1

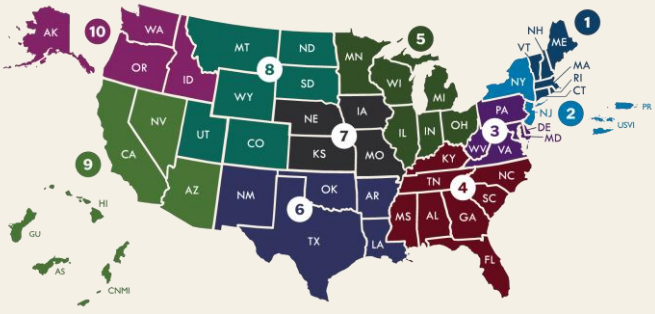
Critical Infrastructure Sectors

CHEMICAL	CISA	FINANCIAL	Treasury
COMMERCIAL FACILITIES	CISA	FOOD & AGRICULTURE	USDA & HHS
COMMUNICATIONS	CISA	GOVERNMENT FACILITIES	GSA & FPS
CRITICAL MANUFACTURING	CISA	ELECTION INFRASTRUCTURE	
DAMS	CISA	HEALTHCARE & PUBLIC HEALTH	HHS
DEFENSE INDUSTRIAL BASE	DOD	INFORMATION TECHNOLOGY	CISA
EMERGENCY SERVICES	CISA	NUCLEAR REACTORS, MATERIALS AND WASTE	CISA
ENERGY	DOE	TRANSPORTATIONS SYSTEMS	TSA & USCG
WATER	EPA	PIPELINE SYSTEMS	

2

CISA & Election Infrastructure

CISA's Regional Field Staff



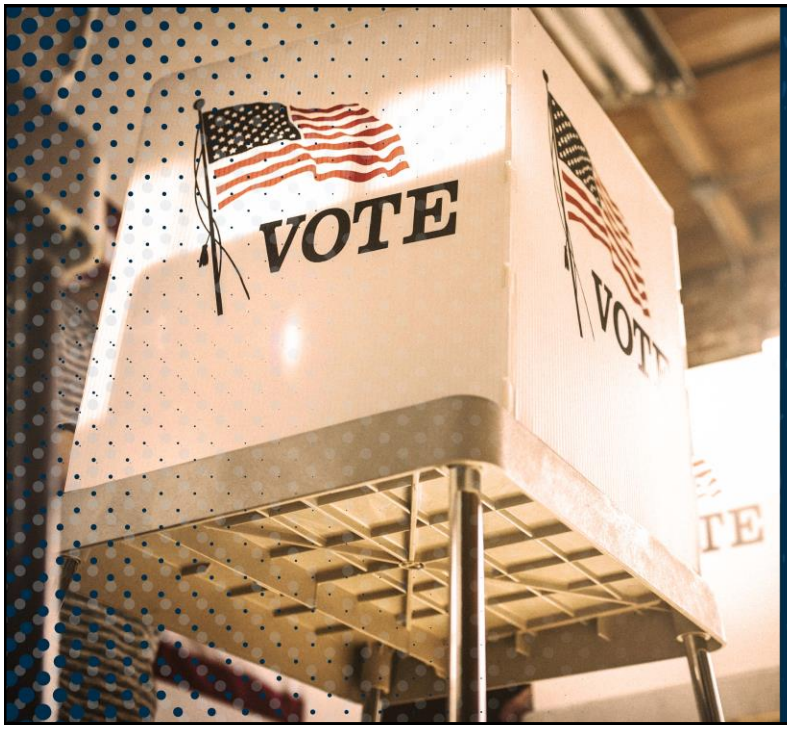
The Cybersecurity and Infrastructure Security Agency's (CISA) mission is to help secure our nation's critical infrastructure.

In January 2017, the Department of Homeland Security (DHS) designated election infrastructure as critical infrastructure.

Through our CISA field staff across the country and our security experts at CISA headquarters, CISA offers a range of voluntary, free services and support to stakeholders to help ensure the security and resiliency of election infrastructure.

CISA's Regional Election Security Advisors help ensure maximum support to the election community through tailored support to meet unique state and local needs.

3



OUR MISSION

Help election officials and election infrastructure stakeholders protect against the cyber, physical, and operational security risks to election infrastructure during the 2024 election cycle.

4

2024 ODNI Annual Threat Assessment

Foreign Actors Likely to Target the 2024 Elections

PEOPLE'S REPUBLIC OF CHINA

"The PRC may attempt to influence the U.S. elections in 2024 at some level because of its desire to sideline critics of China and magnify U.S. societal divisions."

IRAN

"Ahead of the U.S. election in 2024, Iran may attempt to conduct influence operations aimed at U.S. interests, including targeting U.S. elections, having demonstrated a willingness and capability to do so in the past."

RUSSIA

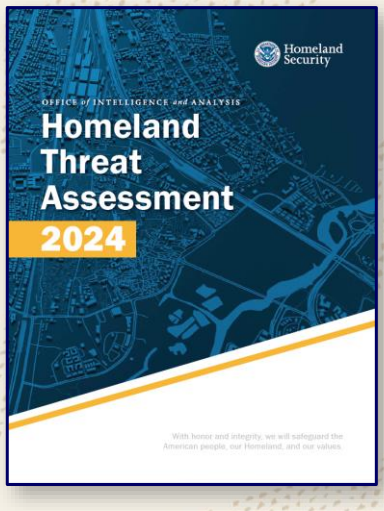
"Moscow views U.S. elections as opportunities and has conducted influence operations for decades and as recently as the U.S. midterm elections in 2022."

5

2024 DHS Homeland Threat Assessment

Threat Actors Likely to Converge on 2024 Elections

- "We expect the 2024 election cycle will be a key event for possible violence and influence targeting election infrastructure, processes, and personnel."
- "Our electoral processes remain an attractive target for many adversaries, and we expect many of them will seek to influence or interfere with the 2024 election."
- "Some DVEs may attempt to disrupt civic and democratic processes, mobilized by their perceptions of the upcoming election cycle."



6

6

Risks to Election Infrastructure

PHYSICAL

- Violence and Harassment
- Swatting
- Hazardous Materials
- Distributed through the Mail
- Insider Threats
- Bomb Threats

CYBER

- Doxing
- Ransomware
- Hack and Leak
- DDoS

OPERATIONAL

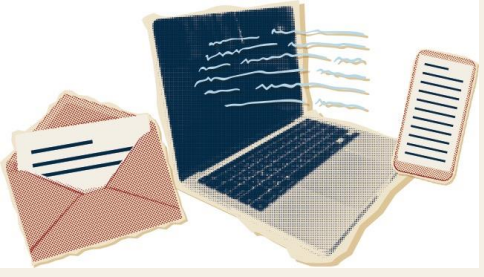
- High Turnover in Staff
- Foreign Influence Operations
- Environmental Disruptions

7

#PROTECT2024: First Things First

Simple steps election officials can still take to enhance their organization's security baseline for the 2024 election cycle:

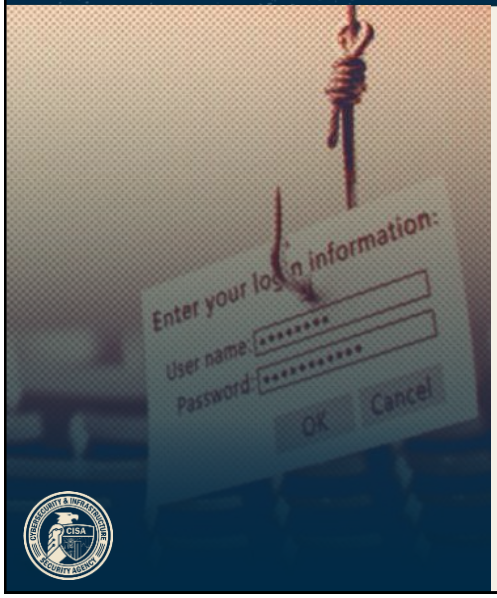
1. Enable Multi-Factor Authentication (MFA)
2. Know and manage your cyber vulnerabilities—Sign up for FREE Cyber Hygiene Services from CISA
3. Request a CISA physical security assessment
4. Transition to a .gov domain
5. Rehearse your incident response plan
6. Join the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)



8

9

Protect Your Email



THREATS TO EMAIL AND HOW TO PROTECT AGAINST THEM

PHISHING

Mitigate phishing risks by:

- Using MFA
- Contacting EI-ISAC to implement endpoint security services (ESS) and malicious domain blocking and reporting (MDBR)
- Switching to a .gov domain
- Using CISA phishing mitigation guides and resources:
  - Phishing Guidance: Stopping the Attack Cycle at Phase One
  - Phishing Postcard

10

Protect Your Website

THREATS TO WEBSITE AND HOW TO PROTECT AGAINST THEM

DENIAL-OF-SERVICE (DOS) AND DISTRIBUTED DENIAL-OF-SERVICE (DDOS)

Mitigate DoS and DDoS risks by:

- Referencing CISA's "No Downtime in Elections: A Guide to Mitigating Risks of Denial-of-Service"
- Contacting CISA to receive free web application scanning
- Check out free DDoS protection services offered by CISA's private sector partners

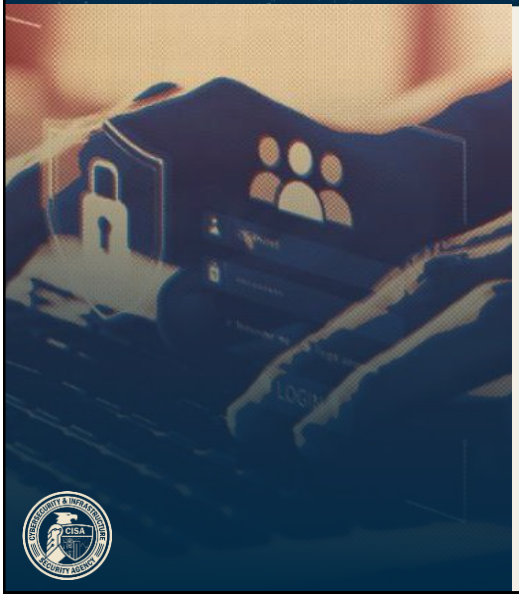
WEBSITE SPOOFING

Mitigate website spoofing risks by:

- Switching to a .gov domain

11

Protect Your Network



THREATS TO NETWORKS AND HOW TO PROTECT AGAINST THEM

RANSOMWARE

Mitigate ransomware risks by:

- Signing up for free CISA Cyber Hygiene Vulnerability Scanning
- Implementing ESS
- Leveraging Stop Ransomware Resources
- Deploying an Albert Intrusion Detection System

BUSINESS EMAIL COMPROMISE

Protect against business email compromise by:

- Enabling MFA
- Implementing ESS
- Implementing MDBR

EXPLOITING KNOWN NETWORK VULNERABILITIES

Mitigate the exploitation of known network vulnerabilities by:

- Using CISA's Known Exploited Vulnerabilities (KEV) Catalog
- Signing up for CISA's free Cyber Hygiene Vulnerability Scanning
- Implementing ESS
- Deploying an Albert Intrusion Detection System

12

Protect Your Election Systems

THREATS TO ELECTION SYSTEMS AND HOW TO PROTECT AGAINST THEM

INSIDER THREATS

Mitigate risks of insider threats by:

- Implementing steps outlined in CISA's "Election Infrastructure Insider Threat Mitigation Guide"
- Using the CISA Insider Threat training video, "Understanding the Insider Threat", to inform and prepare your staff

PHYSICAL COMPROMISE

Mitigate risks of physical compromise by:

- Referencing "CISA Insights: Chain of Custody and Critical Infrastructure Systems"

CYBER THREATS

Mitigate risks of cyber threats by:

- Referencing CISA's "Best Practices for Securing Election Systems"
- Implementing ESS

13

Protect Your Office

THREATS TO OFFICE AND HOW TO PROTECT AGAINST THEM

Mailing of hazardous materials to election offices

- **Address the risk against mailing of hazardous materials by:**
  - Referencing CISA's "Election Mail Handling Procedures to Protect against Hazardous Materials" to identify and safely handle suspicious mail
  - Using resources provided by the U.S. Postal Inspection Service (USPIS) for handling suspicious mail

Physical acts of violence against election offices and personnel

- **Mitigate against physical acts of violence by:**
  - Providing "Non-confrontational Techniques for Election Workers Training" for your staff and poll workers
  - Reaching out to CISA to request a Security Assessment at First Entry (SAFE) for your election office and supporting facilities
  - Requesting specific virtual or in-person Election Security Trainings offered by CISA
  - Referencing CISA's "Physical Security of Voting Locations and Election Facilities" guidance
  - Referencing CISA's "Personal Security Considerations for Critical Infrastructure Workers" guidance

14

Election - Ballot Drop Box Emplacement

Where should ballot drop boxes be located?

Ballot drop boxes should be placed in convenient, accessible locations, including places close to public transportation routes, near or on college campuses, and public buildings, such as libraries and community centers familiar to voters and easy to find. If there is time, getting input from citizens and community groups is recommended.

All drop box locations should be evaluated for:
- ❑ Security
- ❑ Lighting (well-lit 24 hours a day)
- ❑ High visibility
- ❑ Security cameras (more on cameras in the *Security Considerations* section below)
- ❑ Accessibility
- ❑ Voter convenience
- ❑ Parking or drive-through options

15

Election Drop Box Security

Ballot drop boxes similar to the one shown here near the JCPenny store in Sequim are now in place in Sekiu, Neah Bay and Clallam Bay, with another scheduled to open this week near Carlsborg. (Keith Thorpe/Peninsula Daily News)

UNSTAFFED - 24 HOUR DROP BOX

In high-demand areas where votes are or will be cast primarily by mail, installing a permanent ballot drop box—one that can be accessed by voters 24/7—is a good solution. These boxes should be constructed of durable material such as steel and be permanently cemented into the ground.
In addition to purchasing and installing the drop box, you should consider installing:

- ❑ Video surveillance camera
- ❑ Media storage device (for recorded video)
- ❑ Decal (branding and information)
- ❑ Extra keys for opening slot and access door
- ❑ Security seals

16

Additional Drop Box Security Considerations

This ballot drop box in Pierce County is an example of one of the quarter-inch thick steel ballot drop boxes that local elections officials commissioned and designed with security in mind. (Melissa Santos/Crosscut)

Ballot drop boxes must be secured and locked at all times. Only an election official or a designated ballot drop box collection team should have access to the keys and/or combination of the lock. In addition to locks, all drop boxes should be sealed with one or more tamper evident seals.

Ideally, unstaffed 24-hour drop boxes should be located in areas with good lighting and be monitored by video surveillance cameras. When this is not feasible, positioning the box close to a nearby camera is a good option. Also consider placing it in a high traffic area and inviting local law enforcement to make regular observations.

Try to place indoor drop boxes in locations where they can be monitored by a live person. When ballot boxes are unstaffed and not being monitored, the box should be securely fastened to a stationary surface or immovable object in a way that prevents moving or tampering.

17

Drop Box Pick-Up Considerations

Equipment and supplies needed for ballot drop boxes pick-up

Whether you are collecting ballots just from a USPS facility, ballot drop boxes, or both, you will need ballot drop box collection teams. Ideally, these are bipartisan teams (poll workers or temporary workers) hired to drive a collection route and pick up ballots on a regular basis.

Ideally, it would be best if the team were comprised of three personnel, two to collect and one to maintains visual surveillance for security.

Each of these teams will need:
❏ Vehicle such as a van or SUV where the seats can be laid flat (county owned or rented)
❏ Radio or cell phone
❏ Secure ballot collection bag/box
❏ Security seals
❏ Chain of custody procedures/forms
❏ Personal protective equipment (e.g. disposable, sterile gloves), as appropriate and in accordance to current CDC guidance

18

Protect Yourself & Your Staff

THREATS TO YOU AND YOUR STAFF AND HOW TO PROTECT AGAINST THEM

DOXING

- Protect against doxing by:
  - Referencing "CISA Insights on Mitigating the Impacts of Doxing on Critical Infrastructure"
  - Implementing the "Personal Security Considerations Action Guide for Critical Infrastructure Workers"

FOREIGN INFLUENCE OPERATIONS

Mitigate against foreign influence operations by implementing measures recommended in:

- CISA's Insights on Generative AI-Enabled Threats Guide
- CISA's Deepfake Threat Contextualization Guide

19

#PROTECT2024: CISA Service Support

Best Practice Security Guidance to Mitigate Physical, Cyber and Operational Threats to Election Infrastructure

- Current and upcoming products that address emerging threats
- Current and upcoming products that provide actionable solutions for local jurisdictions

CISA Cybersecurity Services

- Cyber Hygiene Services
- Dot.gov Transition
- In-Person and virtual Cyber Security Assessments

Partner Services Funded by CISA

- EI-ISAC Services: ESS, MDBR, Albert Sensors

Physical Security Assessments

Incident Response Management Assistance

20

#PROTECT2024: CISA Training Support

- **Ready to Use Training Videos on Our Website**
- **In Person or Virtual Training Offerings**
  - Generative Artificial Intelligence
  - Securing Local Election Offices
  - Ransomware
  - Building Trust through Secure Practices
  - Non-Confrontational Techniques
  - Insider Threats
  - Phishing
- **Tabletop Exercises**
  - In-person state and local
  - Annual National Tabletop the Vote
  - TTX in a Box (Ready to Use TTX Guides for 3 Different Election Scenarios updated for the 2024 threat environment)

21

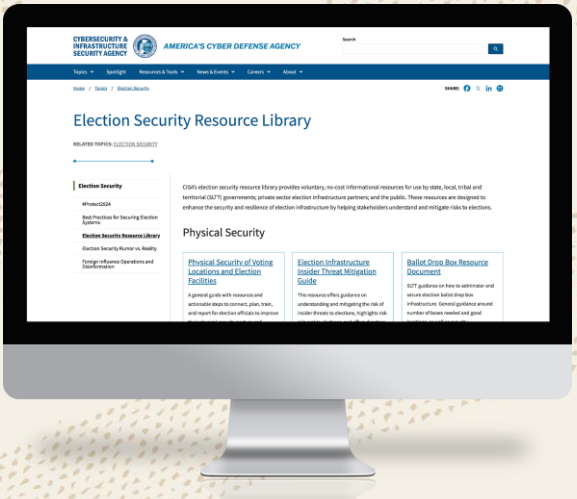
21

#Protect2024 Election Security Resource Library

One stop shop for CISA's free election security informational resources.

Resource topics include:

- Physical Security
- Cybersecurity
- Operational Risk
- Foreign Influence Operations and Disinformation
- Election Infrastructure Subsector
- Joint Releases with Federal Partners
- Election Security Services



CISA.GOV/TOPICS/ELECTION-SECURITY/ELECTION-SECURITY-RESOURCE-LIBRARY

22

Reporting

What is an incident?

A violation or imminent threat of violation of security policies, acceptable use policies, or standard security practices. Examples of incidents include:

- Attempts to gain unauthorized access to a facility, system or system data
- Unwanted disruption or denial of service
- Abuse or misuse of a system or data in violation of policy
- Physical disruptions to critical infrastructure operations

Contact CISA

Report incidents to:

- **888-282-0870**
- **Central@cisa.dhs.gov**
- **https://www.cisa.gov/report**

CISA Incident Management Assistance

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

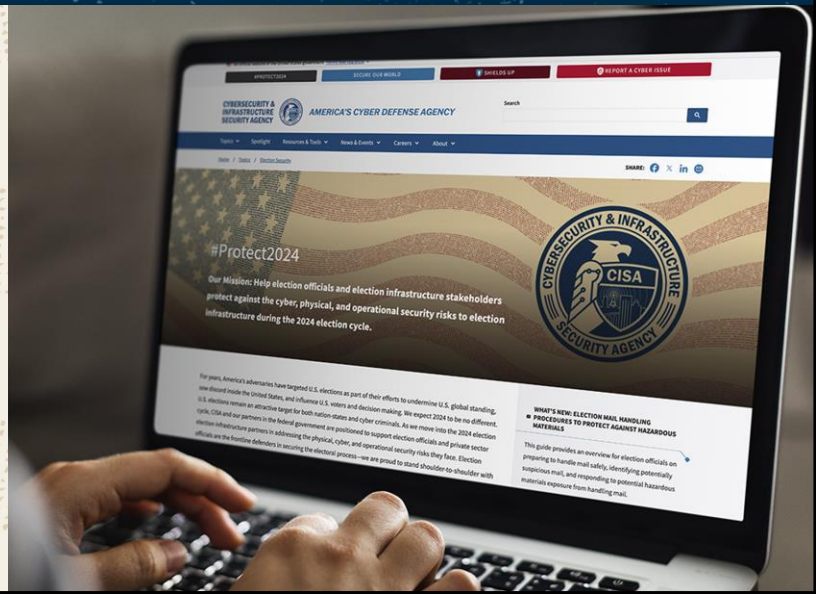
23

23

#Protect2024 Website

Specifically tailored to election officials to help them take full advantage of CISA's services and resources

CISA.GOV/PROTECT2024



24

Questions?

Noe Isaac Cavazos
Protective Security Advisor (WA)
Noe.Cavazos@cisa.dhs.gov

Jana Spring
Protective Security Advisor (WA)
Jana.Spring@hq.dhs.gov

Paul "Bo" Stocklin
Protective Security Advisor (WA)
Paul.Stocklin@cisa.dhs.gov

Lori Augino
Elections Security Advisor
Region 10
Lori.Augino@cisa.dhs.gov

Contact FBI or CISA:
https://www.ic3.gov
Central@cisa.dhs.gov

25

25

26