CISA’S ELECTION SECURITY UPDATE
#Protect 2020

Overview

CISA works closely with the intelligence community, law enforcement, private sector, and others to ensure State and Local election officials have the information they need to defend election systems.

Recognizing that state and local election officials are on the front lines, CISA’s #Protect2020 initiative will engage officials from all 50 states, Washington, DC, and both major political parties to make sure that they are prepared.

We are working to make it harder for adversaries to compromise our systems and to enhance our resilience so that Americans know their votes will count— and will be counted correctly.

Guiding Principles

Customer Oriented
- Emphasizing stakeholder needs and delivering rapid solutions

Resilient
- Building stakeholder capabilities to resist malicious actors and recover rapidly from attacks

Adaptive
- Developing creative solutions to a rapidly evolving threat landscape

Vigilant
- Continuously monitoring threat trends and forecasting future vulnerabilities to provide timely services and information

Trustworthy
- Safeguarding the trust and information of our partners and the American public

Transparent
- Sharing information quickly and effectively
Current Events

- Election Infrastructure Government Coordinating Council and Election Infrastructure Sector Coordinating Council
  (Government Officials) (Private Sector)
- Executive Tabletop Exercise
- Open Source- Post-Election Audit Tool
  - [https://github.com/votingworks/arlo](https://github.com/votingworks/arlo)
- Incident Response Planning Guide
- Election TTX in a Box

### Scenario Overview Synopsis

<table>
<thead>
<tr>
<th>Option</th>
<th>Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td><strong>Vote-by-Mail Scenario</strong>: A threat actor attempts to interfere with vote-by-mail elections. After using phishing to penetrate state and local government systems, they attempt to redirect mailings, alter voter registration data, and deploy ransomware on networks to delay or discredit the election.</td>
</tr>
<tr>
<td>B</td>
<td><strong>Early Voting/Same Day or Election Day Registration Scenario</strong>: A threat actor targets state and local election officials with a spear phishing campaign and gains access to election assets. Once inside, they attempt to modify voter registration data as well as interfere with legitimate voter registration by promoting fake websites during the whole registration period. Threat actors also deface election websites and install ransomware on host machines at state and local election offices. By modifying voter registration data and impacting the printing of pollbooks, election officials are inundated with an increase of election day registration/same day registration requests.</td>
</tr>
<tr>
<td>C</td>
<td><strong>Election Day/Voting Machine Scenario</strong>: Threat actors deploy poisoned software updates in an attempt to access voting equipment and alter the vote count. In addition, threat actors conduct a social media campaign to encourage users to launch independent attacks against state and local government networks.</td>
</tr>
</tbody>
</table>
**What it is**

- **High-level snapshot**, highlighting what states and counties are doing to protect their elections
- **Fully Customizable Poster**, created in collaboration with each state based on the content and design needed to meet their needs
- **Applicable to State and/or County-level**, tailored to match how the state runs their elections

**What it is used for**

- Visual tool for briefing stakeholders (e.g., staff, leadership, regulators, voters) on existing security measures and priority actions
- Easy reference to find security POCs/resources
- Checklist of high-impact initiatives recommended by the SOS and CISA

---

**EXAMPLE**

**2020 Election Security Planning Snapshot**

**The State of Nebraska**

**2020 Election Initiatives**

**SAFEGUARDS / RESILIENCY MEASURES**

**THREAT MITIGATION**

**State Election Data**

- **Actual Size = 30” x 20”**

---

Presenter's Name
February 10, 2020
Election Day Emergency Response Guide

**What it is**
- Fully customized poster, highlighting important information for election day response
- Summary of incident types that can occur, such as weather, fire, violent incident, and cyber
- Overview of the response steps necessary and applicable contacts, providing the information needed to respond to the incident efficiently and effectively

**What it is used for**
- Provides elections officials with high-level response steps and emergency contact numbers for various types of incidents that could occur
- Resource on Election Day
- Training tool

**EXAMPLE**

**ELECTION DAY EMERGENCY RESPONSE GUIDE**

**IMPORTANT CONTACT INFORMATION**

**STATE CONTACTS**
- Nebraska Secretary of State (SOS), Elections Division (402) 297-8273
- Nebraska Office of the CIO (OCIO) (402) 471-3660
- Nebraska Emergency Management Agency (NEMA) (402) 471-7241
- Nebraska Information Analysis Center (NIAC) (402) 473-8640

**FEDERAL CONTACTS**
- National Cybersecurity and Communications Integration Center (NCCIC) (888) 209-0970
- Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) Security Operations Center (800) 787-4722
- FBI Omaha Field Office (402) 493-8689

**WHEN IN DOUBT, CALL THE SOS, ELECTIONS DIVISION**

**ELECTION DAY EMERGENCY RESPONSE GUIDE**

**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 NEMA.
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 NIAC.
2. Bomb threat or suspicious object:
   - Keep everyone away from the object.
   - Call 9-1-1.
   - Notify NIAC & SOS, Elections Division.
3. Active shooter: RUN, HIDE, FIGHT. Report suspicious activity to local law enforcement and NIAC.

**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. Disconnect compromised device from internet and from Wi-Fi.
3. Remember information entered into fraudulent website.
4. Report incident to SOS, Elections Division, OCIO, and NIAC.
5. Report incident to NCCIC, EI-ISAC, and FBI Omaha Field Office.
6. Change passwords by logging into new website from another device.

**Actual Size = 11” x 17”**
**Additional Variations**

**Wisconsin Example**

- **INTRODUCTION**
  - The Wisconsin 2020 Election Security Guide can help election officials in Wisconsin manage risks to the election system and improve election security. The guide provides support and resources to assist election officials in preparing for elections.

- **INITIATIVES CHECKLIST**
  - The Wisconsin 2020 Election Security Guide contains checklists and guidance to help election officials prepare for elections. The checklists are designed to help election officials ensure that their election systems are secure and that their election security measures are effective.

- **PROTECT**

- **DETECT**
  - The Wisconsin 2020 Election Security Guide provides guidance on how to detect security incidents and how to respond to them.

**West Virginia Example**

- **REPORT**

- **RESOURCES**
  - The West Virginia 2020 Election Security Guide contains resources for election officials to help them prepare for elections.

**Actual Size = Folds to 5.5” x 5.5”**

**Actual Size = 20” x 30”**
### Last Mile Statistics

<table>
<thead>
<tr>
<th>Count</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>States have received a completed Snapshot Poster</td>
</tr>
<tr>
<td>16</td>
<td>States have a received a draft Snapshot Poster*</td>
</tr>
<tr>
<td>36</td>
<td>Total States have received completed/draft Snapshot Posters</td>
</tr>
<tr>
<td>1,837</td>
<td>Local Election Offices received a completed Snapshot Poster</td>
</tr>
<tr>
<td>4,145</td>
<td>Local Election Offices pending receipt of a completed Snapshot Poster*</td>
</tr>
<tr>
<td>5,982</td>
<td>Total Local Election Offices received or pending Snapshot Posters</td>
</tr>
</tbody>
</table>

*Excluding the 8 States updating 2018 version

Updated as of January 28, 2020

Request yours…

Email: [ElectionTaskForce@cisa.dhs.gov](mailto:ElectionTaskForce@cisa.dhs.gov)
Private Sector Versions

What it is

- This accordion style “quad” fold product is an 8-panel brochure deliverable developed with election vendors.
- Customized for and by Sector Coordinating Council members to communicate security measures both internally and to third-party partners.

What it is used for

- Vendor employees and third-party providers use it to inform and train employees and third-party providers on current and recommended security measures and available CISA resources.
- Vendor’s can provide the guide to their customers to inform them of security measures and actions the vendor and third-parties are taking to secure election infrastructure, products, services, and customer data.
CISA’s Countering Foreign influence Approach

- Adversary TTPs
- Narratives: Likely and Emerging
- Target Audience

- Message impact
- Channel effectiveness
- Target Audience response

- Build awareness of risk
- Provide “pre-bunk” messaging

Identify

Mitigate
- Rapidly distribute messaging
- Share incident information

Inoculate

Quantify
Existing Products: War on Pineapple
Existing Product: Disinformation Stops with You

Disinformation Stops With You
You have the power to stop foreign influence operations.

Recognize the risk

Understand how foreign actors try to affect behavior.

Foreign actors might build an audience by starting or joining groups and spreading entertaining, non-controversial content. Eventually, they sprinkle in disinformation and steer followers to more extreme positions. The same actor will do this in many groups and pit them against each other.

Question the source

Check who produced the content and question their intent.

Foreign actors can spend a lot of money to make disinformation seem like entertainment or news. U.S. laws require such agents to disclose their relation to foreign governments. Look for those disclosures and think about what slant that relationship might put on how they report before accepting it as truth or linking to it online.

Investigate the issue

Search for other reliable sources before sharing.

Do a quick search for other reliable sources before sharing a controversial or emotionally charged article, post, tweet, or meme you read. Studies show that being well informed requires getting information from many places. If it isn’t from a credible source or if you can’t find a second reliable source, don’t share it.

Think before you link

Ask yourself why you’re sharing—and let your emotions cool.

Take a moment before sharing a link, email, or other message. Disinformation is designed to make you feel angry, shocked, or smug - always ask yourself why you’re sharing first. Are you posting to improve the conversation? Taking no action can be the best way to improve a discussion and thwart disinformation.

Talk to your circle

Talk with your social circle about the risks of spreading disinformation.

It’s probably not worth engaging with every piece of disinformation, but if you are concerned with its spread you may want to speak out. Share what you know about the risks of spreading disinformation and how you handle it. Confronting with emotion may backfire, so when possible, combine humor with facts.

To learn more about how you can stop disinformation, visit our website at www.dhs.gov/cisa/protect2020.
Existing Products Available

- Recognize the Risk
- Question the Source
- Investigate the Issue
- Think Before You Link
- Talk to Your Circle
- Foreign Interference Taxonomy
- Case Study – U.S. Energy Market
- CFI Frequently Asked Questions

Coming Soon – Animated Video
The core goal of this classic awareness campaign is to build the public's resilience, increase confidence in the 2020 Election, and inoculate the American people against disinformation during the Election cycle.

1. Create broad public awareness of disinformation and how to recognize it.
2. Reduce public engagement with disinformation by seeding attitudinal and behavioral changes.
3. Instill a spirit of control, empowerment, and personal responsibility.
4. Create an environment of trust, transparency, and increased confidence in election security and the election process among the American people.
5. Through key local and state partnerships, empower the public with accurate, practical information about the 2020 Election cycle (registration and voting day “know-before-you-go” facts to reduce confusion and uncertainty).
Tactical Considerations

Potential Tactics for Audience Engagement:

- **A range of tailored/customized products** such as toolkits, splash pages, links, collateral, fact sheets, social media posts, etc. that can be customized and co-branded with partners, talking points, and “storytelling scripts” for state/local and third-party organizations that they will leverage.

- **A full suite of materials and content for external and public affairs**, press, PR, and media opportunities.

- **Collateral for government facilities** such as posters, bulletin board collateral, intranet banners (example: DHS Connect’s homepage scroll) and other high-visibility real estate (via GSA) – consider an online game for DHS employees.

- **Non-paid media opportunities** such as social media campaigns, and guerilla channels, including “third spaces,” community/civic/digital forums where people are online, discussing issues and are virtually or physically gathered: libraries, airports, mass transit, coffee shops, festivals, community centers, and universities.

- **Digital paid-media campaign** and test creative executions and placement, timed to align with key Election year events.

- **A mix of private sector, corporate “vehicles”** for messaging and content such as internal communications and training partnerships with companies, HR and CSR entities within business, Chambers of Commerce, advisory boards, coordinating councils, and industry organization that influence business and employees.

- **2 to 3 high-impact/PR buzz/media interest opportunities** (example: Spy Museum sponsorship, McDonald’s trays, and opportunities for storyline/plotline placements in mass media and popular culture.)
Empowering voters with information:
- Here’s how to identify bad information. How does it work? How does it manipulate you?
- Here’s how to find accurate information
- Here’s how to model good behavior

Empowering voters with positive strategies for dealing with bad information:
- Ignore it
- Think before you share or engage
- Giving more attention to bad information is like giving oxygen to a fire

Bad information from foreign actors hurts our election processes:
- It spreads confusion
- It spreads mistrust
- Bad actors who spread bad information are not on anyone’s “side” and especially not yours – confusion and mistrust are their only goals

You can have confidence in our election processes—here’s why.
To learn more about foreign influence and how you can make a difference, visit [www.cisa.gov/protect2020](http://www.cisa.gov/protect2020)