ELECTION SECURITY OVERVIEW

CISA
August 24, 2021

CISA and Election Infrastructure

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:

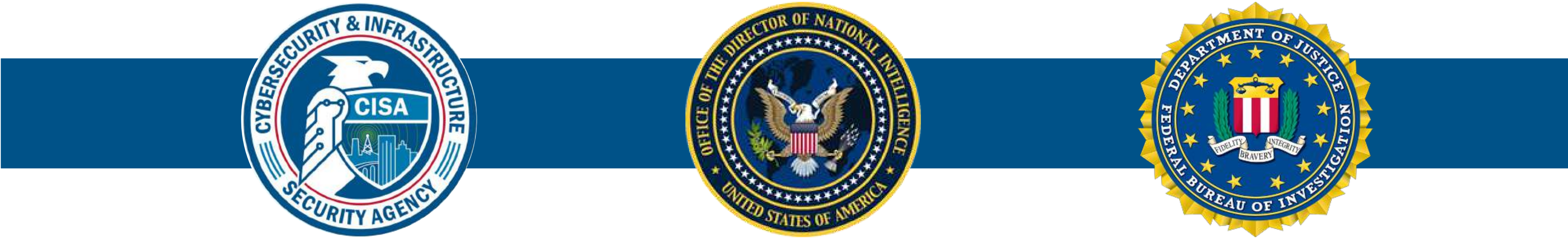
- Recognize the importance of these systems;
- Prioritize services and support to enhancing security for election infrastructure;
- Provide the elections community with the opportunity to work with each other, the Federal Government, and through the Coordinating Councils; and
- Hold anyone who attacks these systems responsible for violating international norms.

Election Security Mission

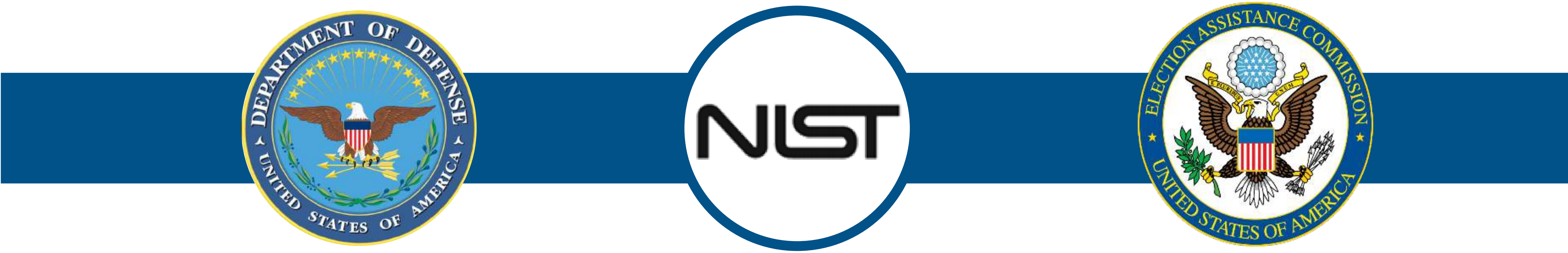
To ensure the election community and American public have the necessary information and tools to adequately assess risks to the election process and protect, detect, and recover from those risks

Jen Easterly, CISA Director

CISA & Election Infrastructure


CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
UNITED STATES OF AMERICA
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY
BRAVERY
INTEGRITY

Federal Partners

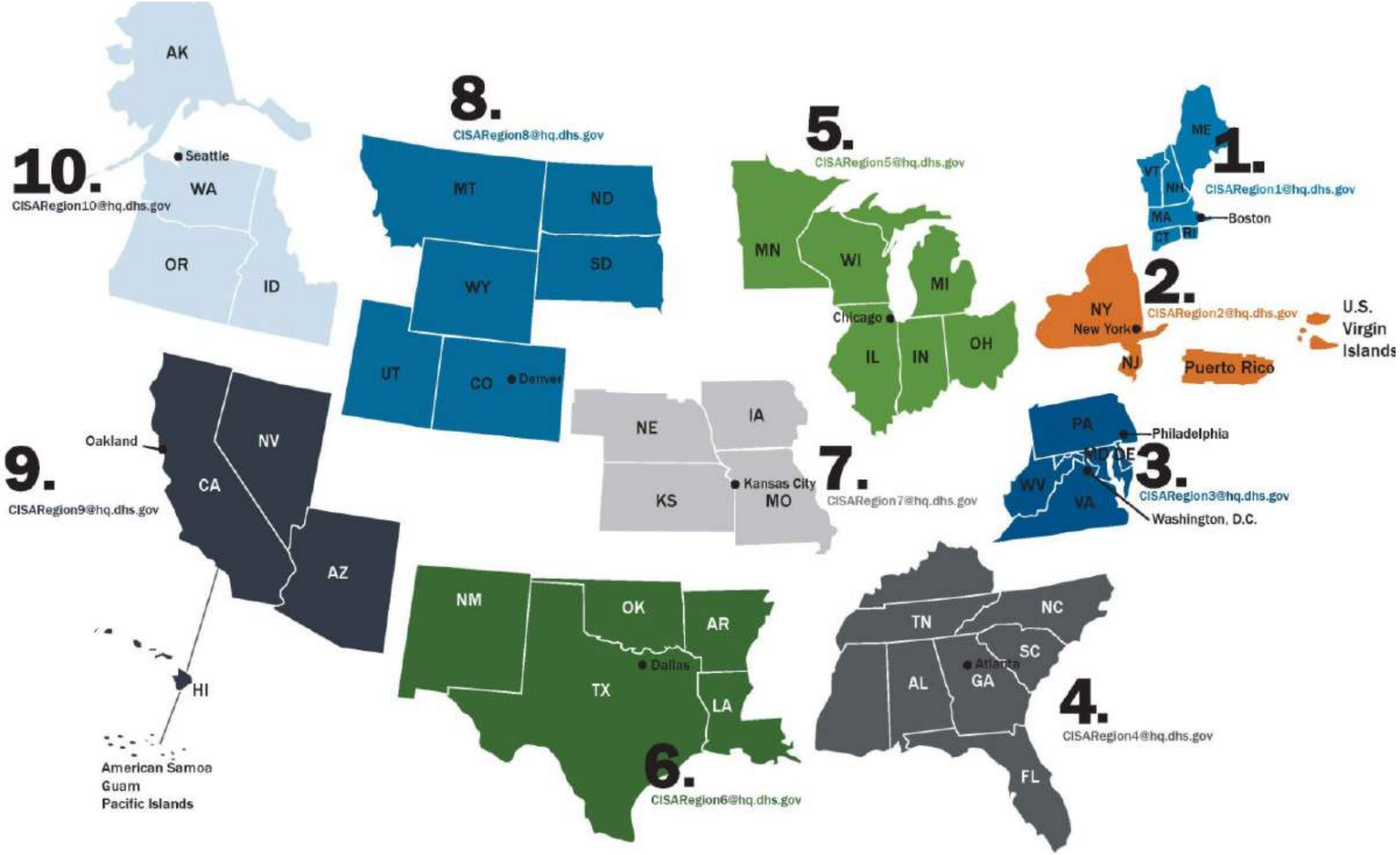


CISA & Election Infrastructure

Election Security Initiative

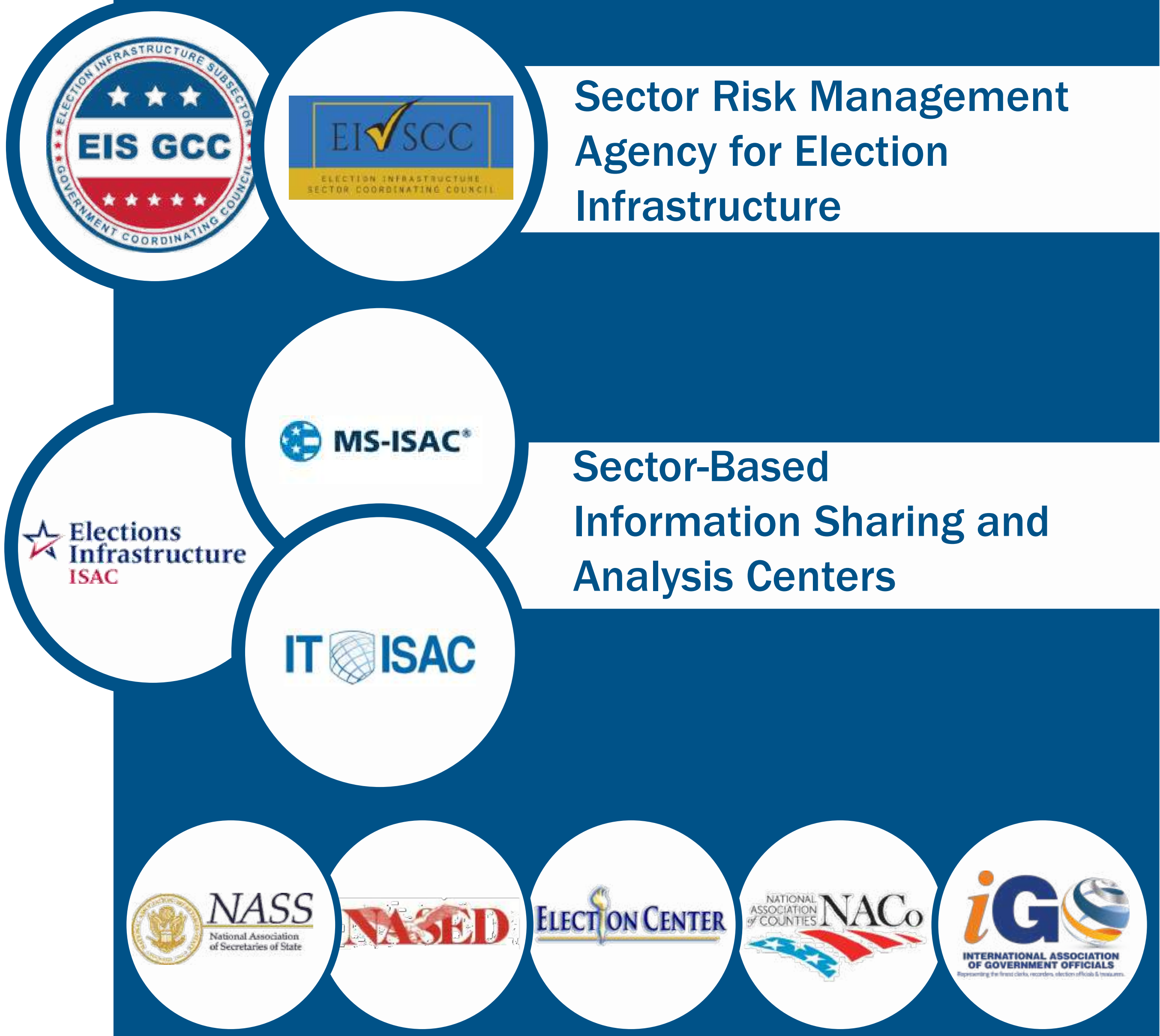
- Sector Risk Management Agency Team
- Mis-, Dis-, and Malinformation Team

CISA Regional Offices



Partnership Model

- All **50 states and 2,954 local jurisdictions** are members of the EI-ISAC
- DHS has granted a total of **204 security clearances** through the election infrastructure clearance program
- Between November 2019 and November 2020, CISA provided approximately **450 Vulnerability Scanning services and Cyber Assessments**
- Albert Sensors are deployed in all **50 states**
- Hosted **three 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 **5,753 election administrators in 29 states**



EIS GCC
Election Infrastructure Subsector Government Coordinating Council
EI SCC
Election Infrastructure Sector Coordinating Council
Elections Infrastructure ISAC
MS-ISAC
IT ISAC
NASS
National Association of Secretaries of State
NASED
Election Center
National Association of Counties NACo
iGO
International Association of Government Officials

Sector Risk Management Agency for Election Infrastructure

Sector-Based Information Sharing and Analysis Centers

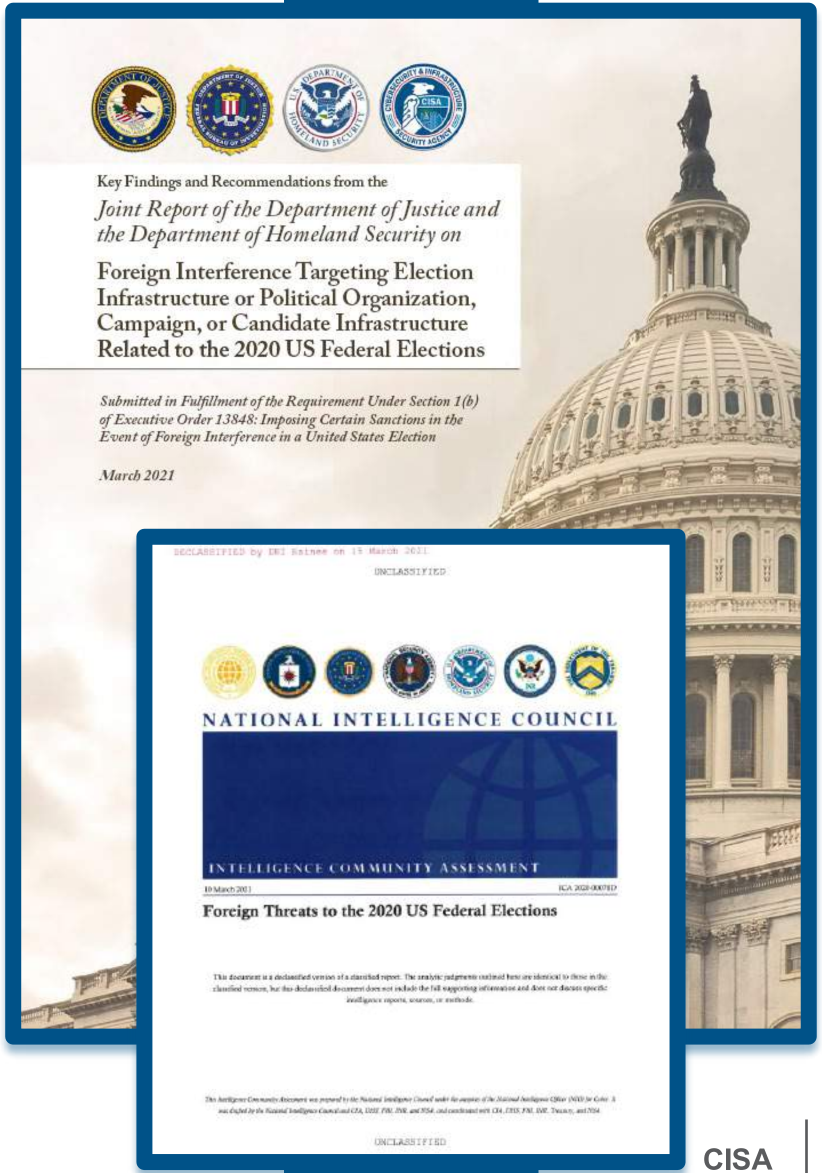
Threat Landscape

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."



Key Findings and Recommendations from the

Joint Report of the Department of Justice and the Department of Homeland Security on

Foreign Interference Targeting Election Infrastructure or Political Organization, Campaign, or Candidate Infrastructure Related to the 2020 US Federal Elections

Submitted in Fulfillment of the Requirement Under Section 1(b) of Executive Order 13848: Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election

March 2021

DECLASSIFIED by DNI Haines on 15 March 2021

UNCLASSIFIED

NATIONAL INTELLIGENCE COUNCIL

INTELLIGENCE COMMUNITY ASSESSMENT

10 March 2021 ICA 2020-00078D

Foreign Threats to the 2020 US Federal Elections

This document is a declassified version of a classified report. The analytic judgments outlined here are identical to those in the classified version, but this declassified document does not include the full supporting information and does not discuss specific intelligence reports, sources, or methods.

This Intelligence Community Assessment was prepared by the National Intelligence Council under the auspices of the National Intelligence Officer (NIO) for Cyber. It was drafted by the National Intelligence Council and CIA, DHS, FBI, INR, and NSA, and coordinated with CIA, DHS, FBI, INR, Treasury, and NSA.

UNCLASSIFIED

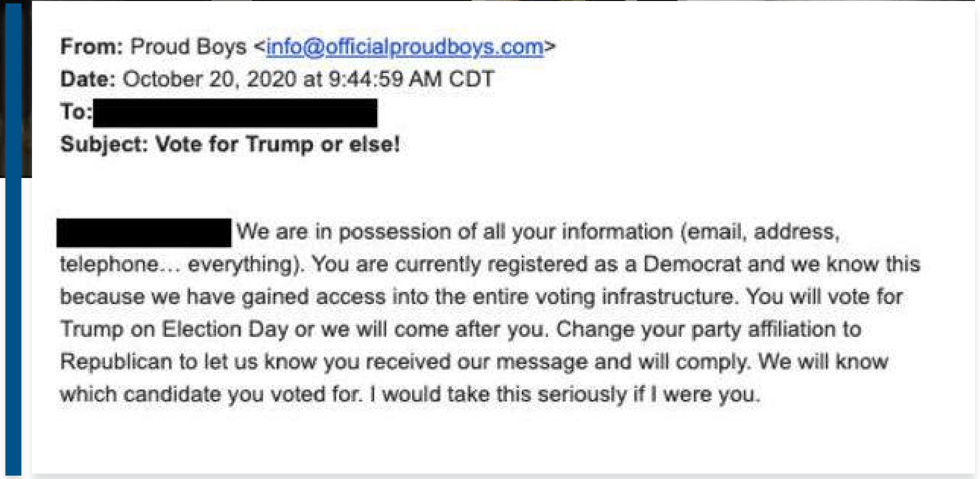
Threat Landscape

2016

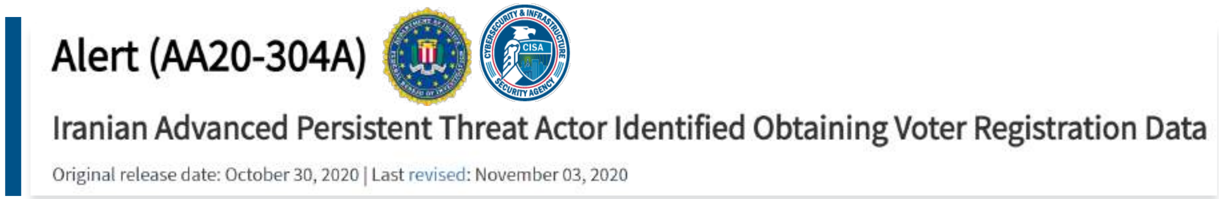
- **Russian** APT cyber and influence activity

2020

- **E-Day** ”just another Tuesday on the Internet”
- **Russian** APT cyber and influence activity
- **Iranian** APT cyber and influence activity
- **Ransomware**
- **Enemies of the People**
- **Mis- and Disinformation**
- **SolarWinds**


From: Proud Boys <info@officialproudboys.com>
Date: October 20, 2020 at 9:44:59 AM CDT
To: [redacted]
Subject: Vote for Trump or else!

[redacted] We are in possession of all your information (email, address, telephone… everything). You are currently registered as a Democrat and we know this because we have gained access into the entire voting infrastructure. You will vote for Trump on Election Day or we will come after you. Change your party affiliation to Republican to let us know you received our message and will comply. We will know which candidate you voted for. I would take this seriously if I were you.


Alert (AA20-304A)

Iranian Advanced Persistent Threat Actor Identified Obtaining Voter Registration Data

Original release date: October 30, 2020 | Last revised: November 03, 2020

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 Officials, Vendors, etc.

Emerging Cyber Threat Trends

- Interconnected systems enabling threat actors.
  - Targets of opportunity.
  - Paths of least resistance.
- PII and data: high value, high-demand commodities.
- Hacking as a service (HaaS)
  - Malicious tools readily available for purchase or download.

Source: DHS I&A

Threat Vectors

- Phishing / Spear-phishing
- Social Engineering
- Business Email Compromise (BEC)
- Exploiting unpatched vulnerabilities on web-facing systems
  - Especially remote-access (e.g., VPN, RDP)
- Exploiting third-parties (e.g., managed services)
- Compromising home networks of employees or family members via emails & telework applications
- Focus on remote / collaboration platforms and cloud services (O365, Webex, Google Drive credentials)

Information Sharing

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

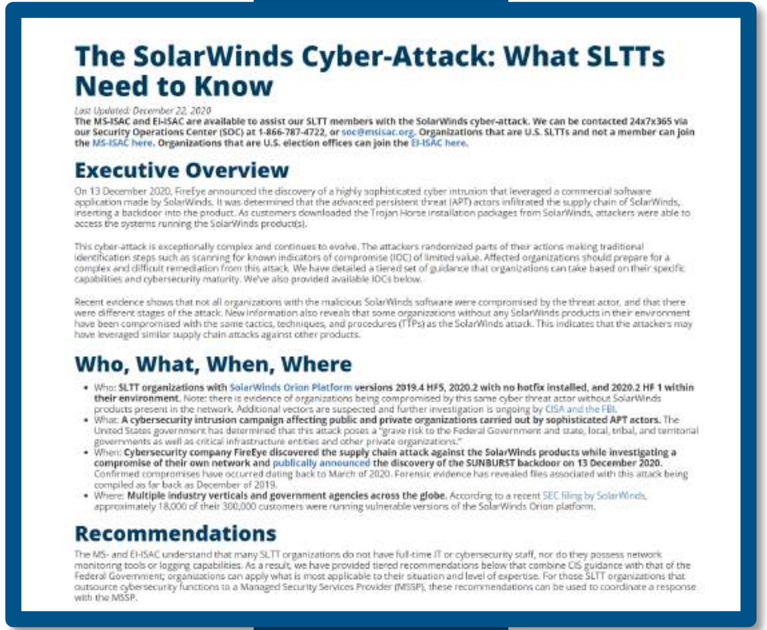
- Central (central@cisa.gov) is the simplest way for critical infrastructure partners and stakeholders to engage with CISA through coordinating situational awareness, information sharing, and incident response

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 product(s).

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 18,000 of their 300,000 customers were running vulnerable versions of the SolarWinds Orion platform.

Recommendations

The MS- and EI-ISAC understand that many SLTT organizations do not have full-time IT or cybersecurity staff, nor do they possess network monitoring tools or logging capabilities. As a result, we have provided tiered recommendations below that combine CIS guidance with that of the Federal Government; organizations can apply what is most applicable to their situation and level of expertise. For those SLTT organizations that outsource cybersecurity functions to a Managed Security Services Provider (MSSP), these recommendations can be used to coordinate a response with the MSSP.

GUIDE TO VULNERABILITY REPORTING FOR AMERICA'S ELECTION ADMINISTRATORS

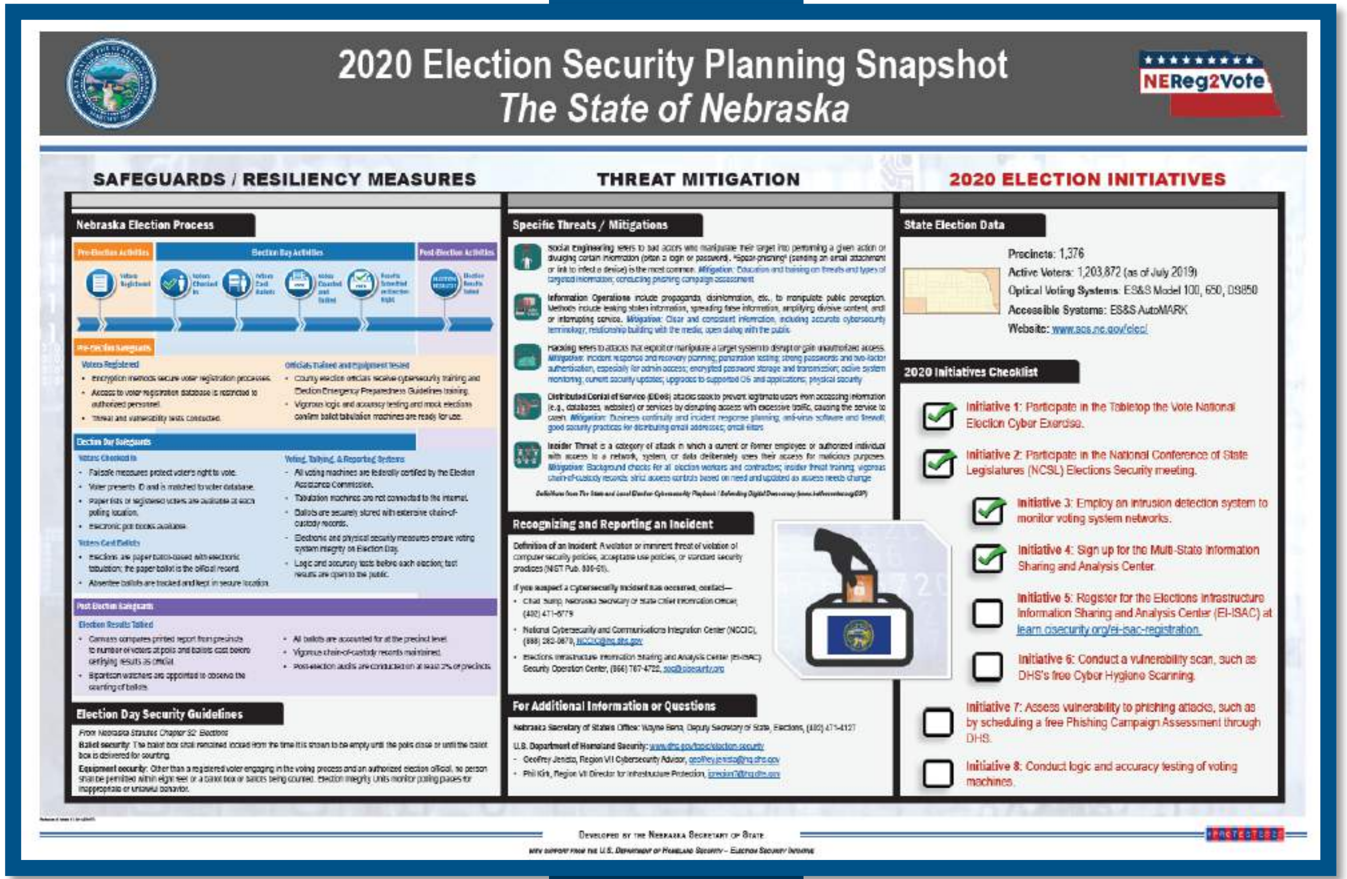
Building Situational Awareness

Last Mile Initiative

- Thousands of local jurisdictions make up the U.S. elections stakeholder community and together represent the “Last Mile” in reducing risk to election infrastructure. The CISA Last Mile initiative offers a range of customizable tools that can be tailored to meet the unique needs of stakeholders

Small/Mid-Size Jurisdictions

- Though CISA aims to engage every election administrator across the nation, Last Mile emphasizes engagement with small and mid-size jurisdictions that may have fewer resources to harden their cybersecurity posture and fewer opportunities to engage with CISA



2020 Election Security Planning Snapshot
The State of Nebraska

NEReg2Vote

SAFEGUARDS / RESILIENCY MEASURES

Nebraska Election Process

Pre-Election Activities | Election Day Activities | Post-Election Activities

Voters Registered
Voters Checked In
Voters Cast Ballots
Votes Counted and Tallied
Results Submitted on Election Night
Election Results Tallied

Pre-Election Safeguards

Voters Registered
- Encryption methods secure voter registration processes.
- Access to voter registration database is restricted to authorized personnel.
- Threat and vulnerability tests conducted.

Officials Trained and Equipment Tested
- County election officials receive cybersecurity training and Election Emergency Preparedness Guidelines training.
- Vigorous logic and accuracy testing and mock elections confirm ballot tabulation machines are ready for use.

Election Day Safeguards

Voters Checked In
- Failsafe measures protect voter's right to vote.
- Voter presents ID and is matched to voter database.
- Paper lists of registered voters are available at each polling location.
- Electronic poll books available.

Voters Cast Ballots
- Elections are paper ballot-based with electronic tabulation; the paper ballot is the official record.
- Absentee ballots are tracked and kept in secure location.

Voting, Tallying, & Reporting Systems
- All voting machines are federally certified by the Election Assistance Commission.
- Tabulation machines are not connected to the internet.
- Ballots are securely stored with extensive chain-of-custody records.
- Electronic and physical security measures ensure voting system integrity on Election Day.
- Logic and accuracy tests before each election; test results are open to the public.

Post-Election Safeguards

Election Results Tallied
- Canvass compares printed report from precincts to number of voters at polls and ballots cast before certifying results as official.
- Bipartisan watchers are appointed to observe the counting of ballots.
- All ballots are accounted for at the precinct level.
- Vigorous chain-of-custody records maintained.
- Post-election audits are conducted on at least 2% of precincts.

Election Day Security Guidelines

From Nebraska Statutes Chapter 32: Elections

Ballot security: The ballot box shall remained locked from the time it is shown to be empty until the polls close or until the ballot box is delivered for counting.

Equipment security: Other than a registered voter engaging in the voting process and an authorized election official, no person shall be permitted within eight feet of a ballot box or ballots being counted. Election Integrity Units monitor polling places for inappropriate or unlawful behavior.

THREAT MITIGATION

Specific Threats / Mitigations

Social Engineering refers to bad actors who manipulate their target into performing a given action or divulging certain information (often a login or password). "Spear-phishing" (sending an email attachment or link to infect a device) is the most common. *Mitigation:* Education and training on threats and types of targeted information; conducting phishing campaign assessment.

Information Operations include propaganda, disinformation, etc., to manipulate public perception. Methods include leaking stolen information, spreading false information, amplifying divisive content, and/or interrupting service. *Mitigation:* Clear and consistent information, including accurate cybersecurity terminology; relationship building with the media; open dialog with the public.

Hacking refers to attacks that exploit or manipulate a target system to disrupt or gain unauthorized access. *Mitigation:* Incident response and recovery planning; penetration testing; strong passwords and two-factor authentication, especially for admin access; encrypted password storage and transmission; active system monitoring; current security updates; upgrades to supported OS and applications; physical security.

Distributed Denial of Service (DDoS) attacks seek to prevent legitimate users from accessing information (e.g., databases, websites) or services by disrupting access with excessive traffic, causing the service to crash. *Mitigation:* Business continuity and incident response planning; anti-virus software and firewall; good security practices for distributing email addresses; email filters.

Insider Threat is a category of attack in which a current or former employee or authorized individual with access to a network, system, or data deliberately uses their access for malicious purposes. *Mitigation:* Background checks for all election workers and contractors; insider threat training; vigorous chain-of-custody records; strict access controls based on need and updated as access needs change.

Definitions from The State and Local Election Cybersecurity Playbook / Defending Digital Democracy (www.belfercenter.org/D3P)

Recognizing and Reporting an Incident

Definition of an Incident: A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices (NIST Pub. 800-61).

If you suspect a cybersecurity incident has occurred, contact—
- Chad Sump, Nebraska Secretary of State Chief Information Officer, (402) 471-6779
- National Cybersecurity and Communications Integration Center (NCCIC), (888) 282-0870, NCCIC@hq.dhs.gov
- Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) Security Operation Center, (866) 787-4722, soc@cisecurity.org

For Additional Information or Questions

Nebraska Secretary of State's Office: Wayne Bena, Deputy Secretary of State, Elections, (402) 471-4127

U.S. Department of Homeland Security: www.dhs.gov/topic/election-security
- Geoffrey Jenista, Region VII Cybersecurity Advisor, geoffrey.jenista@hq.dhs.gov
- Phil Kirk, Region VII Director for Infrastructure Protection, iprregion7@hq.dhs.gov

2020 ELECTION INITIATIVES

State Election Data

Precincts: 1,376
Active Voters: 1,203,872 (as of July 2019)
Optical Voting Systems: ES&S Model 100, 650, DS850
Accessible Systems: ES&S AutoMARK
Website: www.sos.ne.gov/elec/

2020 Initiatives Checklist

☑ **Initiative 1:** Participate in the Tabletop the Vote National Election Cyber Exercise.

☑ **Initiative 2:** Participate in the National Conference of State Legislatures (NCSL) Elections Security meeting.

☑ **Initiative 3:** Employ an intrusion detection system to monitor voting system networks.

☑ **Initiative 4:** Sign up for the Multi-State Information Sharing and Analysis Center.

□ **Initiative 5:** Register for the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) at learn.cisecurity.org/ei-isac-registration.

□ **Initiative 6:** Conduct a vulnerability scan, such as DHS's free Cyber Hygiene Scanning.

□ **Initiative 7:** Assess vulnerability to phishing attacks, such as by scheduling a free Phishing Campaign Assessment through DHS.

□ **Initiative 8:** Conduct logic and accuracy testing of voting machines.

Developed by the Nebraska Secretary of State
with support from the U.S. Department of Homeland Security – Election Security Initiative

#PROTECT2020

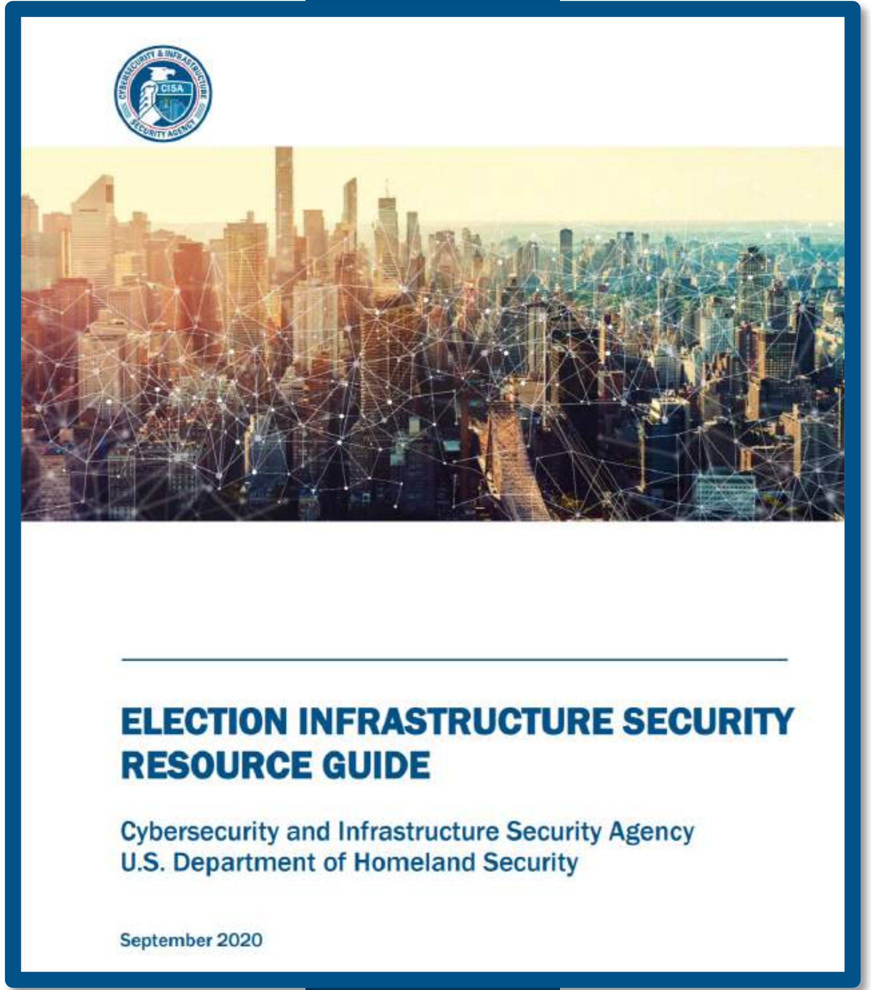
Cybersecurity Services

CISA Services

- **Vulnerability Scanning (Cyber Hygiene)**
- **Remote Penetration Testing**
- Phishing Campaign Assessment
- Critical Product Evaluation
- Crossfeed
- Cyber Resilience Review
- & more

EI-ISAC Services

- Albert Sensors
- Malicious Domain Blocking and Reporting
- & more



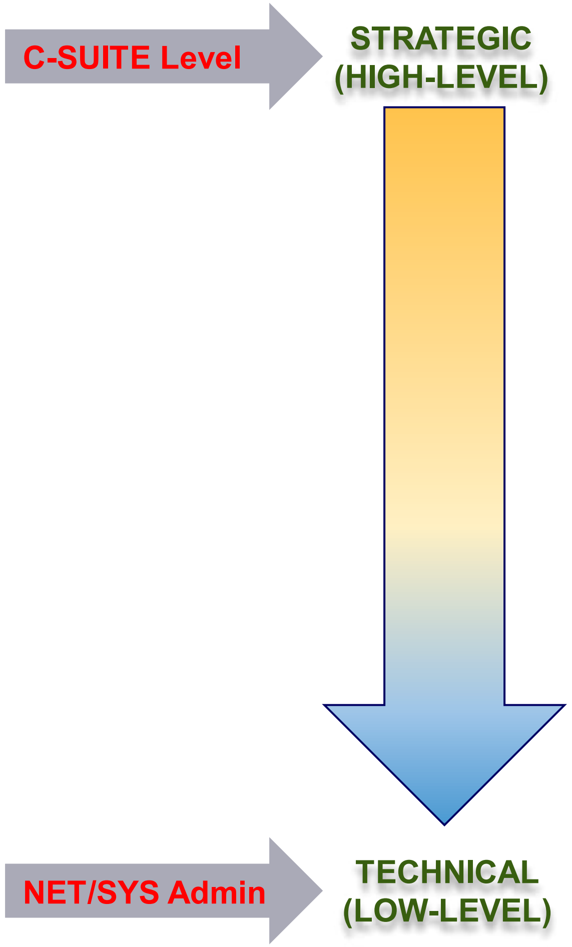
ELECTION INFRASTRUCTURE SECURITY RESOURCE GUIDE

Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

September 2020

Cybersecurity Assessments

- Cyber Resilience Review (CRR)
- External Dependencies Management (EDM)
- Cyber Infrastructure Survey (CIS)
- Cyber Security Evaluation Tool (CSET)
- Cyber Hygiene Services (Systems & Web)
- Phishing Campaign Assessment
- Validated Architecture Design Review (VADR)
- Remote Penetration Testing (RPT)
- Risk and Vulnerability Assessment (aka “Pen” Test)



Cyber Resilience Review (CRR)

- **Purpose:** Evaluate operational resilience and cybersecurity practices of **critical services.**

- **Delivery:** Either CSA-facilitated, or self-administered

- **Benefits:** Report detailing an organizations capability and maturity in security management, and gaps against NIST CSF

***Voluntary assessment** that is available at **no-cost** to requesting organizations*

External Dependencies Mgmt. Assessment

- **Purpose:** Evaluate the maturity and capacity of an entity’s external dependencies risk management across the following three areas:
  1. Relationship formation
  2. Relationship management and governance
  3. Service protection and sustainment

- **Delivery:** CSA-facilitated

- **Benefits:** Comprehensive report that provides stakeholders with the organization’s third-party risk management practices and capabilities options for improvements that includes peer performance comparisons.

Cyber Infrastructure Survey (CIS)

- **Purpose:** Evaluate security controls, cyber preparedness, overall resilience.
- **Delivery:** CSA-facilitated
- **Benefits:** Receive an interactive dashboard to support cybersecurity planning / resource allocation. The dashboard allows entities to:
  - See their results compared against other members of their critical infrastructure sectors.
  - Review their results in context of specific cyber and physical threat scenarios.
  - Dynamically adjust the status of in-place practices.

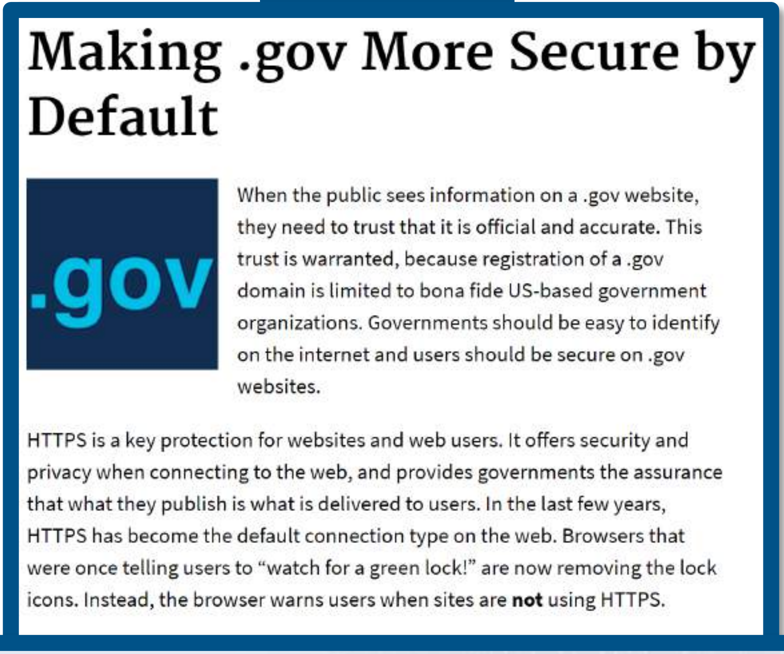
Cybersecurity Evaluation Tool

The Cyber Security Evaluation Tool (CSET®) is a no-cost, voluntary desktop stand-alone application that guides asset owners and operators through a systematic process to evaluate their operational technology (OT) and information technology (IT) network security practices. The tool helps organizations evaluate their cybersecurity posture against recognized standards and best practice recommendations in a systematic, disciplined, and repeatable manner

DOTGOV Top-Level Domain

DOTGOV Act of 2020

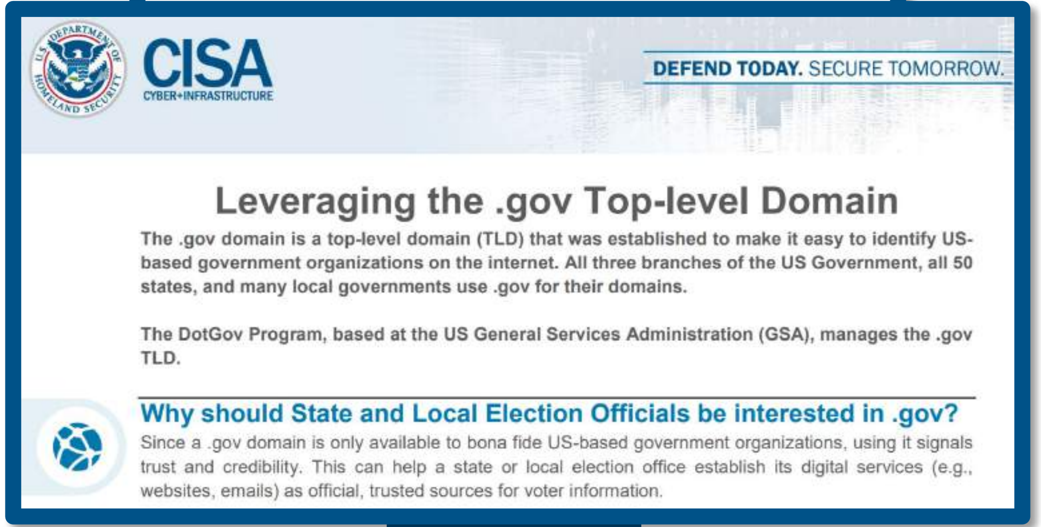
- **Responsibility** of administering official web domains shifted to CISA from GSA
- **Fees** become an allowable expense under the DHS Homeland Security Grant Program*
- Increased use of .gov domains will **improve cybersecurity and trust** in public services across the United States



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.



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.

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.**

Report to the SBE:

Report cybersecurity incidents and vulnerabilities:

☎ **(410) 269-2840**, (800) 222-8683 (Toll Free),
(800) 735-2258 (TTY)

✉ **info.sbe@maryland.gov**

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

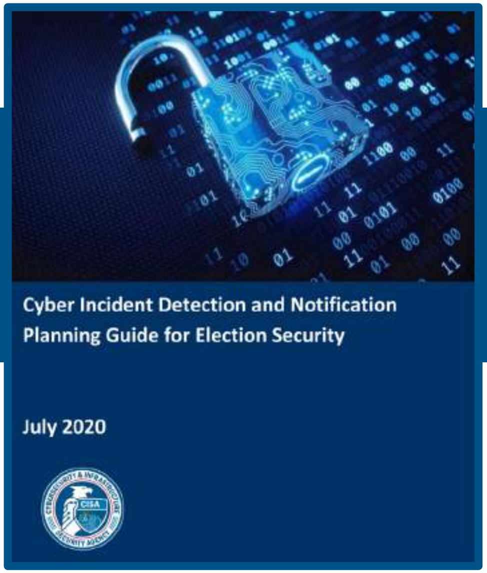
Incident Response

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

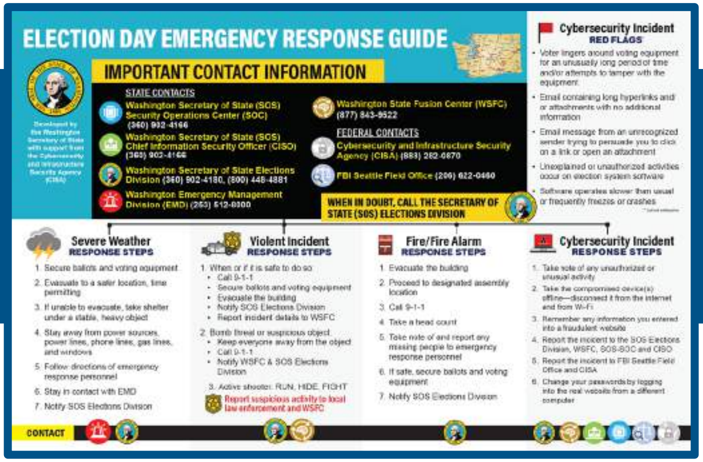


Cyber Incident Detection and Notification Planning Guide for Election Security

July 2020

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



ELECTION DAY EMERGENCY RESPONSE GUIDE

Developed by the Washington Secretary of State with support from the Cybersecurity and Infrastructure Security Agency (CISA)

IMPORTANT CONTACT INFORMATION

STATE CONTACTS

Washington Secretary of State (SOS) Security Operations Center (SOC) (360) 902-4166

Washington Secretary of State (SOS) Chief Information Security Officer (CISO) (360) 902-4166

Washington Secretary of State Elections Division (360) 902-4180, (800) 448-4881

Washington Emergency Management Division (EMD) (253) 512-8000

Washington State Fusion Center (WSFC) (877) 843-9522

FEDERAL CONTACTS

Cybersecurity and Infrastructure Security Agency (CISA) (888) 282-0870

FBI Seattle Field Office (206) 622-0460

WHEN IN DOUBT, CALL THE SECRETARY OF STATE (SOS) ELECTIONS DIVISION

Cybersecurity Incident RED FLAGS

- Voter lingers around voting equipment for an unusually long period of time and/or attempts to tamper with the equipment
- Email containing long hyperlinks and/or attachments with no additional information
- Email message from an unrecognized sender trying to persuade you to click on a link or open an attachment
- Unexplained or unauthorized activities occur on election system software
- Software operates slower than usual or frequently freezes or crashes

Severe Weather RESPONSE STEPS

1. Secure ballots and voting equipment
2. Evacuate to a safer location, time permitting
3. If unable to evacuate, take shelter under a stable, heavy object
4. Stay away from power sources, power lines, phone lines, gas lines, and windows
5. Follow directions of emergency response personnel
6. Stay in contact with EMD
7. Notify SOS Elections Division

Violent Incident RESPONSE STEPS

1. When or if it is safe to do so
   - Call 9-1-1
   - Secure ballots and voting equipment
   - Evacuate the building
   - Notify SOS Elections Division
   - Report incident details to WSFC
2. Bomb threat or suspicious object
   - Keep everyone away from the object
   - Call 9-1-1
   - Notify WSFC & SOS Elections Division
3. Active shooter: RUN, HIDE, FIGHT

Report suspicious activity to local law enforcement and WSFC

Fire/Fire Alarm RESPONSE STEPS

1. Evacuate the building
2. Proceed to designated assembly location
3. Call 9-1-1
4. Take a head count
5. Take note of and report any missing people to emergency response personnel
6. If safe, secure ballots and voting equipment
7. Notify SOS Elections Division

Cybersecurity Incident RESPONSE STEPS

1. Take note of any unauthorized or unusual activity
2. Take the compromised device(s) offline—disconnect it from the internet and from Wi-Fi
3. Remember any information you entered into a fraudulent website
4. Report the incident to the SOS Elections Division, WSFC, SOS-SOC and CISO
5. Report the incident to FBI Seattle Field Office and CISA
6. Change your passwords by logging into the real website from a different computer

CONTACT

Integrated CISA Watch

The mission of **CISA Central** is to serve as a national center for reporting of and mitigating communications and incidents.

- Provide alerts, warnings, common operating picture on cyber and communications incidents in real time to virtual and on-site partners
- Work 24X7 with partners to mitigate incidents (On-site partners include the DoD, FBI, Secret Service, Information Sharing and Analysis Centers (ISACs) and other DHS components and public partners)

Federal Cybersecurity Response

PPD 41 Highlights:

- Released in July 2016, sets forth the principles governing the Federal Government’s response to any cyber incident. Cybersecurity Act of 2018, landmark legislation that established CISA elevating their mission and authority within the Federal Government.
- Establishes the National Cyber Incident Response Plan and Defines cyber incident and significant cyber incident severity schema scoring.
- CISA National Cyber Incident Scoring System (reference below)

Reference CISA NCISS: https://us-cert.cisa.gov/CISA-National-Cyber-Incident-Scoring-System

Federal Cybersecurity Response—continued

- Established architecture for Federal Government response for to significant cyber incidents through concurrent lines of effort:
  - Asset Response: DHS Cybersecurity and Infrastructure Security Agency (CISA) through what is now CISA Central (Former NCCIC)
  - Threat Response: Department of Justice (DOJ) through the Federal Bureau of Investigation (FBI)
  - Intelligence Support: Office of the Director of National Intelligence (ODNI)
- Codified role and stand-up procedures for Cyber Unified Coordination Group (UCG)

Reference: CISA Insights & CISA.GOV

Federal Incident Response

- **Threat Response:** Attributing, pursuing, and disrupting malicious cyber actors and malicious cyber activity. Conducting criminal investigations and other actions to counter the malicious cyber activity.
- **Asset Response:** Protecting assets and mitigating vulnerabilities in the face of malicious cyber activity, reducing the impact to systems and data; strengthening, recovering, and restoring services; identifying other entities at risk; and assessing potential risk to broader community.

Key Federal Points of Contact

Threat Response

Federal Bureau of Investigation
855-292-3937 or cywatch@ic.fbi.gov

FBI Field Office Cyber Task Forces
http://www.fbi.gov/contact-us/field

Report cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity to FBI Field Office Cyber Task Forces

U.S. Secret Service
https://www.secretservice.gov/contact/field-offices

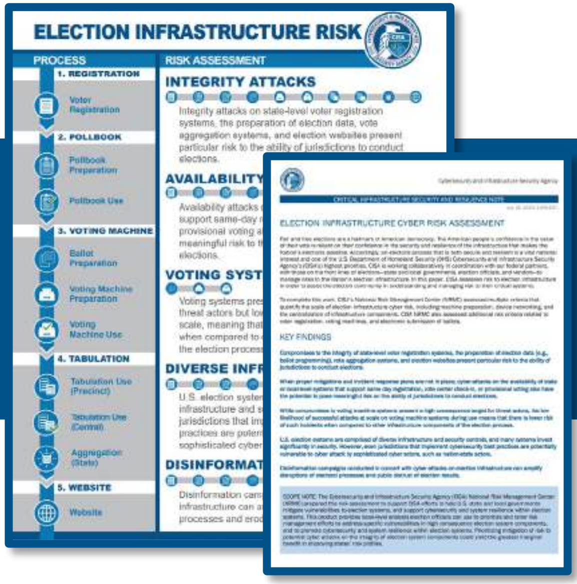
Asset Response

CISA Watch
888-282-0870 or central@cisa.dhs.gov

Report suspected or confirmed cyber incidents, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to further improve security.

FBI Internet Crime Complaint Center
https://www.ic3.gov/

Risk Analysis


ELECTION INFRASTRUCTURE RISK

PROCESS

RISK ASSESSMENT

1. REGISTRATION

2. POLLBOOK

3. VOTING MACHINE

4. TABULATION

5. WEBSITE

INTEGRITY ATTACKS

AVAILABILITY

VOTING SYST

DIVERSE INFR

DISINFORMAT

ELECTION INFRASTRUCTURE CYBER RISK ASSESSMENT

KEY FINDINGS

Election Infrastructure Cyber Risk Assessment

MAIL-IN VOTING RISK: INFRASTRUCTURE AND PROCESS

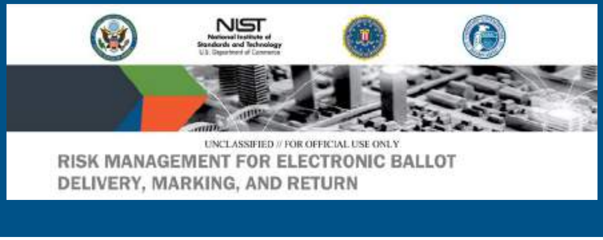
RISK

COMPENSATING CONTROLS

MAIL-IN VOTING IN 2020 INFRASTRUCTURE RISK ASSESSMENT

KEY FINDINGS

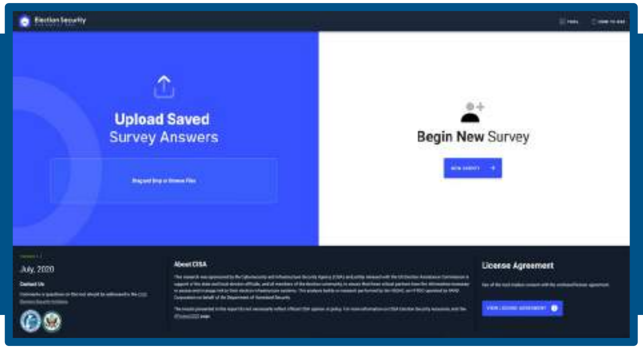
Mail-In Voting Risk Assessment


NIST

UNCLASSIFIED // FOR OFFICIAL USE ONLY

RISK MANAGEMENT FOR ELECTRONIC BALLOT DELIVERY, MARKING, AND RETURN

Risk Management for Electronic Ballot Delivery, Marking, and Return



Election Security Risk Profile Tool

What Election Infrastructure Stakeholders Can Do

Mitigate Internet Vulnerabilities in a Timely Manner. Mitigate all high and critical severity level vulnerabilities to internet-accessible systems within 30 days. Vulnerabilities with lower severity levels should be reviewed and mitigated within 60 days.

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.

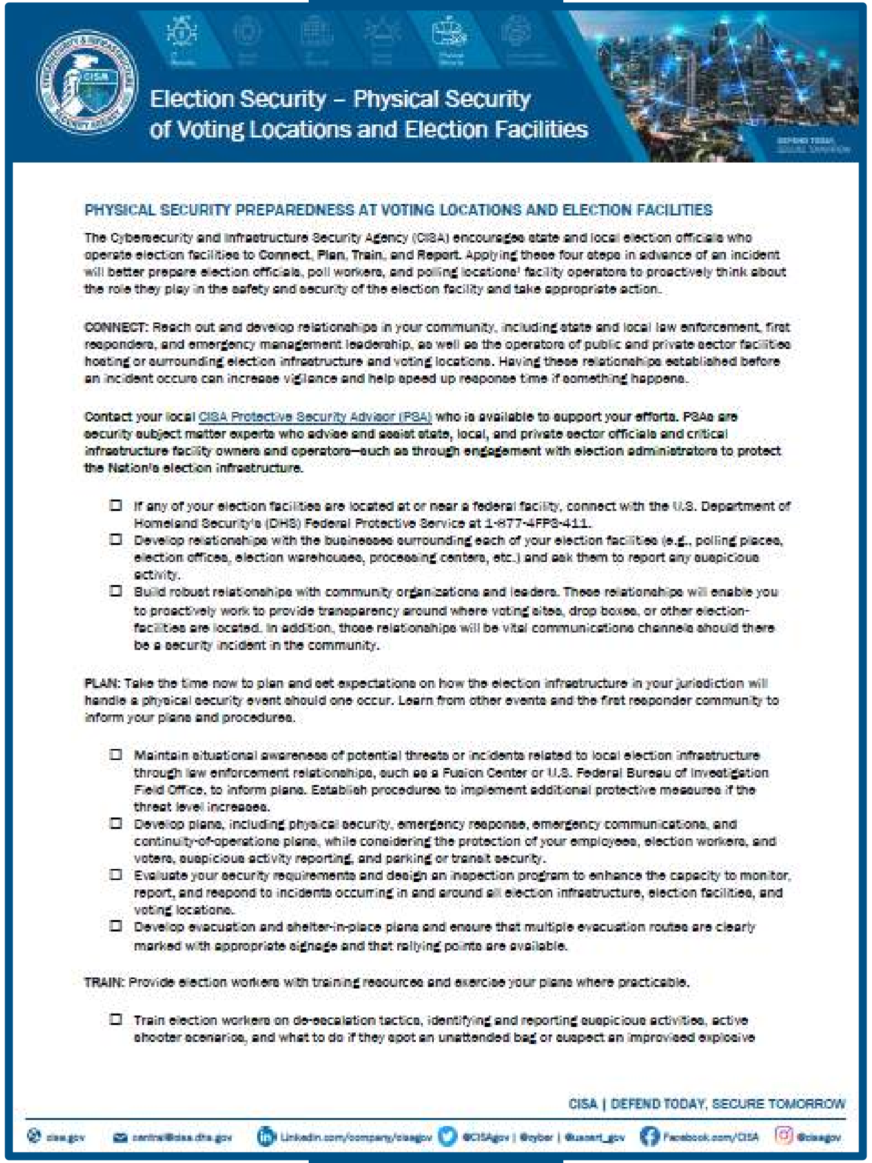
Replace Unmaintainable Equipment. Use equipment that is maintainable with current security patching. Exceptions should be minimized and isolated.

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.

Physical Security

CISA resources available to election officials

- Protective Security Advisors
- Physical Security Assessments
- Physical Security at Voting Locations and Election Facilities Guide
- Hometown Security page and resources: https://www.cisa.gov/hometown-security



Election Security – Physical Security of Voting Locations and Election Facilities

PHYSICAL SECURITY PREPAREDNESS AT VOTING LOCATIONS AND ELECTION FACILITIES

The Cybersecurity and Infrastructure Security Agency (CISA) encourages state and local election officials who operate election facilities to Connect, Plan, Train, and Report. Applying these four steps in advance of an incident will better prepare election officials, poll workers, and polling locations' facility operators to proactively think about the role they play in the safety and security of the election facility and take appropriate action.

CONNECT: Reach out and develop relationships in your community, including state and local law enforcement, first responders, and emergency management leadership, as well as the operators of public and private sector facilities hosting or surrounding election infrastructure and voting locations. Having these relationships established before an incident occurs can increase vigilance and help speed up response time if something happens.

Contact your local CISA Protective Security Advisor (PSA) who is available to support your efforts. PSAs are security subject matter experts who advise and assist state, local, and private sector officials and critical infrastructure facility owners and operators—such as through engagement with election administrators to protect the Nation's election infrastructure.

- ☐ If any of your election facilities are located at or near a federal facility, connect with the U.S. Department of Homeland Security's (DHS) Federal Protective Service at 1-877-4FPS-411.
- ☐ Develop relationships with the businesses surrounding each of your election facilities (e.g., polling places, election offices, election warehouses, processing centers, etc.) and ask them to report any suspicious activity.
- ☐ Build robust relationships with community organizations and leaders. These relationships will enable you to proactively work to provide transparency around where voting sites, drop boxes, or other election-facilities are located. In addition, those relationships will be vital communications channels should there be a security incident in the community.

PLAN: Take the time now to plan and set expectations on how the election infrastructure in your jurisdiction will handle a physical security event should one occur. Learn from other events and the first responder community to inform your plans and procedures.

- ☐ Maintain situational awareness of potential threats or incidents related to local election infrastructure through law enforcement relationships, such as a Fusion Center or U.S. Federal Bureau of Investigation Field Office, to inform plans. Establish procedures to implement additional protective measures if the threat level increases.
- ☐ Develop plans, including physical security, emergency response, emergency communications, and continuity-of-operations plans, while considering the protection of your employees, election workers, and voters, suspicious activity reporting, and parking or transit security.
- ☐ Evaluate your security requirements and design an inspection program to enhance the capacity to monitor, report, and respond to incidents occurring in and around all election infrastructure, election facilities, and voting locations.
- ☐ Develop evacuation and shelter-in-place plans and ensure that multiple evacuation routes are clearly marked with appropriate signage and that rallying points are available.

TRAIN: Provide election workers with training resources and exercise your plans where practicable.

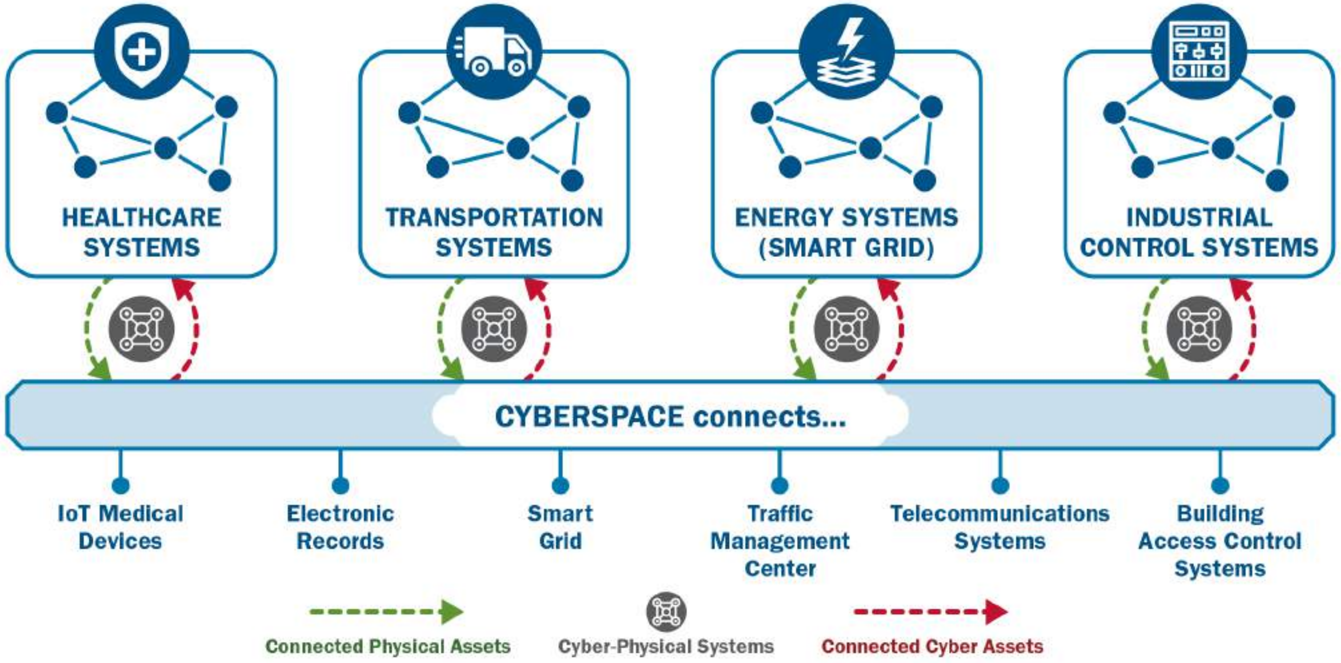
- ☐ Train election workers on de-escalation tactics, identifying and reporting suspicious activities, active shooter scenarios, and what to do if they spot an unattended bag or suspect an improvised explosive

CISA | DEFEND TODAY, SECURE TOMORROW

cisa.gov central@cisa.dhs.gov Linkedin.com/company/cisagov @CISAgov | @cyber | @uscert_gov Facebook.com/CISA @cisagov

Cyber-Physical Convergence

Today's threats are targeting physical and cyber assets through sophisticated hybrid attacks with potentially devastating impacts to data, property and physical safety. CISA defines convergence as formal collaboration between previously disjoined security functions.



HEALTHCARE SYSTEMS
TRANSPORTATION SYSTEMS
ENERGY SYSTEMS (SMART GRID)
INDUSTRIAL CONTROL SYSTEMS
CYBERSPACE connects...
IoT Medical Devices
Electronic Records
Smart Grid
Traffic Management Center
Telecommunications Systems
Building Access Control Systems
Connected Physical Assets
Cyber-Physical Systems
Connected Cyber Assets

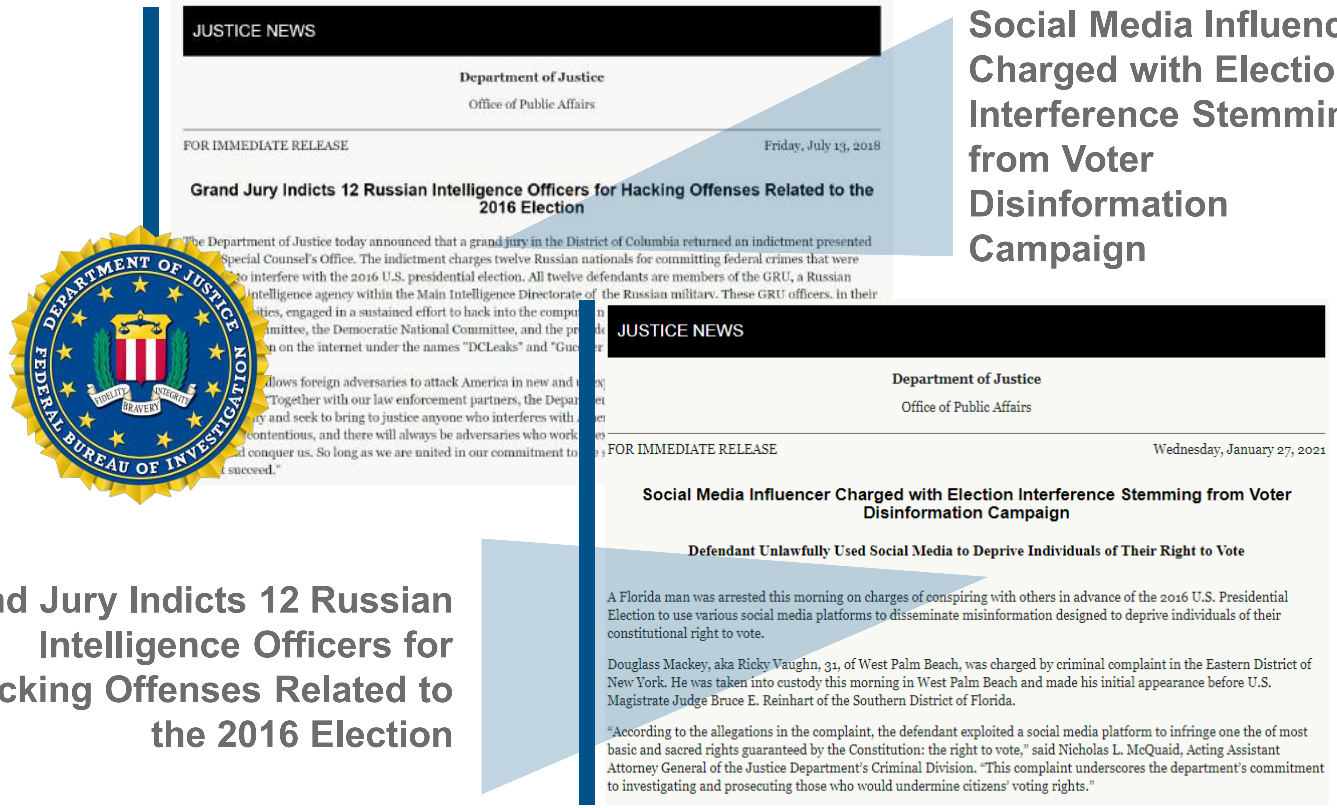
Source: https://www.cisa.gov/cybersecurity-and-physical-security-convergence

Countering Mis- Dis- and Malinformation: Supply

Social Media Companies

- CISA has relationships with ~10 social media/technology platforms
- CISA facilitates rapid, repetitive, and sustained information sharing between election officials and social media companies to address incidents
- In 2020, CISA routed ~150 reports of suspected mis/disinformation to the affected platform for remediation

Law Enforcement Partners



JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Friday, July 13, 2018

Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election

The Department of Justice today announced that a grand jury in the District of Columbia returned an indictment presented
Special Counsel's Office. The indictment charges twelve Russian nationals for committing federal crimes that were
to interfere with the 2016 U.S. presidential election. All twelve defendants are members of the GRU, a Russian
intelligence agency within the Main Intelligence Directorate of the Russian military. These GRU officers, in their
ities, engaged in a sustained effort to hack into the compu n
mittee, the Democratic National Committee, and the pr de
n on the internet under the names "DCLeaks" and "Guc r

llows foreign adversaries to attack America in new and ex
"Together with our law enforcement partners, the Depar e
y and seek to bring to justice anyone who interferes with e
contentious, and there will always be adversaries who work e
d conquer us. So long as we are united in our commitment to
t succeed."

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Wednesday, January 27, 2021

Social Media Influencer Charged with Election Interference Stemming from Voter Disinformation Campaign

Defendant Unlawfully Used Social Media to Deprive Individuals of Their Right to Vote

A Florida man was arrested this morning on charges of conspiring with others in advance of the 2016 U.S. Presidential Election to use various social media platforms to disseminate misinformation designed to deprive individuals of their constitutional right to vote.

Douglass Mackey, aka Ricky Vaughn, 31, of West Palm Beach, was charged by criminal complaint in the Eastern District of New York. He was taken into custody this morning in West Palm Beach and made his initial appearance before U.S. Magistrate Judge Bruce E. Reinhart of the Southern District of Florida.

"According to the allegations in the complaint, the defendant exploited a social media platform to infringe one the of most basic and sacred rights guaranteed by the Constitution: the right to vote," said Nicholas L. McQuaid, Acting Assistant Attorney General of the Justice Department's Criminal Division. "This complaint underscores the department's commitment to investigating and prosecuting those who would undermine citizens' voting rights."

Social Media Influencer Charged with Election Interference Stemming from Voter Disinformation Campaign

Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election

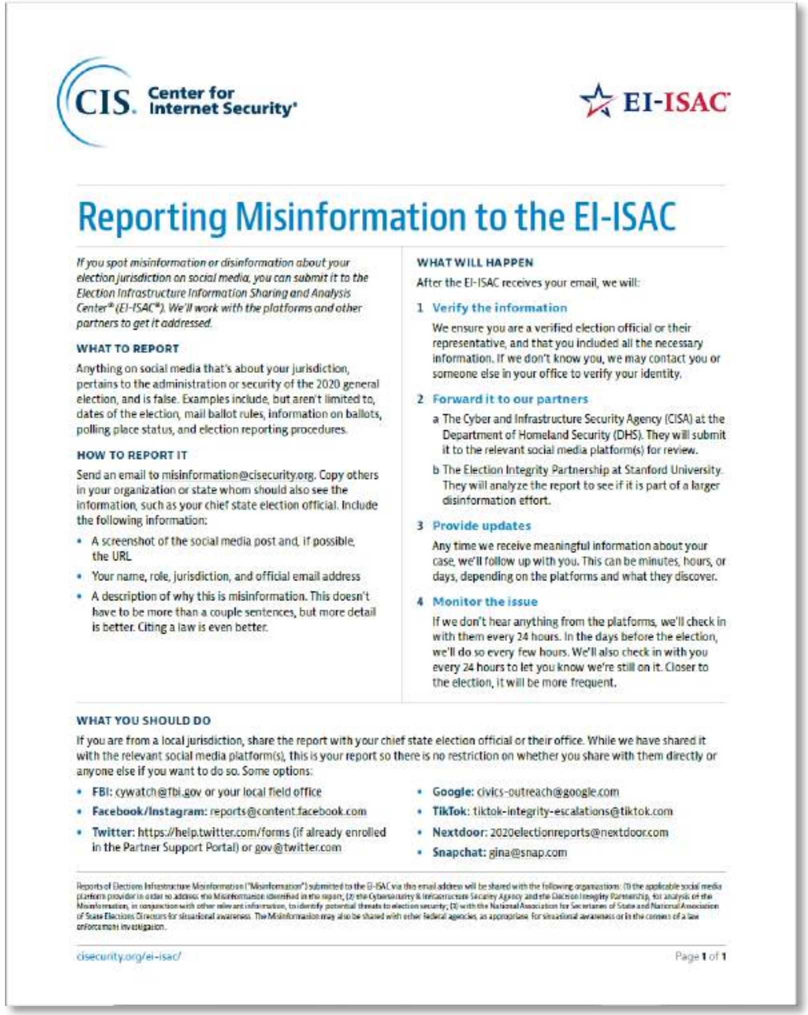
Countering MDM: Supply

Reporting MDM Incidents to EI-ISAC:

- **Email**: misinformation@cisecurity.org

Other options:

- **FBI**: cywatch@fbi.gov or your local field office
- **Facebook/Instagram**: reports@content.facebook.com
- **Twitter**: http://help.twitter.com/forms or gov@twitter.com
- **Google**: civics-outreach@google.com
- **TikTok**: tiktok-integrity-escalations@tiktok.com
- **Nextdoor**: 2020electionreports@nextdoor.com
- **Snapchat**: gina@snap.com



CIS. Center for Internet Security®

EI-ISAC®

Reporting Misinformation to the EI-ISAC

If you spot misinformation or disinformation about your election jurisdiction on social media, you can submit it to the Election Infrastructure Information Sharing and Analysis Center® (EI-ISAC®). We'll work with the platforms and other partners to get it addressed.

WHAT TO REPORT

Anything on social media that's about your jurisdiction, pertains to the administration or security of the 2020 general election, and is false. Examples include, but aren't limited to, dates of the election, mail ballot rules, information on ballots, polling place status, and election reporting procedures.

HOW TO REPORT IT

Send an email to misinformation@cisecurity.org. Copy others in your organization or state whom should also see the information, such as your chief state election official. Include the following information:

- A screenshot of the social media post and, if possible, the URL
- Your name, role, jurisdiction, and official email address
- A description of why this is misinformation. This doesn't have to be more than a couple sentences, but more detail is better. Citing a law is even better.

WHAT WILL HAPPEN

After the EI-ISAC receives your email, we will:

1 **Verify the information**

We ensure you are a verified election official or their representative, and that you included all the necessary information. If we don't know you, we may contact you or someone else in your office to verify your identity.

2 **Forward it to our partners**

a The Cyber and Infrastructure Security Agency (CISA) at the Department of Homeland Security (DHS). They will submit it to the relevant social media platform(s) for review.

b The Election Integrity Partnership at Stanford University. They will analyze the report to see if it is part of a larger disinformation effort.

3 **Provide updates**

Any time we receive meaningful information about your case, we'll follow up with you. This can be minutes, hours, or days, depending on the platforms and what they discover.

4 **Monitor the issue**

If we don't hear anything from the platforms, we'll check in with them every 24 hours. In the days before the election, we'll do so every few hours. We'll also check in with you every 24 hours to let you know we're still on it. Closer to the election, it will be more frequent.

WHAT YOU SHOULD DO

If you are from a local jurisdiction, share the report with your chief state election official or their office. While we have shared it with the relevant social media platform(s), this is your report so there is no restriction on whether you share with them directly or anyone else if you want to do so. Some options:

- **FBI:** cywatch@fbi.gov or your local field office
- **Facebook/Instagram:** reports@content.facebook.com
- **Twitter:** https://help.twitter.com/forms (if already enrolled in the Partner Support Portal) or gov@twitter.com
- **Google:** civics-outreach@google.com
- **TikTok:** tiktok-integrity-escalations@tiktok.com
- **Nextdoor:** 2020electionreports@nextdoor.com
- **Snapchat:** gina@snap.com

Reports of Elections Infrastructure Misinformation ("Misinformation") submitted to the EI-ISAC via this email address will be shared with the following organizations: (1) the applicable social media platform provider in order to address the Misinformation identified in the report; (2) the Cybersecurity & Infrastructure Security Agency and the Election Integrity Partnership, for analysis of the Misinformation, in conjunction with other relevant information, to identify potential threats to election security; (3) with the National Association for Secretaries of State and National Association of State Elections Directors for situational awareness. The Misinformation may also be shared with other Federal agencies, as appropriate, for situational awareness or in the context of a law enforcement investigation.

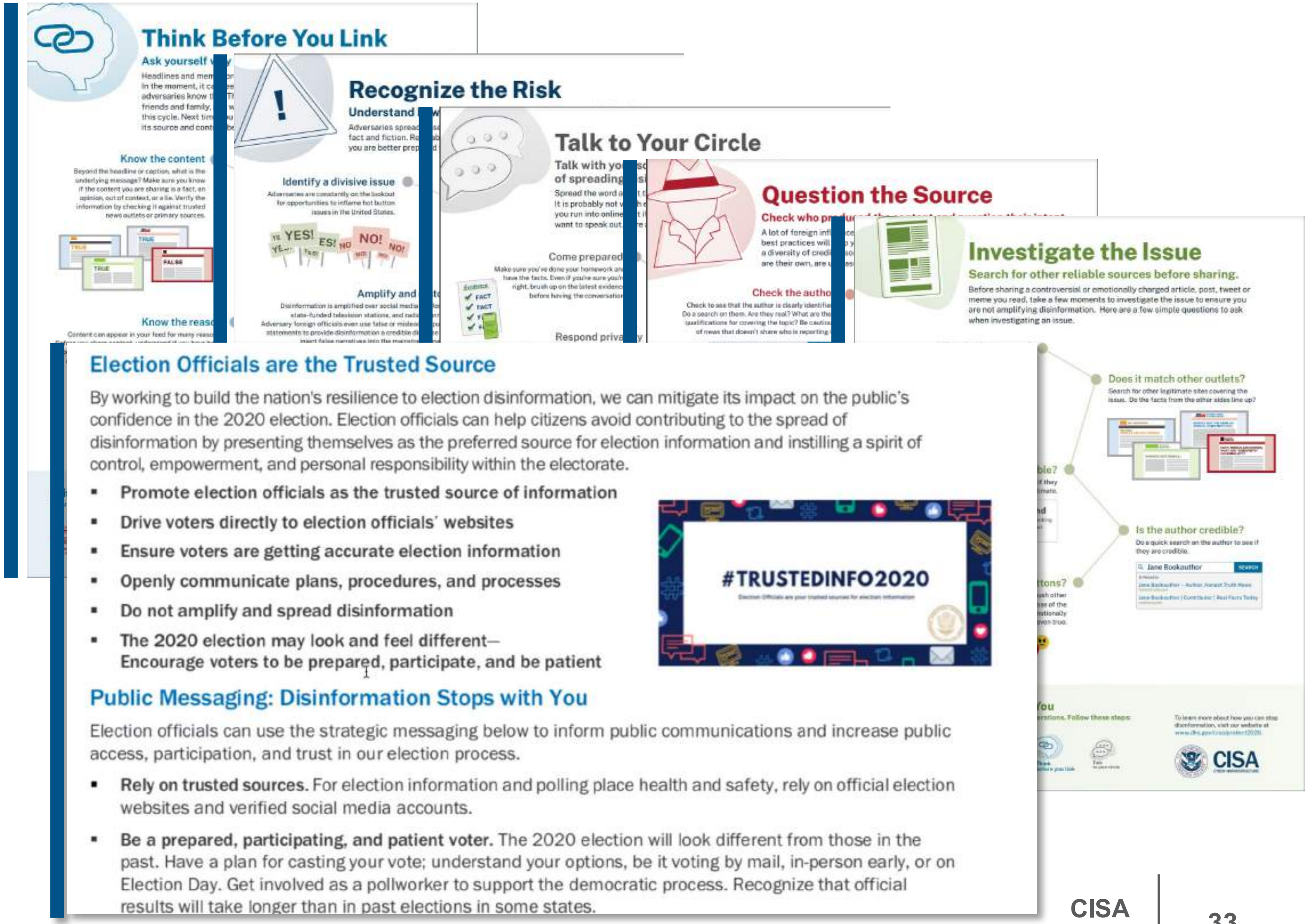
cisecurity.org/ei-isac/

Page 1 of 1

Countering MDM: Demand

Resources for Election Officials

- Disinformation Toolkit
- Disinformation Stops with You
- Think Before You Link
- Recognize the Risk
- Talk to Your Circle
- Question the Source
- Investigate the Issue
- Foreign Influence Taxonomy
- Social Media Bots



Think Before You Link

Recognize the Risk

Talk to Your Circle

Question the Source

Investigate the Issue

Search for other reliable sources before sharing.

Election Officials are the Trusted Source

By working to build the nation's resilience to election disinformation, we can mitigate its impact on the public's confidence in the 2020 election. Election officials can help citizens avoid contributing to the spread of disinformation by presenting themselves as the preferred source for election information and instilling a spirit of control, empowerment, and personal responsibility within the electorate.

- **Promote election officials as the trusted source of information**
- **Drive voters directly to election officials' websites**
- **Ensure voters are getting accurate election information**
- **Openly communicate plans, procedures, and processes**
- **Do not amplify and spread disinformation**
- **The 2020 election may look and feel different—Encourage voters to be prepared, participate, and be patient**

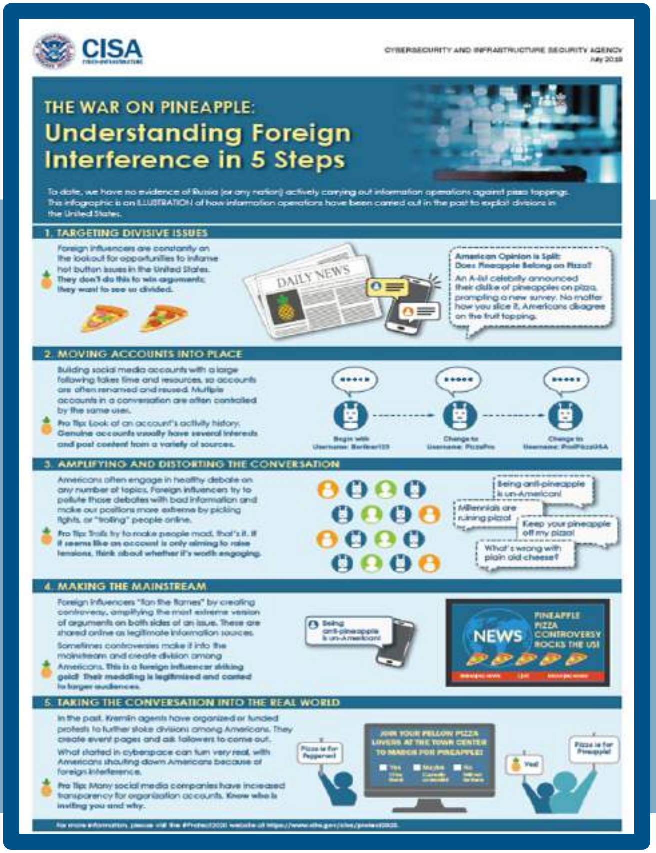
#TRUSTEDINFO2020

Public Messaging: Disinformation Stops with You

Election officials can use the strategic messaging below to inform public communications and increase public access, participation, and trust in our election process.

- **Rely on trusted sources.** For election information and polling place health and safety, rely on official election websites and verified social media accounts.
- **Be a prepared, participating, and patient voter.** The 2020 election will look different from those in the past. Have a plan for casting your vote; understand your options, be it voting by mail, in-person early, or on Election Day. Get involved as a pollworker to support the democratic process. Recognize that official results will take longer than in past elections in some states.

Countering MDM: Demand



CISA

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY
July 2019

THE WAR ON PINEAPPLE:
Understanding Foreign Interference in 5 Steps

To date, we have no evidence of Russia (or any nation) actively carrying out information operations against pizza toppings. This infographic is an ILLUSTRATION of how information operations have been carried out in the past to exploit divisions in the United States.

1. TARGETING DIVISIVE ISSUES

Foreign influencers are constantly on the lookout for opportunities to inflame hot button issues in the United States. **They don't do this to win arguments; they want to see us divided.**

American Opinion is Split: Does Pineapple Belong on Pizza?
An A-list celebrity announced their dislike of pineapples on pizza, prompting a new survey. No matter how you slice it, Americans disagree on the fruit topping.

2. MOVING ACCOUNTS INTO PLACE

Building social media accounts with a large following takes time and resources, so accounts are often renamed and reused. Multiple accounts in a conversation are often controlled by the same user.

Pro Tip: Look at an account's activity history. **Genuine accounts usually have several interests and post content from a variety of sources.**

Begin with Username: Berliner123
Change to Username: PizzaPro
Change to Username: ProPizzaUSA

3. AMPLIFYING AND DISTORTING THE CONVERSATION

Americans often engage in healthy debate on any number of topics. Foreign influencers try to pollute those debates with bad information and make our positions more extreme by picking fights, or "trolling" people online.

Pro Tip: Trolls try to make people mad, that's it. **If it seems like an account is only aiming to raise tensions, think about whether it's worth engaging.**

Being anti-pineapple is un-American!
Millennials are ruining pizza!
Keep your pineapple off my pizza!
What's wrong with plain old cheese?

4. MAKING THE MAINSTREAM

Foreign influencers "fan the flames" by creating controversy, amplifying the most extreme version of arguments on both sides of an issue. These are shared online as legitimate information sources.

Sometimes controversies make it into the mainstream and create division among Americans. **This is a foreign influencer striking gold! Their meddling is legitimized and carried to larger audiences.**

Being anti-pineapple is un-American!
NEWS
PINEAPPLE PIZZA CONTROVERSY ROCKS THE US!

5. TAKING THE CONVERSATION INTO THE REAL WORLD

In the past, Kremlin agents have organized or funded protests to further stoke divisions among Americans. They create event pages and ask followers to come out.

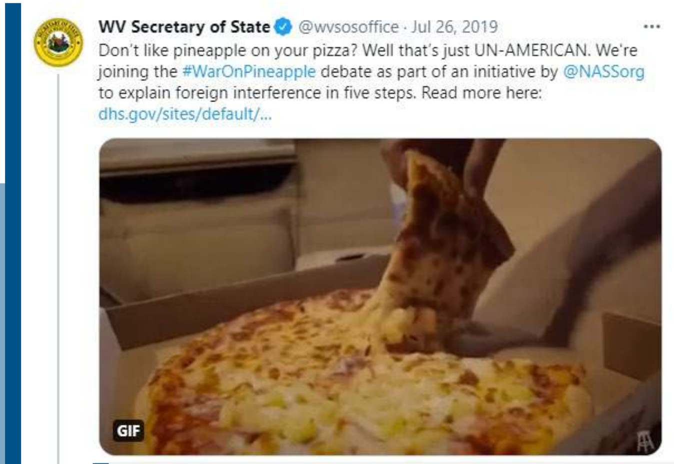
What started in cyberspace can turn very real, with Americans shouting down Americans because of foreign interference.

Pro Tip: Many social media companies have increased transparency for organization accounts. **Know who is inviting you and why.**

Pizza is for Pepperoni!
JOIN YOUR FELLOW PIZZA LOVERS AT THE TOWN CENTER TO MARCH FOR PINEAPPLE!
Yes
Maybe
No
Yes!
Pizza is for Pineapple!

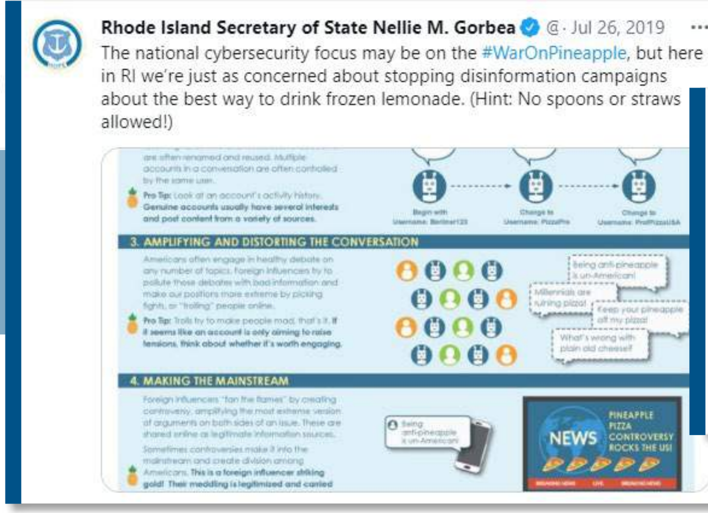
For more information, please visit the #Protect2020 website at https://www.dhs.gov/cisa/protect2020.

The War on Pineapple



WV Secretary of State @wvsosoffice · Jul 26, 2019

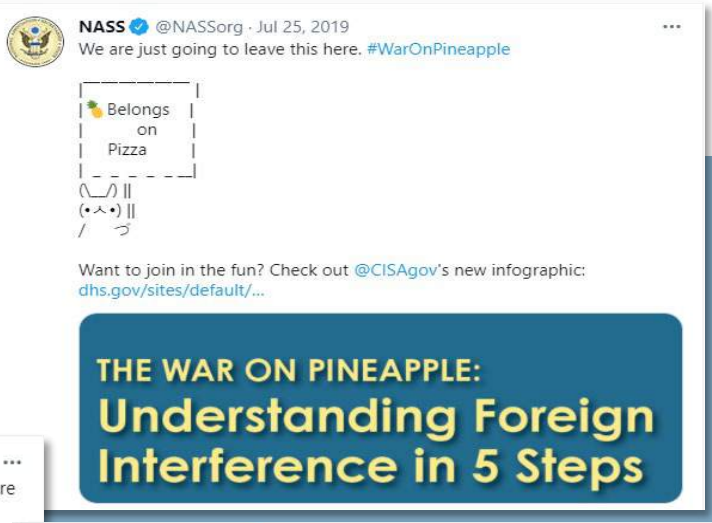
Don't like pineapple on your pizza? Well that's just UN-AMERICAN. We're joining the #WarOnPineapple debate as part of an initiative by @NASSorg to explain foreign interference in five steps. Read more here: dhs.gov/sites/default/...



Rhode Island Secretary of State Nellie M. Gorbea @ · Jul 26, 2019

The national cybersecurity focus may be on the #WarOnPineapple, but here in RI we're just as concerned about stopping disinformation campaigns about the best way to drink frozen lemonade. (Hint: No spoons or straws allowed!)

are often renamed and reused. Multiple accounts in a conversation are often controlled by the same user.
Pro Tip: Look at an account's activity history. Genuine accounts usually have several interests and post content from a variety of sources.
Begin with Username: Berliner123 · Change to Username: PizzaPro · Change to Username: ProPizzaUSA
3. AMPLIFYING AND DISTORTING THE CONVERSATION
Americans often engage in healthy debate on any number of topics. Foreign influencers try to pollute those debates with bad information and make our positions more extreme by picking fights, or "trolling" people online.
Pro Tip: Trolls try to make people mad, that's it. If it seems like an account is only aiming to raise tensions, think about whether it's worth engaging.
Being anti-pineapple is un-American! · Millennials are ruining pizza! · Keep your pineapple off my pizza! · What's wrong with plain old cheese?
4. MAKING THE MAINSTREAM
Foreign influencers "fan the flames" by creating controversy, amplifying the most extreme version of arguments on both sides of an issue. These are shared online as legitimate information sources.
Sometimes controversies make it into the mainstream and create division among Americans. This is a foreign influencer striking gold! Their meddling is legitimized and carried
Being anti-pineapple is un-American! · NEWS · PINEAPPLE PIZZA CONTROVERSY ROCKS THE US!



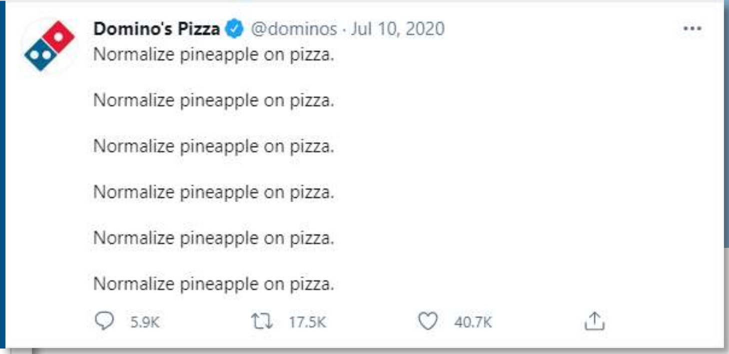
NASS @NASSorg · Jul 25, 2019

We are just going to leave this here. #WarOnPineapple

```
|‾‾‾‾‾‾‾‾‾‾‾‾|
| 🍍 Belongs  |
|     on      |
|   Pizza     |
| _ _ _ _ _ _|
(\__/) ||
(•ㅅ•) ||
/   づ
```

Want to join in the fun? Check out @CISAgov's new infographic: dhs.gov/sites/default/...

THE WAR ON PINEAPPLE:
Understanding Foreign Interference in 5 Steps



Domino's Pizza @dominos · Jul 10, 2020

Normalize pineapple on pizza.

Normalize pineapple on pizza.

Normalize pineapple on pizza.

Normalize pineapple on pizza.

Normalize pineapple on pizza.

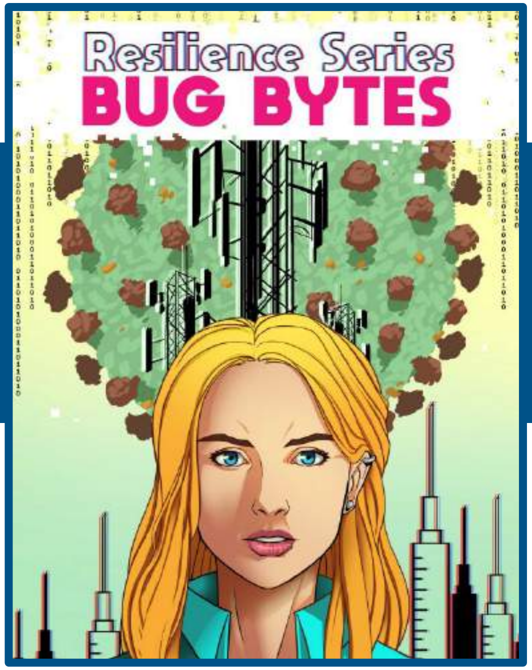
Normalize pineapple on pizza.

Countering MDM: Demand

Real Fake
Graphic Novel

Resilience Series
REAL FAKE
Commissioned by the Cybersecurity and Infrastructure Security Agency
Written by Clint Watts and Farid Haque

Bug Bytes
Graphic Novel



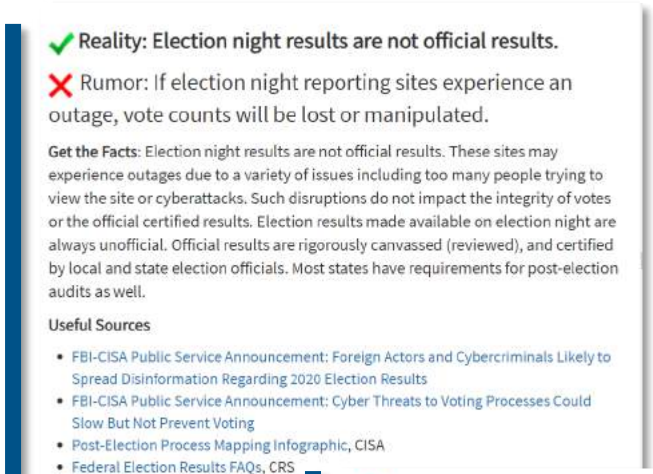
Breaking
Harmony Square

Countering MDM

Public Service Announcements

Rumor Control

- CISA stood up webpage designed to pre- and debunk common mis- and disinformation narratives and themes that related broadly to the security of election infrastructure and the related process.
- Preemptive debunking, or **pre-bunking**, is preemptively warning and exposing people to weakened doses of misinformation. This approach can help cultivate "mental antibodies" against MDM.



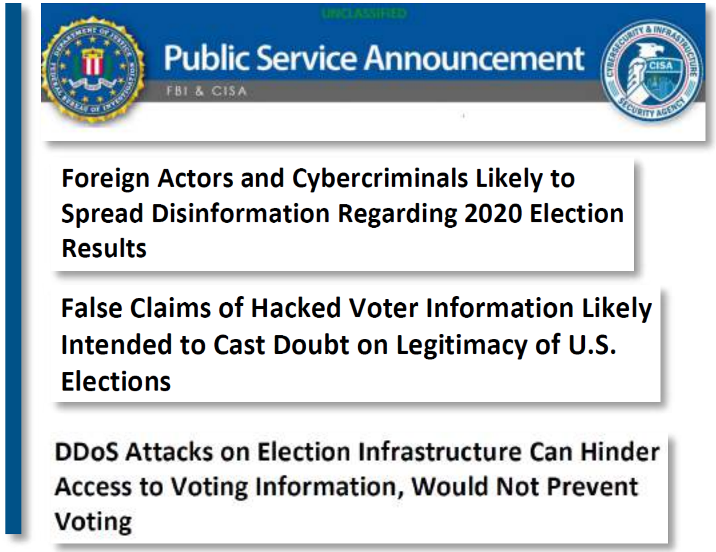
✓ Reality: Election night results are not official results.

✗ Rumor: If election night reporting sites experience an outage, vote counts will be lost or manipulated.

Get the Facts: Election night results are not official results. These sites may experience outages due to a variety of issues including too many people trying to view the site or cyberattacks. Such disruptions do not impact the integrity of votes or the official certified results. Election results made available on election night are always unofficial. Official results are rigorously canvassed (reviewed), and certified by local and state election officials. Most states have requirements for post-election audits as well.

Useful Sources

- FBI-CISA Public Service Announcement: Foreign Actors and Cybercriminals Likely to Spread Disinformation Regarding 2020 Election Results
- FBI-CISA Public Service Announcement: Cyber Threats to Voting Processes Could Slow But Not Prevent Voting
- Post-Election Process Mapping Infographic, CISA
- Federal Election Results FAQs, CRS
- Link directly to this rumor by using:



UNCLASSIFIED

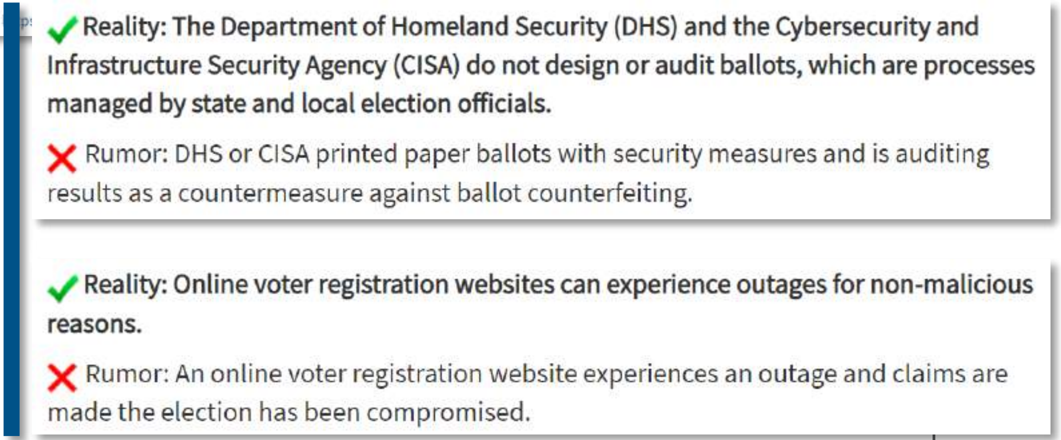
Public Service Announcement

FBI & CISA

Foreign Actors and Cybercriminals Likely to Spread Disinformation Regarding 2020 Election Results

False Claims of Hacked Voter Information Likely Intended to Cast Doubt on Legitimacy of U.S. Elections

DDoS Attacks on Election Infrastructure Can Hinder Access to Voting Information, Would Not Prevent Voting



✓ Reality: The Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA) do not design or audit ballots, which are processes managed by state and local election officials.

✗ Rumor: DHS or CISA printed paper ballots with security measures and is auditing results as a countermeasure against ballot counterfeiting.

✓ Reality: Online voter registration websites can experience outages for non-malicious reasons.

✗ Rumor: An online voter registration website experiences an outage and claims are made the election has been compromised.

Exercises and Training

Tabletop Exercises (TTX) and "Tabletop-In-A-Box"

ESI Training Offerings

- Elections Security Overview
- Building Trust through Secure Practices
- Phishing
- Ransomware

Federal Virtual Training Environment (FedVTE)

CISA
CYBER+INFRASTRUCTURE

ELECTIONS CYBER TABLETOP EXERCISE PACKAGE

Situation Manual

January 2020

Cybersecurity and Infrastructure Security Agency
Exercise Program

CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

BUILDING TRUST THROUGH SECURE PRACTICES

ELECTION SECURITY INITIATIVE
CISA

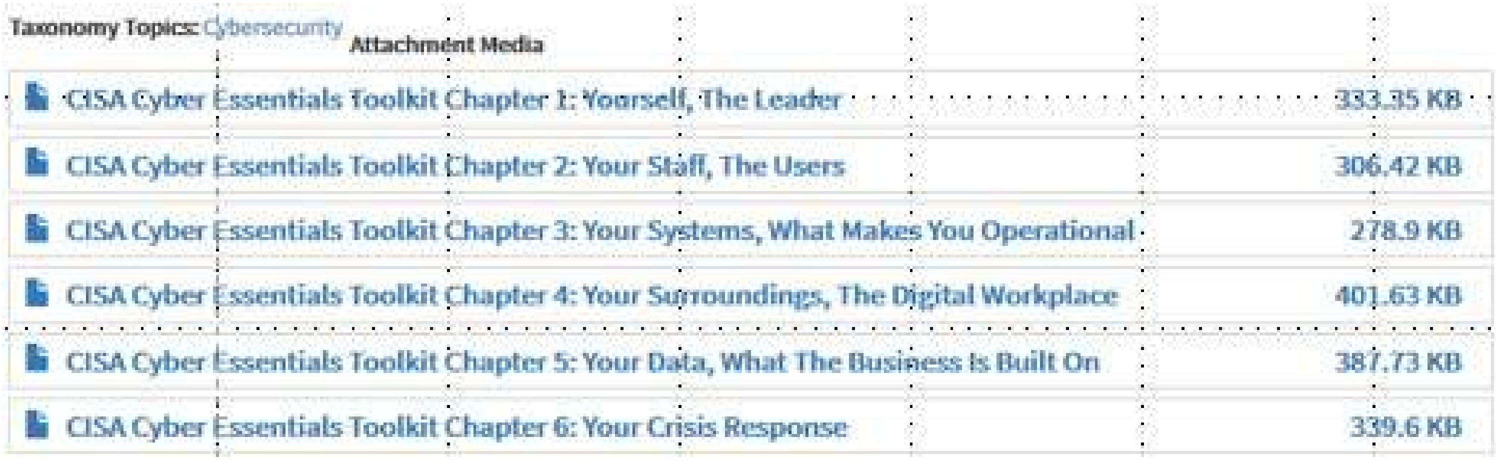
What Is Ransomware?

- 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 | 4

CISA Cyber Essentials

The Cyber Essentials Toolkit is a set of modules designed to break down the CISA Cyber Essentials into bite-sized actions for IT and C-suite leadership to work toward full implementation of each Cyber Essential. Each chapter focuses on recommended actions to build cyber readiness into the six interrelated aspects of an organizational culture of cyber readiness.

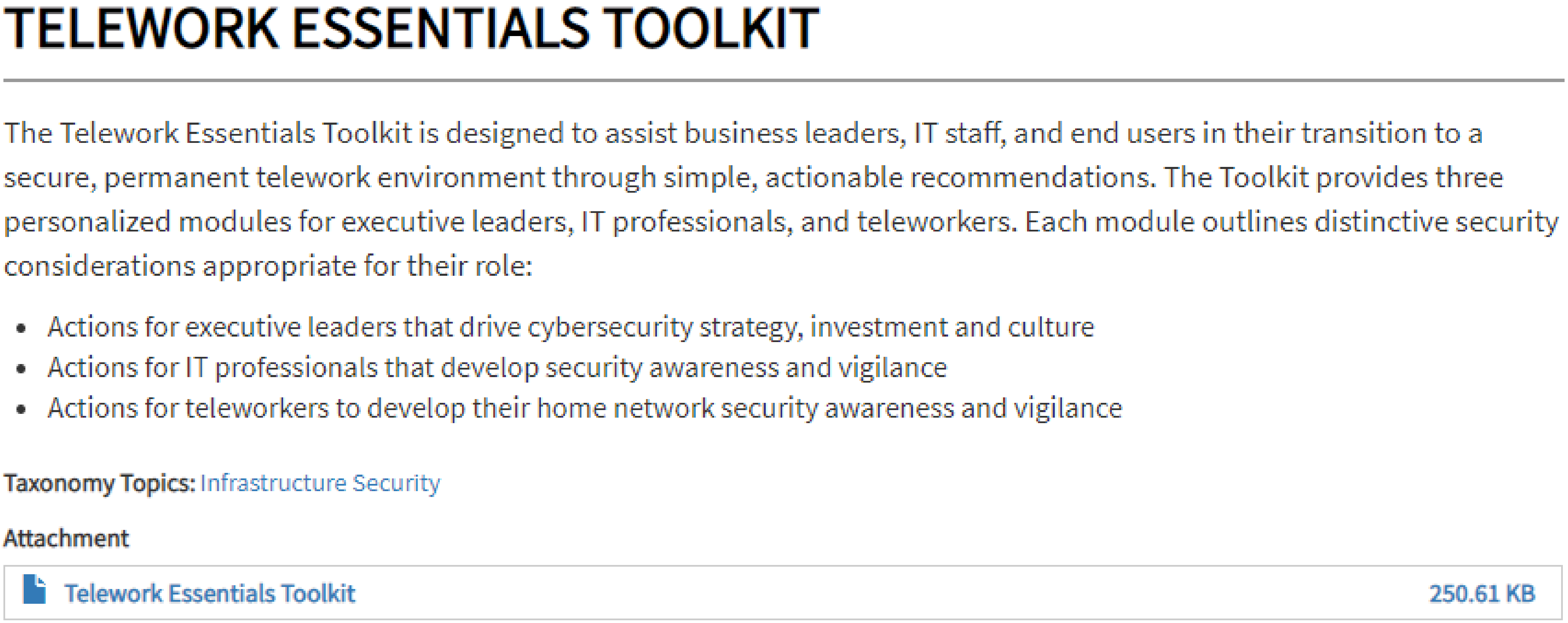


Taxonomy Topics: Cybersecurity

Attachment Media	
CISA Cyber Essentials Toolkit Chapter 1: Yourself, The Leader	333.35 KB
CISA Cyber Essentials Toolkit Chapter 2: Your Staff, The Users	306.42 KB
CISA Cyber Essentials Toolkit Chapter 3: Your Systems, What Makes You Operational	278.9 KB
CISA Cyber Essentials Toolkit Chapter 4: Your Surroundings, The Digital Workplace	401.63 KB
CISA Cyber Essentials Toolkit Chapter 5: Your Data, What The Business Is Built On	387.73 KB
CISA Cyber Essentials Toolkit Chapter 6: Your Crisis Response	339.6 KB

Source: https://www.cisa.gov/publication/cyber-essentials-toolkits

Telework Essentials Toolkit



TELEWORK ESSENTIALS TOOLKIT

The Telework Essentials Toolkit is designed to assist business leaders, IT staff, and end users in their transition to a secure, permanent telework environment through simple, actionable recommendations. The Toolkit provides three personalized modules for executive leaders, IT professionals, and teleworkers. Each module outlines distinctive security considerations appropriate for their role:

- Actions for executive leaders that drive cybersecurity strategy, investment and culture
- Actions for IT professionals that develop security awareness and vigilance
- Actions for teleworkers to develop their home network security awareness and vigilance

Taxonomy Topics: Infrastructure Security

Attachment

Telework Essentials Toolkit 250.61 KB

Source: https://www.cisa.gov/publication/telework-essentials-toolkit

CISA Mailing Lists and Feeds

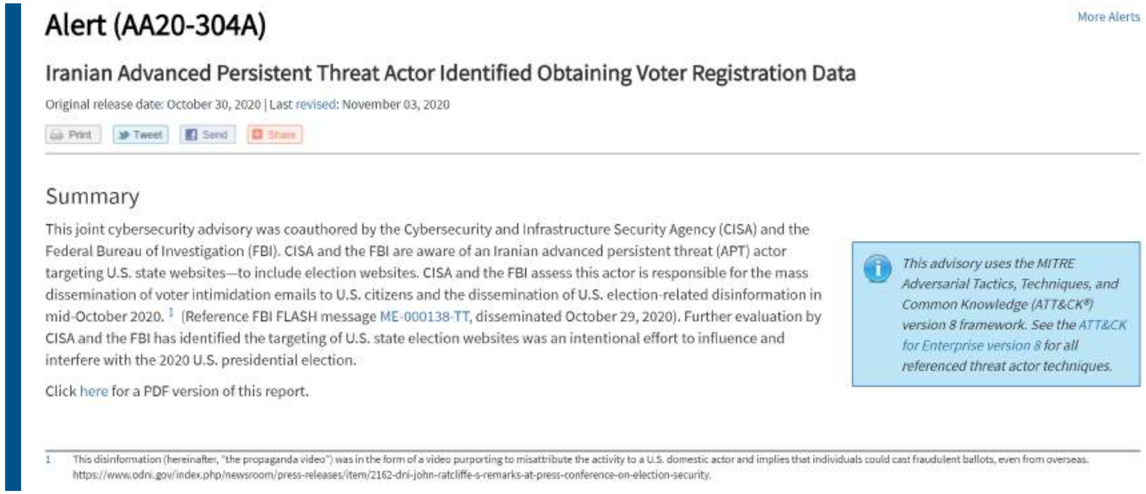
- **Alerts** — timely information about current security issues, vulnerabilities, and exploits
- **Analysis Reports** — in-depth analysis on new or evolving cyber threats
- **Bulletins** — weekly summaries of new vulnerabilities. Patch information is provided when available
- **Tips** — advice about common security issues for the general public
- **Current Activity** — up-to-date information about high-impact types of security activity affecting the community at large

Source: US-CERT.gov

What Election Infrastructure Stakeholders Can Do

- **Join the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)**
- **Share alerts with your IT managers and network defenders**
- **Connect with your CISA Cybersecurity and Protective Security Advisor (CSA/PSA)**
- **Sign up for CISA Services**
  - Vulnerability Scanning (CyHy)
  - Remote Penetration Testing (RPT)
  - DOTGOV Top-Level Domain (.gov TLD)
  - Cyber / Physical Security Assessment

Elections Infrastructure ISAC™



Alert (AA20-304A)

More Alerts

Iranian Advanced Persistent Threat Actor Identified Obtaining Voter Registration Data

Original release date: October 30, 2020 | Last revised: November 03, 2020

Summary

This joint cybersecurity advisory was coauthored by the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI). CISA and the FBI are aware of an Iranian advanced persistent threat (APT) actor targeting U.S. state websites—to include election websites. CISA and the FBI assess this actor is responsible for the mass dissemination of voter intimidation emails to U.S. citizens and the dissemination of U.S. election-related disinformation in mid-October 2020.[1] (Reference FBI FLASH message ME-000138-TT, disseminated October 29, 2020). Further evaluation by CISA and the FBI has identified the targeting of U.S. state election websites was an intentional effort to influence and interfere with the 2020 U.S. presidential election.

Click here for a PDF version of this report.

This advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) version 8 framework. See the ATT&CK for Enterprise version 8 for all referenced threat actor techniques.

[1] This disinformation (hereinafter, "the propaganda video") was in the form of a video purporting to misattribute the activity to a U.S. domestic actor and implies that individuals could cast fraudulent ballots, even from overseas. https://www.odni.gov/index.php/newsroom/press-releases/item/2162-dni-john-ratcliffe-s-remarks-at-press-conference-on-election-security.

What Election Infrastructure Stakeholders Can Do

Request a training or exercise

Connect us with your:

- Local authorities
- Private sector partners

Tell us what you need

Ryan Macias
SME Election Security Consultant
electionsecurity@hq.dhs.gov

Franco Cappa
Cybersecurity Advisor
franco.cappa@cisa.dhs.gov

Contact CISA:
Central@cisa.dhs.gov

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA

CISA

CYBER+INFRASTRUCTURE