

CISA Elections Security 101



Overview

- CISA & Election Infrastructure Overview
- Threat Landscape
- CISA Services Overview
- 2023-24 Roadmap
- CISA Election Security Resources



CISA & Election Infrastructure

The Cybersecurity and Infrastructure Security Agency's (CISA) mission is to promote the **security and resilience** of our critical infrastructure.

In January 2017, the Department of Homeland Security (DHS) designated election infrastructure as critical infrastructure. Among other things, this designation:

- Recognizes the importance of these systems;
- Helps to prioritize services for and support to the election infrastructure community;
- Organizes DHS/CISA's:
 - Responses to incidents involving election systems and assets;
 - Composition of coordinating councils



Election Security Mission

CISA works to provide election stakeholders with the information they need to manage risk to their systems and assets.



Jen Easterly,
CISA Director

First Principles



Voluntary Partnerships

- Elections are run by state and local officials, CISA stands in support through **voluntary partnerships**.



Security Focus

- CISA focuses on the **security of systems and infrastructure**, not election administration and not voter engagement. Decisions on how to administer elections are state and local policies.



Non-Partisan

- Elections include partisan individuals and partisan organizations. CISA will engage in a **non-partisan and equitable** manner, focused on security and resilience of systems and assets.



CISA & Election Infrastructure



Note: diagram is not a comprehensive listing of all CISA divisions, offices, subcomponents, and functions; it is a summary of those which Election Infrastructure partners interact with most directly.

CISA & Election Infrastructure

Election Security & Resilience

- Program Management Office & Integration
- Engagement, Assistance, and Training
- Subsector Risk Management Agency
- Foreign Influence & Disinformation

CISA Regional Offices

- Cybersecurity Advisors & Cybersecurity State Coordinators
- Protective Security Advisors
- Election Security Advisors
- Training & Exercise Coordinators
- External Affairs Officers



Federal Partners



Partnership Model

All **50 states** and over **3,500 local jurisdictions and private sector organizations** are members of the EI-ISAC

DHS has granted a total of **233 security clearances** through the election infrastructure clearance program

Between October 2021 and September 2022, CISA provided over **500 Vulnerability Scanning services and Cyber Assessments**

Albert Sensors are deployed in all **50 states**

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

Last Mile products are in use by **6,102 election administrators in 35 states**



Threat Landscape



Potential Adversaries

- Nation-State Actors
- Black Hat Hackers
- Criminals
- Politically Motivated Groups
- Insider Threats
- Terrorists
- Domestic Violent Extremists



Possible Motivations

- Undermine Trust in Democracy and/or Election Results
- Foreign Policy Goals
- Sow Social Division
- Financial Gain
- Fame and Reputation
- Foment Chaos/Anarchy
- Retribution for Perceived Grievances



Potential Targets

- Voter Registration Databases
- Voting Systems
- Election Reporting Systems
- Public Information Websites
- Ballot Processing and Storage Facilities
- Polling Places
- Election Offices
- People: Election Officials, Vendors, etc.



Evolution of the Election Threat Landscape

2016 Election Cycle

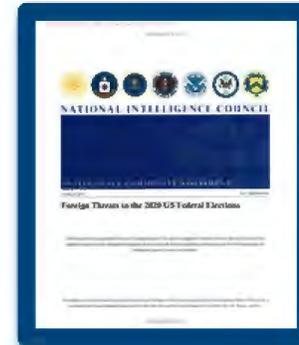
- **Russian** advanced persistent Threat (APT) cyber and influence activity

2020 Election Cycle

- **Russian** APT cyber and influence activity
- **Iranian** APT cyber and influence activity
 - Enemies of the People
- **Ransomware**
- **Physical Threats to Election Facilities and Personnel**

2022 Election Cycle

- **APT and Other Cyber Threat Activity**
 - Nation State Scanning
 - DDOS Attacks
- **Ransomware**
- **Physical Threats to Election Facilities and Personnel Supply Chain**



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 [...] 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.”



2022 Heightened Threat Environment

FBI report on Likely Threats to Election Workers

- Released **April 2022**
- “Expected increase in reports of threats to election workers as the 2022 elections approach.”

DHS National Terrorism Advisory System (NTAS) Bulletin

- NTAS Bulletin Updated in **June 2022**
- “As the U.S. enters mid-term election season...we assess that calls for violence by [DVEs] directed at...election events, and election workers will likely increase”

FBI report on Likely, More Prevalent Threats to Election Workers in Close Contests

- Released **August 2022**
- “The majority of...threats are likely to occur in states or counties where recounts, audits, or public election disputes occur during the 2022 U.S. Midterm Elections”

DHS/FBI/NCTC/USCP Report on Heightened DVE Threat Environment during 2022 U.S. Midterm Election Cycle (FOUO)

- Released **October 2022**
- “...Election-related perceptions of fraud and DVE reactions to divisive topics will likely drive DVE plotting of violence...[before and after] the 2022 midterm election(s)”



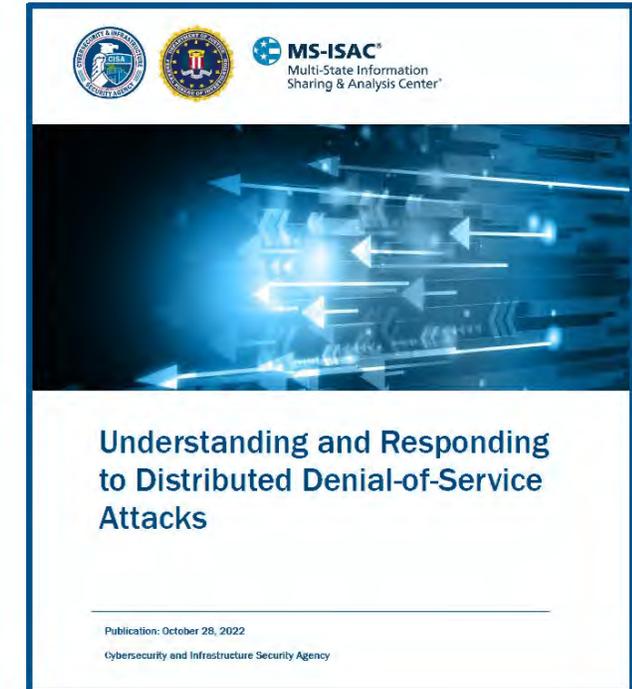
2022 Recap: Highlighted Activity

Nation-State Threat Actor Scanning Activity

- State/local government & national/state partisan websites.
- CISA-FBI Alert (TLP AMBER), shared Oct. 21 via EI-ISAC.
- **Mitigation:** importance of identifying & remediating vulnerabilities
 - Identify vulnerabilities via no-cost CISA Vulnerability Scanning
 - Remediate, prioritizing Known Exploited Vulnerabilities (KEVs), [CISA KEVs Catalog](#).

DDoS Attacks & Website Outages

- Multiple state/local government websites faced DDoS or suspected DDoS attacks before & on E-day.
- [CISA-FBI-MS-ISAC Guide](#) on DDoS attacks, released Oct. 28; related alerts.
- **Mitigation:**
 - No-cost DDoS mitigation resources, [JCDC Election Cybersecurity Toolkit](#).





CISA-Coordinated Services in Support of Election Infrastructure Security

SCALABLE SERVICES



Centrally provided by CISA to continuously detect vulnerabilities and weaknesses. Generally, require low-resource action by participants to fix identified issues, such as applying a patch.

VULNERABILITY SCANNING

• Description: Provides enrollees with a recurring report on vulnerabilities and other exploitable conditions visible from the Internet, prioritizing those that are known to be exploited by adversaries.

CROSSFEED

• Description: Collects data from open-source tools, publicly-available resources, and data feeds to provide participants with their risk posture and exposure from an attacker's perspective.

.GOV

• Description: Offers a managed top-level domain, easily identifiable as a government organization to protect against hijacking and impersonation.

WEB APP SCANNING

• Description: Provides enrollees with recurring updates on vulnerabilities in web applications.

CYBERSECURITY TOOLKIT TO PROTECT ELECTIONS

• Description: This toolkit includes free tools, services, and resources provided by CISA, JCDC members, and others across the cybersecurity community and is available to state and local government officials, election officials, and vendors.

PRIORITY TELECOMMUNICATION SERVICES

• Description: Provides subscribers with end-to-end communications priority via three services: Government Emergency Telecommunications Service (GETS), Wireless Priority Service (WPS), and Telecommunications Service Priority (TSP).

ELECTIONS ISAC SERVICES



Funded by CISA and delivered by the ISAC to actively detect and prevent threats. Often addresses risks without further action by the participant or requires participant to further investigate.

EI-ISAC MEMBERSHIP

• Description: Provides timely reporting of cyber threats facing the Election Infrastructure subsector.

MALICIOUS DOMAIN BLOCKING AND REPORTING (MDRR)

• Description: Blocks attempts to communicate with malicious infrastructure.

ALBERT

• Description: Enables detection of malicious traffic targeting SLTT networks.

ENDPOINT DETECTION AND RESPONSE (EDR)

• Description: Identifies and blocks threats targeting computers and servers.

EDUCATION AND AMPLIFICATION



Provided by CISA to educate, assist, and train election officials and private sector partners as they prepare for and administer elections.

ELECTION SECURITY TRAININGS

• Description: Elections Security trainings created for election infrastructure stakeholders at convenings of election officials, such as association meetings and conferences. Trainings can be tailored to meet specific stakeholder needs.

EXERCISES

• Description: Cyber and physical security exercises with government and industry partners to enhance the security and resilience of critical infrastructure.

CUSTOMIZABLE PRODUCTS

• Description: Customizable security resources, known as Last Mile products, intended to reach small and midsized election jurisdictions by highlighting current security measures, identifying key points of contact and identifying additional security measures.

PLANNING ASSISTANCE

• Description: Assistance with incident response planning, including guidance documents and templates to help jurisdictions recognize potential incidents and develop a basic response plan.

ELECTION LITERACY EFFORTS

• Description: Amplification of election officials as trusted voices in election security through CISA's public platform. Development of educational toolkits as well as maintenance of CISA's Election Security Rumor vs Reality webpage.

FIELD-DELIVERED CYBER ASSESSMENTS



Provided by CISA field personnel to help organizations build mature cybersecurity programs. Requires action by participants to implement program improvements.

CYBER PROTECTIVE VISIT

• Description: The initial visit facilitated by the CISA Regions, prior to conducting a formal engagement. Used to assess an organization's interest in CISA services.

CYBER RESILIENCE REVIEW

• Description: Non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices across a range of ten domains including risk management, incident management, service continuity, and others.

CYBER INFRASTRUCTURE SURVEY (CIS)

• Description: Evaluates effectiveness of organizational security controls, cybersecurity preparedness, and the overall resilience of an organization's cybersecurity ecosystem.

EXTERNAL DEPENDENCIES MANAGEMENT (EDM)

• Description: Interview-based assessment to evaluate how an organization manages risks derived from its use of the Information and Communications Technology Supply Chain in the deliverance of services.

CYBERSECURITY PERFORMANCE GOAL ASSESSMENT

• Description: New module of CISA's Cybersecurity Evaluation Tool (CSET) intended to aid organizations in assessing their progress towards implementing the Cybersecurity Performance Goals.

FIELD-DELIVERED PHYSICAL ASSESSMENTS AND TRAINING



Provided by CISA field personnel to help organizations build resilient physical security programs. Requires action by participants to implement program improvements.

SECURITY ASSESSMENT AT FIRST ENTRY

• Description: SAFE is a rapid physical security assessment that provides a structured review of a facility's existing security measures and delivers feedback on observed vulnerabilities and options for improving security.

NON-CONFRONTATIONAL TECHNIQUES FOR ELECTION WORKERS

• Description: Overview of non-confrontational techniques to help election workers recognize potentially escalating situations, determine if emergency response is needed, safely de-escalate, and report appropriately within their organization or to law enforcement.

INFRASTRUCTURE SURVEY TOOL

• Description: A voluntary, web-based assessment that Protective Security Advisors conduct in coordination with facilities owners and operators to identify and document the overall security and resilience of the facility.

REGIONAL PARTNER ELECTION ENGAGEMENTS

• Description: Outreach and engagement with Election Infrastructure partners to share information, discuss best practices and provide an overview of CISA services.

IN-DEPTH CYBER SERVICES



Point-in-time assessments that require a CISA team to identify weaknesses and architectural flaws in an environment. Provides participants with technical recommendations often relevant to long-term investments.

RISK AND VULNERABILITY ASSESSMENTS

• Description: Combines national threat and vulnerability information with technical hands-on assessment to find potential weakness on a stakeholder's network remotely and onsite.

REMOTE PENETRATION TEST

• Description: Technical testing to identify remote vulnerabilities in a network, web application, phishing susceptibility and design issues.

VALIDATED ARCHITECTURE AND DESIGN REVIEW

• Description: In-depth analysis of an organization's network design as validated by packet capture review. Generally best suited for operational technology (OT) infrastructures.



2023-2024 Roadmap

Goal 1: Get Connected

- Join an information sharing community
- Apply for security clearance, if eligible under CISA's Election Infrastructure Clearance Program

Goal 2: Address Internet Facing Vulnerabilities

- Connect with CISA Regional teams
- Identify & mitigate vulnerabilities

Goal 3: Improve Physical Security

- Connect with CISA Regional teams
- Engage state grant-making authority
- Take part in a physical security assessment
- Establish relationships with state & local law enforcement

Goal 4: Prepare for Incidents

- Create incident response plans
- Train & exercise

Goal 5: Inform and Educate

- Migrate to .gov
- Develop a communications plan and election security public education effort



Goal 1: Get Connected

Elections Infrastructure Information Sharing & Analysis Center (EI-ISAC)

- A dedicated resource that gathers, analyzes, and shares information on critical infrastructure and facilitates two-way cybersecurity threat information sharing between the public and the private sectors

CISA Alerts

- Alerts provide timely information about current security issues, vulnerabilities, and exploits

Security Clearance Program

- DHS provides security clearances for state election officials and GCC & SCC members

CISA Central

- Central (central@cisa.gov) is the simplest way for critical infrastructure partners and stakeholders to engage with CISA through coordinating situational awareness, information sharing, and incident response

Election Day Situation Room

- Each Election Day, CISA and the EI-ISAC host the National Cybersecurity Situational Awareness Room. This online portal for election officials and vendors facilitates rapid information sharing and provided election officials with virtual access to CISA's 24/7 operational watch floor.

Vulnerability Reporting

- Vulnerability disclosures can be an effective way for organizations to benefit from cybersecurity expertise without having it resident to their organization

The SolarWinds Cyber-Attack: What SLTTs Need to Know

Last Updated: December 22, 2020
The MS-ISAC and EI-ISAC are available to assist our SLTT members with the SolarWinds cyber-attack. We can be contacted 24x7x365 via our Security Operations Center (SOC) at 1-866-787-4722, or soc@msisac.org. Organizations that are U.S. SLTTs and not a member can join the MS-ISAC here. Organizations that are U.S. election offices can join the EI-ISAC here.

Executive Overview

On 13 December 2020, FireEye announced the discovery of a highly sophisticated cyber intrusion that leveraged a commercial software application made by SolarWinds. It was determined that the advanced persistent threat (APT) actors infiltrated the supply chain of SolarWinds, inserting a backdoor into the product. As customers downloaded the Trojan Horse installation packages from SolarWinds, attackers were able to access the systems running the SolarWinds products.

This cyber-attack is exceptionally complex and continues to evolve. The attackers randomized parts of their actions making traditional identification steps such as scanning for known indicators of compromise (IOC) of limited value. Affected organizations should prepare for a complex and difficult remediation from this attack. We have detailed a tiered set of guidance that organizations can take based on their specific capabilities and cybersecurity maturity. We've also provided available IOCs below.

Recent evidence shows that not all organizations with the malicious SolarWinds software were compromised by the threat actor, and that there were different stages of the attack. New information also reveals that some organizations without any SolarWinds products in their environment have been compromised with the same tactics, techniques, and procedures (TTPs) as the SolarWinds attack. This indicates that the attackers may have leveraged similar supply chain attacks against other products.

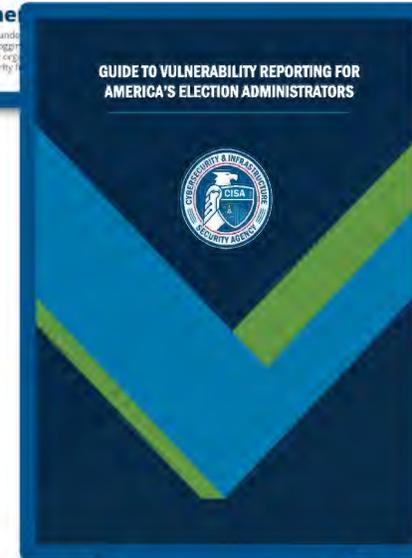
Who, What, When, Where

- Who: SLTT organizations with SolarWinds Orion Platform versions 2019.4 HF5, 2020.2 with no hotfix installed, and 2020.2 HF 1 within their environment. Note: there is evidence of organizations being compromised by this same cyber threat actor without SolarWinds products present in the network. Additional vectors are suspected and further investigation is ongoing by CISA and the FBI.
- What: A cybersecurity intrusion campaign affecting public and private organizations carried out by sophisticated APT actors. The United States government has determined that this attack poses a "grave risk to the Federal Government and state, local, tribal, and territorial governments as well as critical infrastructure entities and other private organizations."
- When: Cybersecurity company FireEye discovered the supply chain attack against the SolarWinds products while investigating a compromise of their own network and publically announced the discovery of the SUNBURST backdoor on 13 December 2020. Confirmed compromises have occurred dating back to March of 2020. Forensic evidence has revealed files associated with this attack being compiled as far back as December of 2019.
- Where: Multiple industry verticals and government agencies across the globe. According to a recent SEC filing by SolarWinds, approximately 10,000 of their 300,000 customers were running vulnerable versions of the SolarWinds Orion platform.

Recommendations

The MS- and EI-ISAC will provide monitoring tools or logon Federal Government organizations cybersecurity with the MSISAC.

Organizations that coordinate a response



Goal 2: Address Internet Facing Vulnerabilities

Cybersecurity Advisors (CSAs)

- CSAs offer cybersecurity assistance to critical infrastructure owners and operators and state, local, tribal, and territorial governments. CSAs can provide cyber preparedness, assessments and protective resources, strategic messaging, and incident coordination and support in times of cyber threat, disruption, and attack.

CISA Cybersecurity Services

- CISA offers a wide range of cybersecurity services, from scalable services like Vulnerability Scanning, Web Application Scanning, and Crossfeed to more in-depth, resource intensive services like Remote Penetration Tests and Risk and Vulnerability Assessments.

EI-ISAC Services

- CISA-funded, ISAC-delivered services actively detect and prevent threats. These services include Endpoint Detection and Response (EDR) and Malicious Domain Blocking and Reporting (MDBR).

CISA Joint Cyber Defense Collaborative (JCDC)

- JCDC is a public-private cybersecurity collaborative that leverages new authorities granted by Congress to unite the cyber community in the collective defense of cyberspace. JCDC's core functions include developing and coordinating plans for cyber defense operations, driving operational collaboration and cybersecurity information fusion, and producing and sharing cyber defense guidance.



Election Infrastructure Subsector Recommendations

CISA recommends the following mitigations to reduce cyber risk among EI Subsector entities:

- ✓ Improve **phishing defenses** by implementing a phishing awareness training program.
- ✓ **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 operating systems** to supported versions.
- ✓ Identify **all internet-accessible services** and **secure or disable risky services** according to the documented business reason for each service to operate.



Additional Recommendations



Strengthen Password Policy and Auditing Processes.

Use multi-factor authentication and perform regular audits of password policies. Password best practices include ensuring that strong passwords are required and that administrators utilize encrypted password vaults.

Have a Plan and Implement Backups. Follow established enterprise network best practices for IT infrastructure. This includes implementing a strong patching methodology for operating systems and third-party products. Your organization should also create an Incident Response Plan and Continuity of Operations Plan.

Patch and Update Systems. Use equipment that is maintainable with current security patching. Exceptions should be minimized and isolated.

Implement Network Segmentation. Internal network architecture should protect and control access to the entity's most sensitive systems. User workstations should be less trusted and connections to external networks should be isolated, controlled, and monitored.



Goal 3: Improve Physical Security

Protective Security Advisors (PSAs)

- PSAs are trained critical infrastructure protection and vulnerability mitigation subject matter experts.

Physical Security Assessments

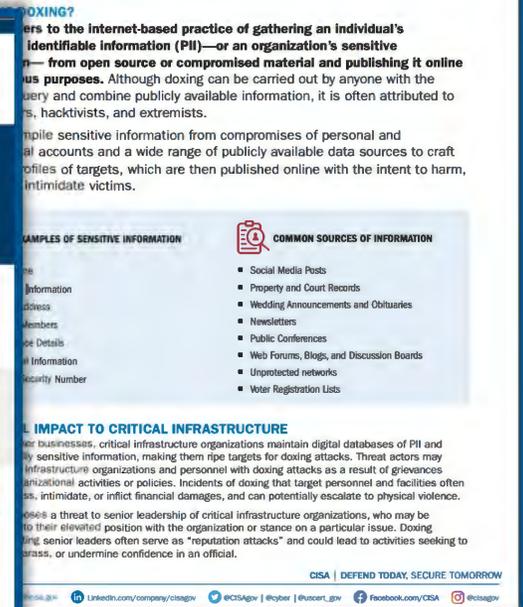
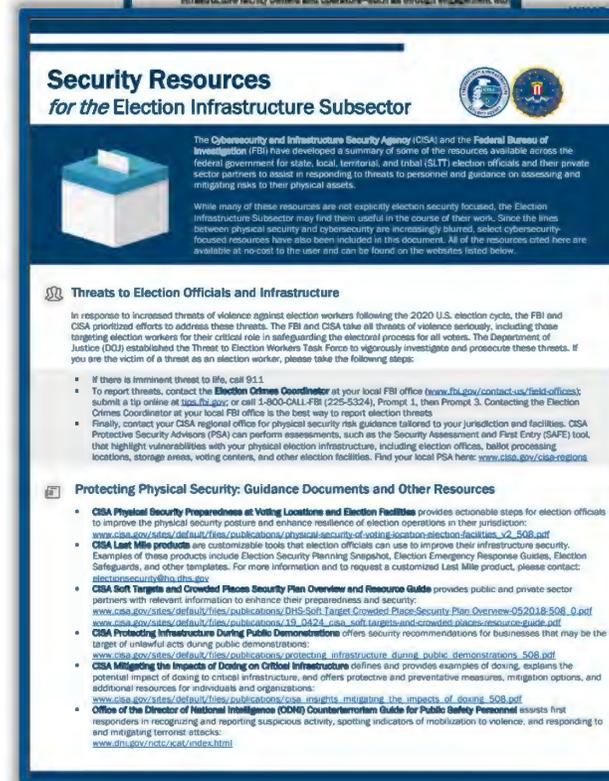
- CISA field personnel offer a variety of physical security assessments and resources to improve the physical security of election infrastructure assets, like Security Assessment at First Entry (SAFE), Non-Confrontational Techniques for Election Workers, and the Infrastructure Survey Tool.

Hometown Security

- The Hometown Security page (<https://www.cisa.gov/hometown-security>) is a one-stop shop for CISA's physical security resources

Publicly Available Physical Security Guidance

- CISA has issued guidance on a number of physical security topics, including *Physical Security of Voting Locations and Election Facilities* and *Mitigating the Impacts of Doxing on Critical Infrastructure*.



Goal 4: Prepare for Incidents

CISA-facilitated Training

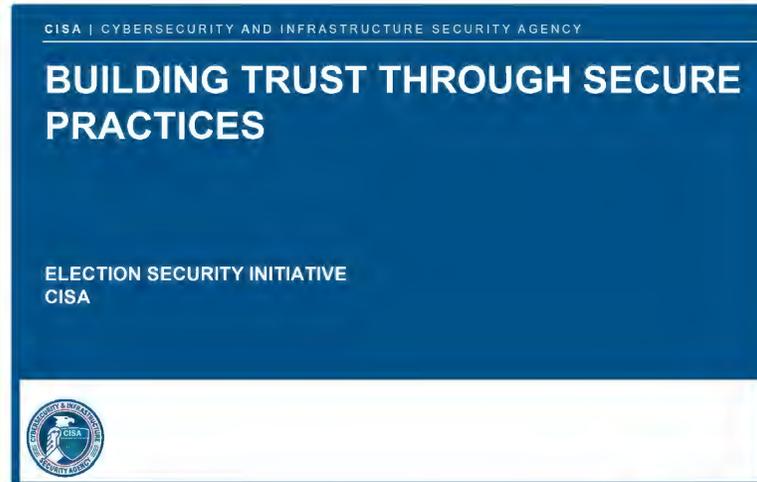
- CISA has a team of subject matter experts available to facilitate and deliver training on a variety of election security topics, including Ransomware, Phishing, Building Trust Through Secure Practices, and more.

CISA Tabletop Exercise Packages (CTEPs)

- CTEPs are a comprehensive set of customizable resources designed to assist stakeholders in conducting their own exercises. Partners can use CTEPs to initiate discussions within their organizations about their ability to address a variety of threat scenarios. Election-specific CTEPs include Active Shooter, Insider Threat, Potential Civil Unrest, Early Voting, Election Day Voting Machines, and Vote-by-Mail.

Asynchronous Training Options

- CISA Election Security Trainings on CISA's YouTube channel: <https://www.youtube.com/@CISAgov>
- Federal Virtual Training Environment (FedVTE)



What Is Ransomware?

- Ransomware is a type of **malicious software designed to deny access to a computer systems or data until a ransom is paid.**
- If ransom demands are not met, the system or encrypted data remains unavailable, or data may be deleted.
- In elections this could be used to deny access to or delete Voter Registration and/or Vote Tabulation data.



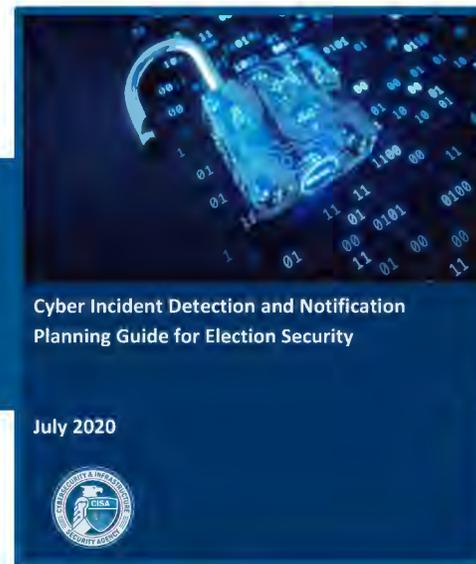
Planning

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**.

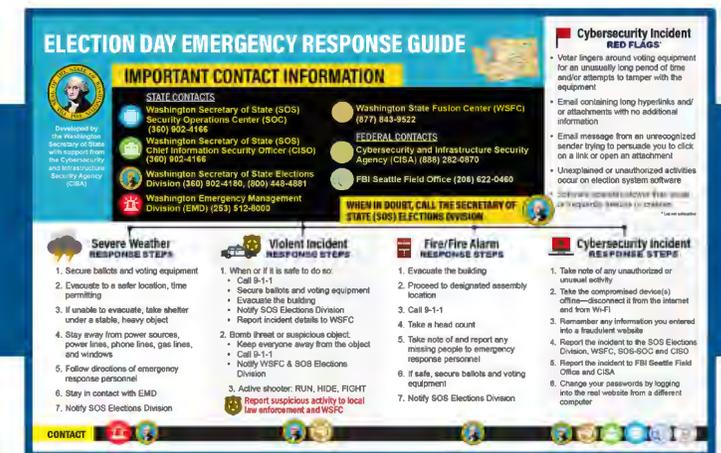
Incident Response Guide

- 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



.GOV Top-Level Domain

CISA administers the .gov Top-Level Domain and makes it available **at no cost** solely to U.S.-based government organizations.

It should be easy to identify governments on the internet, and using a .gov domain shows you're official.

DOTGOV Act of 2020

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://get.gov/about/elections/> for more information.



Exercises and Training

CISA Exercises

- Annual National “Tabletop the Vote”
- State-based exercises
- “Tabletop-in-a-box”

Training Offerings

- Elections Security Overview
- Ransomware
- Phishing
- Building Trust through Secure Practices
- Insider Threat Mitigation
- De-Escalation Techniques for Election Officials

A collage of three CISA training materials. The top right is a blue slide titled 'BUILDING TRUST THROUGH SECURE PRACTICES' under the 'ELECTION SECURITY INITIATIVE'. The middle left is a white slide titled 'ELECTIONS CYBER TABLETOP EXERCISE PACKAGE Situation Manual' dated January 2020. The bottom right is a white slide titled 'What Is Ransomware?' with a list of bullet points and an illustration of a hand holding cash in front of a laptop with a red padlock on the screen.

BUILDING TRUST THROUGH SECURE PRACTICES

ELECTION SECURITY INITIATIVE
CISA

ELECTIONS CYBER TABLETOP EXERCISE PACKAGE

Situation Manual

January 2020

Cybersecurity and Infrastructure Security Agency
Exercise Program

What Is Ransomware?

- Ransomware is a type of **malicious software designed to deny access to a computer systems or data until a ransom is paid.**
- If ransom demands are not met, the system or encrypted data remains unavailable, or data may be deleted.
- In elections this could be used to deny access to or delete Voter Registration and/or Vote Tabulation data.

Ryan Macias
February 24, 2021

Core Services & Resources

Alerts & Information Sharing

- Cooperative Agreement funding MS-ISAC & EI-ISAC
 - Albert Sensors, MDBR, EDR
- Threat Briefings, Security Clearance Program
- E-Day Ops Center & EI-ISAC Virtual Sit. Room

Cybersecurity Services & Incident Response

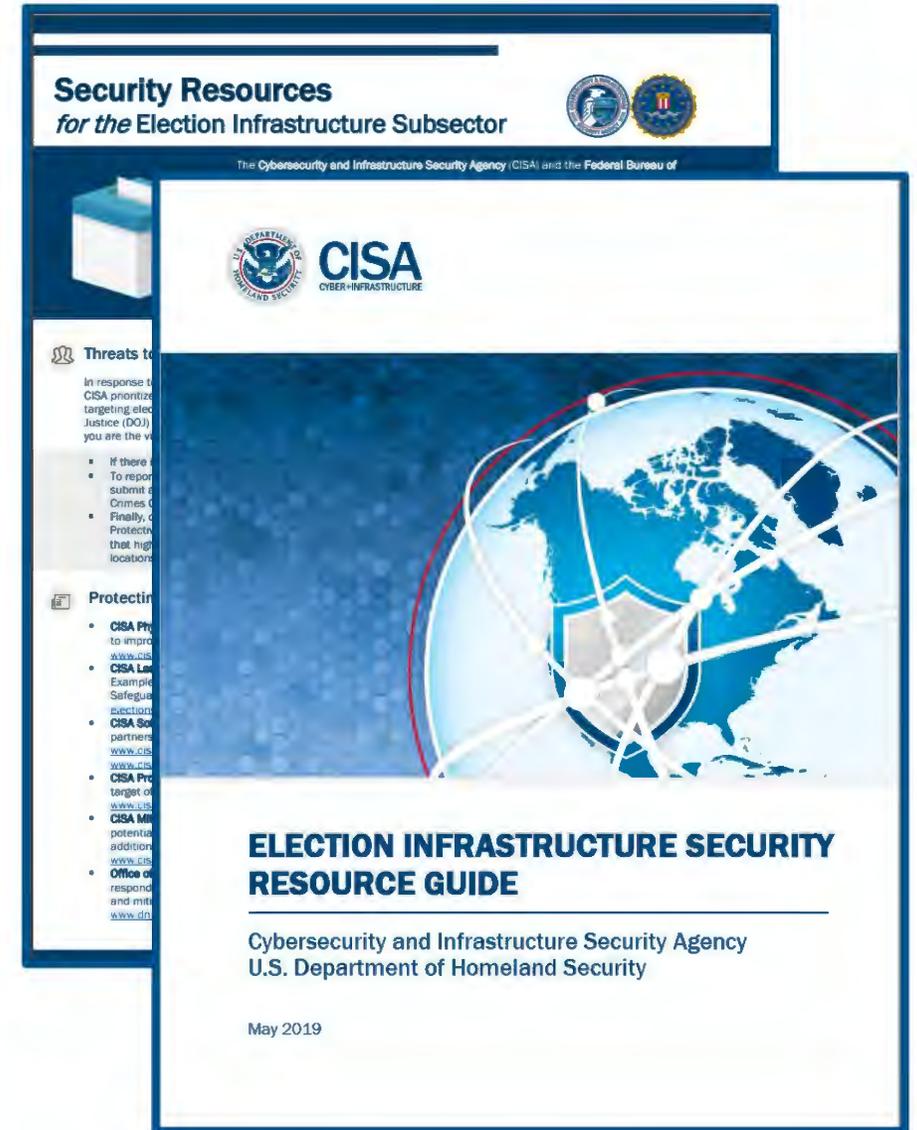
- Vulnerability Scanning, Phishing Campaign Assessments, Remote Penetration Testing, etc.
- .gov TLD

Cybersecurity & Protective Security Advisors

- Physical Security Assessments

Exercises & Trainings

Last Mile Products





Keith Ingram

Election Security Advisor

Keith.Ingram@cisa.dhs.gov

(202)538-1198

Joel Meyers

Protective Security Advisor

Joel.Meyers@cisa.dhs.gov

(202)702-3065

<https://www.cisa.gov/electionsecurity>



January 26, 2024