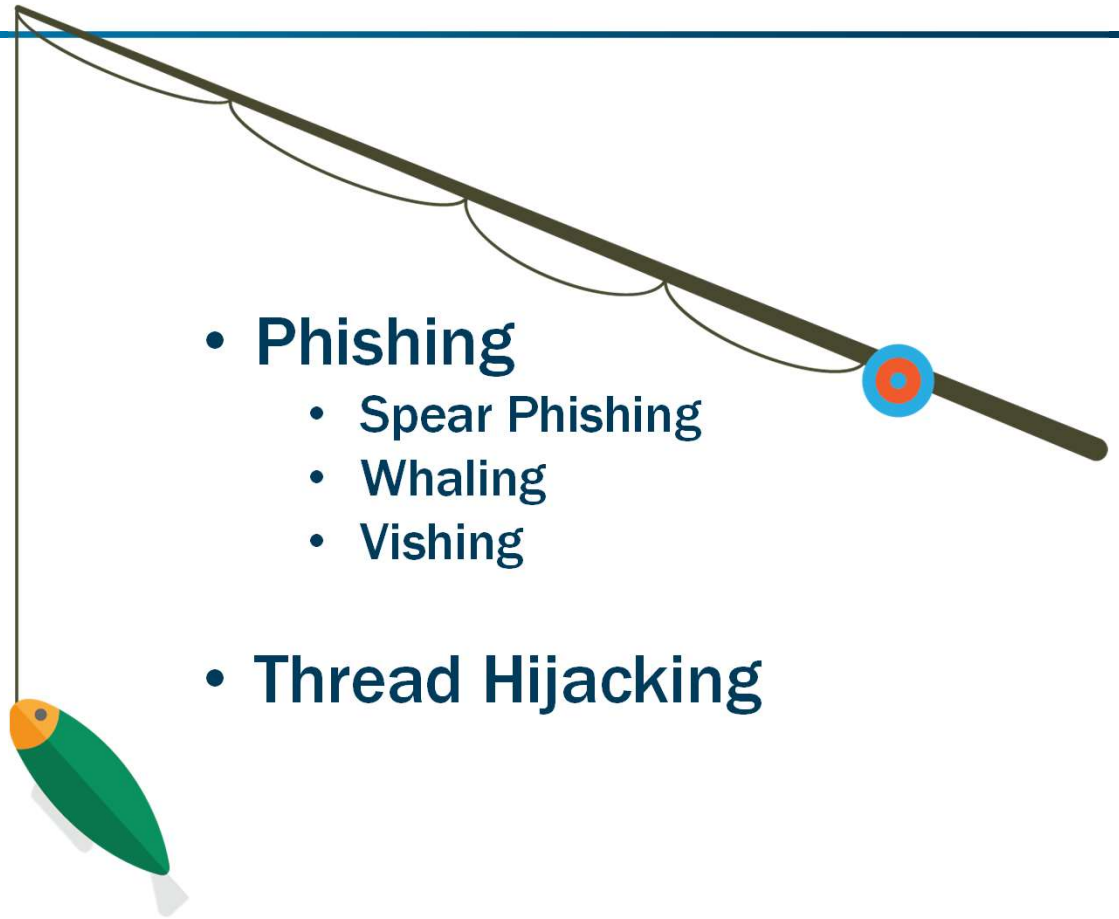
Who to Contact

Election offices at every level of government have access to a wide range of public and private security resources and organizations. Each organization can typically be contacted by telephone, email, video conference, or online chat session.

What's Out There?

Malware

- Ransomware
- Virus
- Worm
- Trojan Horse
- Spyware



Threat Highlight: Phishing

Q1 2022

- **70% of member-reported incidents were spam/phishing**
- **Initial access point to systems**
- **Common themes**
  - "Invoices"
  - "Requested documents"
  - Unusual requests for information
  - Email address doesn't match the name
- Malicious Code Analysis Platform (MCAP)
  - mcap@cisecurity.org

Threat Highlight: Thread Hijacking

Q1 2022

- **Attackers compromise an account, steal legitimate correspondence**
- **Reply to that correspondence with a malicious document/link**
- **Look for the signs!**
  - Original email dated from months ago
  - Email address doesn't match the name
  - Content completely unrelated to original thread
  - Asking you to do something

EI-ISAC

Endpoint Detection and Response (EDR)

- Partnered with CrowdStrike to deliver endpoint protection services
- EDR quickly identifies and limits the spread of malicious activity
- ***No charge*** for election offices
- SOC monitors 24x7x365
- Added functionality for additional protection

CROWDSTRIKE

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

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

Misinformation Reporting

- Single point of contact for reporting **Mis- Dis- Mal-Information** (MDM)
  - EI-ISAC will contact social media platforms and follow up with you
- **What to Include:**
  - Screenshot
  - URL (if available)
  - Official Contact Info
  - Description of why it is misinformation
- **Email:** misinformation@cisecurity.org

The Challenge Ahead: Trust

- Rampant MDM undermines confidence and trust in:
  - Election technology
  - Election officials, workers, facilities
  - Election processes
- Public misunderstanding of processes allows for MDM to grow and thrive
- Isolated errors & confusion can be used to feed destructive narratives
- #Trustedinfo2022
- .gov

Vulnerability Disclosure Program (VDP)

- VDP is a formalized process to receive, validate, remediate, and communicate vulnerability information on specific technology systems from security researchers
  - proven successful in many organizations from the largest tech companies to small governments.
  - effective and efficient way for an organization to improve its security posture.
  - allows the organization to leverage the wide-ranging talent of security researchers to improve security on its systems while giving the researcher an opportunity to practice and gain recognition for their skills

Tabletop Exercises (TTX)

- Tabletop exercises are meant to help election offices consider different risk scenarios and prepare for potential cyber threats.
- TTX's can be conducted:
  - In-person
  - Virtually
  - Online
    - Can be completed in as little as 15 minutes
- Each scenario will list the processes that are tested, threat actors that are identified, and the assets that are impacted.

Cyber STRONG

Strong Elections Are Cyber STRONG

Action Step	What We Can Promote
Stay Connected	EI-ISAC membership & engagement
Train & Communicate	Tabletop Exercises (TTX); EI-ISAC training/threat briefings; SANS; Communicate basic cyber hygiene steps (like strong passwords, email discipline, etc.)
Ready Your Network & Devices	Lock down your network and devices; MDBR, EDR (Albert – not always no-cost)
Own Your Environment	Combat Mis-/Dis-information; Take responsibility for cybersecurity
Nurture Your Cyber Strength	Essential Guide; NCSR; Controls/Benchmarks
Go Tell Your Story	Raise public confidence that you are “Cyber Strong”; email signatures; signing events; press releases

Protecting Against Potential Russian Cyber-Attacks

Protecting Against Potential Russian Cyber-Attacks

Guidance for Election Officials

- Join the EI-ISAC and/or MS-ISAC
- Join online at www.cisecurity.org
- No charge to join

Protecting Against Potential Russian Cyber-Attacks

Guidance for Election Officials

- Stop malicious internet activity with Malicious Domain Blocking and Reporting (MDBR)
- MDBR is provided at ***no charge*** to election offices
- Prevents users from connecting to known or suspected malicious sites
- Takes about 15 minutes to redirect domain name system resolution
- No other configuration or maintenance required

Protecting Against Potential Russian Cyber-Attacks

Guidance for Election Officials

- Turn on multi-factor authentication (MFA) for any system that offers it.
- MFA is a feature that comes with many systems.
- Level of effort: as little as 10 minutes.

Protecting Against Potential Russian Cyber-Attacks

Guidance for Election Officials

- Make sure you have a recent vulnerability scan of externally facing IT assets.
- Install all possible patches and updates.
- Level of effort: minimal.

Protecting Against Potential Russian Cyber-Attacks

Guidance for Election Officials

- Enable logging on any device that is capable
- Configure a log collection system
- Helps put the puzzle together:
  - Who the adversary was
  - How they got in
  - How long were they in the system
  - What did they do while in the system

Protecting Against Potential Russian Cyber-Attacks

Guidance for Election Officials

- Develop or update an incident response (IR) plan.
- Ensure systems are properly backed up and backups are protected from ransomware attacks.
  - Endpoint security

Annual Meeting

- August 7-10
- Baltimore, Maryland

Who Do I Contact?

- **EI-ISAC Team:**
  - elections@cisecurity.org
- **EI-ISAC Registration**
  - https://learn.cisecurity.org/ei-isac-registration
- **Mis-Dis- Information**
  - misinformation@cisecurity.org
- **Marci Andino**
  - Marci.Andino@cisecurity.org

Elections Infrastructure ISAC

Thank You!

elections@cisecurity.org

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