CISA ELECTION SECURITY

HOMELAND SECURITY TASK FORCE (HSTF) AND RE-ISAC

OCTOBER 27, 2022

Overview

- Threat Landscape
- Core CISA Support to Election Officials
- Incident Response
- Election Cybersecurity Toolkit
- Election Physical Security Toolkit

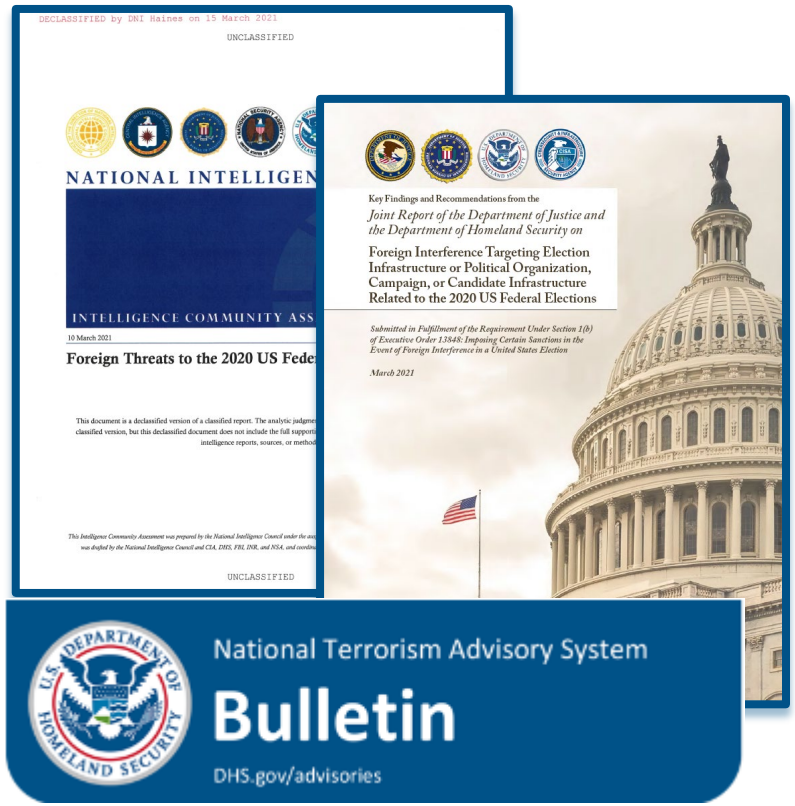
Threat Landscape

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, […] 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 […]"



Threat Landscape

Potential Adversaries

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

Possible Motivations

- Undermine Trust in Democracy and/or Election Results
- Foreign Policy Goals
- Sow Social Division
- Financial Gain
- Subvert Political Opposition
- 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 Workers, Vendors, etc.

Geopolitical Considerations

Shields Up - cisa.gov/shields-up

- Russia's invasion of Ukraine could impact organizations beyond the region, to include malicious cyber activity against the U.S. homeland, including as a response to the unprecedented economic costs imposed on Russia by the U.S. and our allies and partners.
- Evolving intelligence indicates that the Russian Government is exploring options for potential cyberattacks.
- Every organization—large and small—must be prepared to respond to disruptive cyber incidents.
- Each and everyday we remain focused on these threats

Core Resources

Alerts & Information Sharing

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

Cyber Security Services

- Vulnerability Scanning, .gov

Cyber Security Advisors

Exercises & Trainings

Making .gov More Secure by Default

.gov

When the public sees information on a .gov website, they need to trust that it is official and accurate. This trust is warranted, because registration of a .gov domain is limited to bona fide US-based government organizations. Governments should be easy to identify on the internet and users should be secure on .gov websites.

HTTPS is a key protection for websites and web users. It offers security and privacy when connecting to the web, and provides governments the assurance that what they publish is what is delivered to users. In the last few years,

CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

Leveraging the .gov Top-level Domain

The .gov domain is a top-level domain (TLD) that was established to make it easy to identify US-based government organizations on the internet. All three branches of the US Government, all 50 states, and many local governments use .gov for their domains.

The DotGov Program, based at the US General Services Administration (GSA), manages the .gov TLD.

Why should State and Local Election Officials be interested in .gov?

Since a .gov domain is only available to bona fide US-based government organizations, using it signals trust and credibility. This can help a state or local election office establish its digital services (e.g., websites, emails) as official, trusted sources for voter information.

Election Cybersecurity Toolkit

- CISA, through the JCDC, has developed a one-stop catalogue of free election cyber services, tools, and resources
- The **Protecting U.S. Elections: A Cybersecurity Toolkit** can be used to help election officials and vendors to enhance their cyber security and resilience of election infrastructure
- Toolkit is available here: https://www.cisa.gov/cybersecurity-toolkit-protect-elections

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

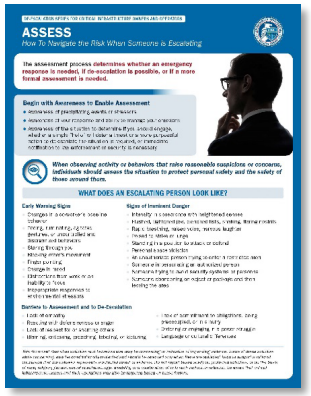
Election Physical Security Resources

- CISA Protective Security Advisor: CISA Assessments & Evaluations
- Risk mitigation training: Office for Bombing Prevention, Active Shooter preparedness and insider threat training
- Non–Confrontational Techniques for ELECTION Workers

De-Escalation Series

Recognize

the warning signs for someone on a path to violence, identify stressors, changes in baseline behavior, and observable behavioral indicators.

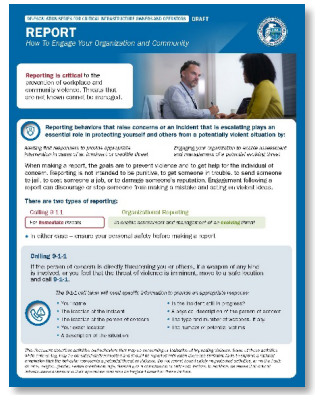


Assess

the situation to protect personal safety and the safety of those around you. Identify what an escalating person may look like and warning signs.

De-Escalation

encourages the use of purposeful actions, verbal techniques, and body language to calm a potentially dangerous situation. Safety is the highest priority, know your limits and obtain help immediately if needed.



Report

concerning behavior or an escalating incident through organizational reporting to enable assessment and management of an evolving threat, and 9-1-1 for immediate threats.

cisa.gov/de-escalation-series

CISA Election Security Resources

ELECTION SECURITY RESOURCES

Provides state and local governments, election workers, campaigns, the vendor community, and voters with voluntary tools and security capacity building resources to secure election-related assets, facilities, networks and systems from cyber and physical risks.

cisa.gov/election-security-library

- Multiple Infographic products to combat election dis-information
- *Election Security Rumor vs. Reality*
- *Physical Security of Voting Locations* and *Election Facilities Guide*
- *Security Resources for the Election Infrastructure Subsector*

cisa.gov/active-shooter-preparedness

- *Physical Security Considerations for Temporary Facilities*
- *Emergency Action Plan* Template and Guide
- *Options for Consideration* Video
- *Active Shooter: What You Can Do – Access and Functional Needs* Video
- *Personal Security Considerations* Fact Sheet
- *Protecting Infrastructure During Public Demonstrations* Fact Sheet

Contact your local Protective Security Advisor at **cisa.gov/protective-security-advisors** or email **central@cisa.dhs.gov**

Operating Posture on Election Day

Election Day Operations

- CISA In-Person Operations Room with Federal and Private Sector Partners
- Monitoring EI-ISAC Situation Room
- Frequent Check-ins with Stakeholders
- Cyber Incident Response Outreach, If requested
- Respond to State/Local/Private Sector Inquiries

Mohamed Telab
Deputy Regional Director, Region 2
Cybersecurity and Infrastructure Security Agency
Mohamed.telab@hq.dhs.gov

Contact CISA:
electionsecurity@cisa.dhs.gov

Risk Mitigations for Voting Facilities

Based upon the results of your vulnerability assessment, election workers may consider some of the below cost-effective protective measures to enhance security:

- Post appropriate way-finding and accessibility signage on entrances and paths
- Ensure CCTV systems are operable and monitored
- Restrict high-speed avenues of approach; have appropriate lighting
- Limit amount of people at entry point
- Ensure support personnel are familiar with de-escalation tactics; use “buddy system”
- Secure or post election workers to monitor non-public entrances
- Consider measures related to access control/bag check procedures
- Ensure a clean perimeter area; remove/lock trash receptacles
- Establish several communication methods with local law enforcement (LE) for reporting
- Train election workers to report suspicious bags, parcels or cookware to local LE

This is not a complete list of measures; each voting location is unique, and you should consult your local law enforcement agency .