ELECTION SECURITY OVERVIEW

JANUARY 5, 2022
As the nation’s risk advisor, the Cybersecurity and Infrastructure Security Agency’s (CISA) mission is to ensure the security and resiliency of our critical infrastructure.

The 2017 designation of election infrastructure as critical infrastructure provides a basis for the Department of Homeland Security (DHS) and other federal agencies to:

- Recognize the importance of these systems;
- Prioritize services and support to enhancing security for election infrastructure;
- Provide the elections community with the opportunity to work with each other, the Federal Government, and through the Coordinating Councils; and
- Hold anyone who attacks these systems responsible for violating international norms.
All 50 states and over 3,000 local jurisdictions and private sector organizations are members of the EI-ISAC

219 stakeholders currently hold security clearances through the election infrastructure clearance program

Between October 2020 and September 2021, CISA provided over 500 Vulnerability Scanning services and Cyber Assessments

Albert Sensors are deployed in all 50 states

Hosted four national tabletop exercises for EI stakeholders and more than 50 exercises for state and local election officials and other stakeholders

Between October 2020 and September 2021, CISA delivered tailored security products for 1,860 election administrators
Threat Landscape

Intelligence Community Assessment on Foreign Threats to 2020 Elections

- “We have no indications that any foreign actor attempted to alter any technical aspect of the voting process in the 2020 U.S. elections, including voter registration, casting ballots, vote tabulation, or reporting results. […] Some foreign actors, such as Iran and Russia, spread false or inflated claims about alleged compromises of voting systems to undermine public confidence in election processes and results.”

DHS-CISA-DOJ-FBI Report on Impact of Foreign Interference Targeting Election Infrastructure in 2020

- “We […] have no evidence that any foreign government-affiliated actor prevented voting, changed votes, or disrupted the ability to tally votes or to transmit election results in a timely manner; altered any technical aspect of the voting process; or otherwise compromised the integrity of voter registration information of any ballots cast during 2020 federal elections.”
- “Broad Russian and Iranian campaigns targeting multiple critical infrastructure sectors did compromise the security of several networks that managed some election functions, but they did not materially affect the integrity of voter data, the ability to vote, the tabulation of votes, or the timely transmission of election results.”
EI-ISAC

Election Infrastructure Information Sharing and Analysis Center
- Voluntary collaborative effort between CISA, the Center for Internet Security (CIS), and the Election Infrastructure Subsector Government Coordinating Council (EIS GCC)
- No cost to election officials
- Suite of elections-focused cyber defense tools, threat intelligence products, and incident response and forensics, training products, and more

EI-ISAC Services
- Albert Sensors
- Malicious Domain Blocking and Reporting
- Threat Alerts
- & more

Visit https://learn.cisecurity.org/ei-isac-registration for more information
Responsibility of administering official web domains shifted to CISA from GSA

Under CISA, .gov domains are available at no cost for qualifying organizations

Increased use of .gov domains will improve cybersecurity and trust in public services across the United States

Visit https://home.dotgov.gov/about/elections/ for more information
Election Infrastructure Subsector Recommendations*

CISA recommends the following mitigations to reduce EI entity cyber risk

 ✓ Improve phishing defenses

 ✓ Patch vulnerabilities on internet-accessible systems and devices on a regular schedule. CISA recommends regularly scanning internet-accessible hosts and remediating critical and high vulnerabilities within 15 and 30 days, respectively.

 ✓ Update software and OS to supported versions

 ✓ Securely configure internet-accessible ports and services on systems and devices

*CISA Election Infrastructure Subsector Cyber Risk Summary, March 2021
Cybersecurity Services

CISA Services

- Vulnerability Scanning
- Remote Penetration Testing
- Phishing Campaign Assessment
- Critical Product Evaluation
- Web Application Scanning
- Crossfeed
- Cyber Resilience Review
- Exercises and Training
- & more

For more information on these services, visit www.cisa.gov/election-security
Incident Response

What is an incident?

The CISA Cybersecurity Division (CSD) Threat Hunting team defines an individual incident as a distinct, potentially malicious event, perpetrated by a single threat actor, using a single tactic, technique, or procedure (TTP); or series of related TTPs, against a single victim.

Contact CISA
Report cybersecurity incidents and vulnerabilities:

📞 888-282-0870
✉️ Central@cisa.gov

Threat Hunting Services
Provides incident response, management and coordination activities for cyber incidents occurring in the critical infrastructure sectors as well as government entities at the Federal, State, Local, Tribal, and Territorial levels.
Incident Response

CISA has identified incident response and reporting as a capability gap among state and local election authorities.

CISA also recognizes that polling places, election offices, and storage facilities are vulnerable to a variety of threats.

Incident Response Guide

- Voluntary tool to help jurisdictions effectively recognize and respond to potential cyber incidents
- Useful as a basic cyber incident response plan or integrate it into a broader plan based on specific needs

Election Day Emergency Response Guide

- Provides local election personnel with a simple tool for determining what steps to take when an incident occurs and where to report incidents
- CISA works with states to determine most appropriate response steps and contacts
**Physical Security**

**CISA resources available to election officials**

- Protective Security Advisors
- Physical Security Assessments
- Physical Security at Voting Locations and Election Facilities Guide

**DOJ Taskforce to Address Threats against Election Personnel**

- DOJ, DHS, FBI, and others are working together in recognition of increasing threats against election workers/administrators/officials

- Report threats to the FBI Election Crime Coordinators. You can also report threats and violent acts against election officials to the FBI at 1-CALL-FBI (225-5324), prompt 1, then prompt 3

**REPORT THREATS**

**DOJ**

- Report immediate threats to (9-1-1)

**CISA**

- Report threats to the FBI Election Crime Coordinators.
- You can also report threats and violent acts against election officials to the FBI at 1-CALL-FBI (225-5324), prompt 1, then prompt 3.
Exercises and Training

CISA Tabletop and other Exercises
- CISA led: Virtual or in-person
- Self-led: “Tabletop in a Box”

ESI Training Offerings
- Elections Security Overview
- Ransomware
- Phishing
- Building Trust through Secure Practices

Federal Virtual Training Environment (FedVTE)
You can sign-up for CISA trainings or an exercise by emailing electionsecurity@hq.dhs.gov

For more information on these services, visit www.cisa.gov/election-security
What Election Infrastructure Stakeholders Can Do

Connect with your CISA Cybersecurity and Protective Security Advisor (CSA/PSA)

Sign up for CISA Services/Check out our Products
- Vulnerability Scanning (CyHy)
- .gov Top-Level Domain (.gov TLD)
- Physical Security Assessment
- Cyber Incident Response Plan
- Mis-, dis-, and malinformation resources

Request CISA trainings and exercises

Join the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)

Most importantly – tell us what you need