CISA ELECTION SECURITY UPDATES
NASED OPEN SESSION

February 25, 2022
Overview

- CISA’s Priorities for the 2022 Election Cycle
- Cybersecurity
- Mis-, Dis- and Malinformation
- Physical Security
- Questions and Feedback
Cybersecurity

Ukraine/Russia

2022 Election Infrastructure Subsector Cyber Risk Summary Report (TLP: AMBER)
- Known Exploited Vulnerabilities (KEVs)

Voter Registration Systems & Information
- Web Application Scanning

CISA-Funded EI-ISAC Services
- Endpoint Detection and Response (EDR)
- Malicious Domain Blocking and Reporting (MDBR)
CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure

Rumor Control

GCC-SCC Joint Working Group on MDM
- Rumor Control Start-Up Guide
- MDM Planning and Incident Response Guide
Mis-, Dis- & Malinformation

.gov Top Level Domain

Training
• Election Security: Building Trust through Secure Practices
• MDM: Communications in a Dynamic Election Environment

Making .gov More Secure by Default

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, HTTPS has become the default connection type on the web. Browsers that were once telling users to “watch for a green lock!” are now removing the lock icons. Instead, the browser warns users when sites are not using HTTPS.

Governments should never be "not secure".
Physical Security

DHS NTAS Bulletin
• Domestic Violent Extremists

CISA-FBI Security Resources for the Election Infrastructure Subsector

Protective Security Advisors
• Physical Security Assessments

Last Mile Product: Election Personnel Threat Reporting Guide
New Last Mile Product

Election Personnel Threat Reporting Guide

- Shares tailorable threat documentation and reporting guidance for election officials

Guide Development

- Voluntary product available by request through CISA’s Last Mile initiative
- Fully customizable based on each jurisdiction’s laws, process, and procedures
Additional Resources

Threat Briefings & Security Clearance Program

Cybersecurity Services & Incident Response

Last Mile Products
- Election Security Safeguards
- Election Day Emergency Response Guide

Exercises & Trainings
- National Tabletop the Vote 2022
- State-based Tabletop Exercises

Election Day Operations Center & EI-ISAC Virtual Situational Awareness Room
Feedback and Questions

Requests: electionsecurity@cisa.dhs.gov
Kim Wyman
Senior Election Security Lead
Cybersecurity and Infrastructure Security Agency

Geoff Hale
Director, Election Security Initiative
Cybersecurity and Infrastructure Security Agency

Contact CISA:
electionsecurity@cisa.dhs.gov