CISA
CYBER+INFRASTRUCTURE

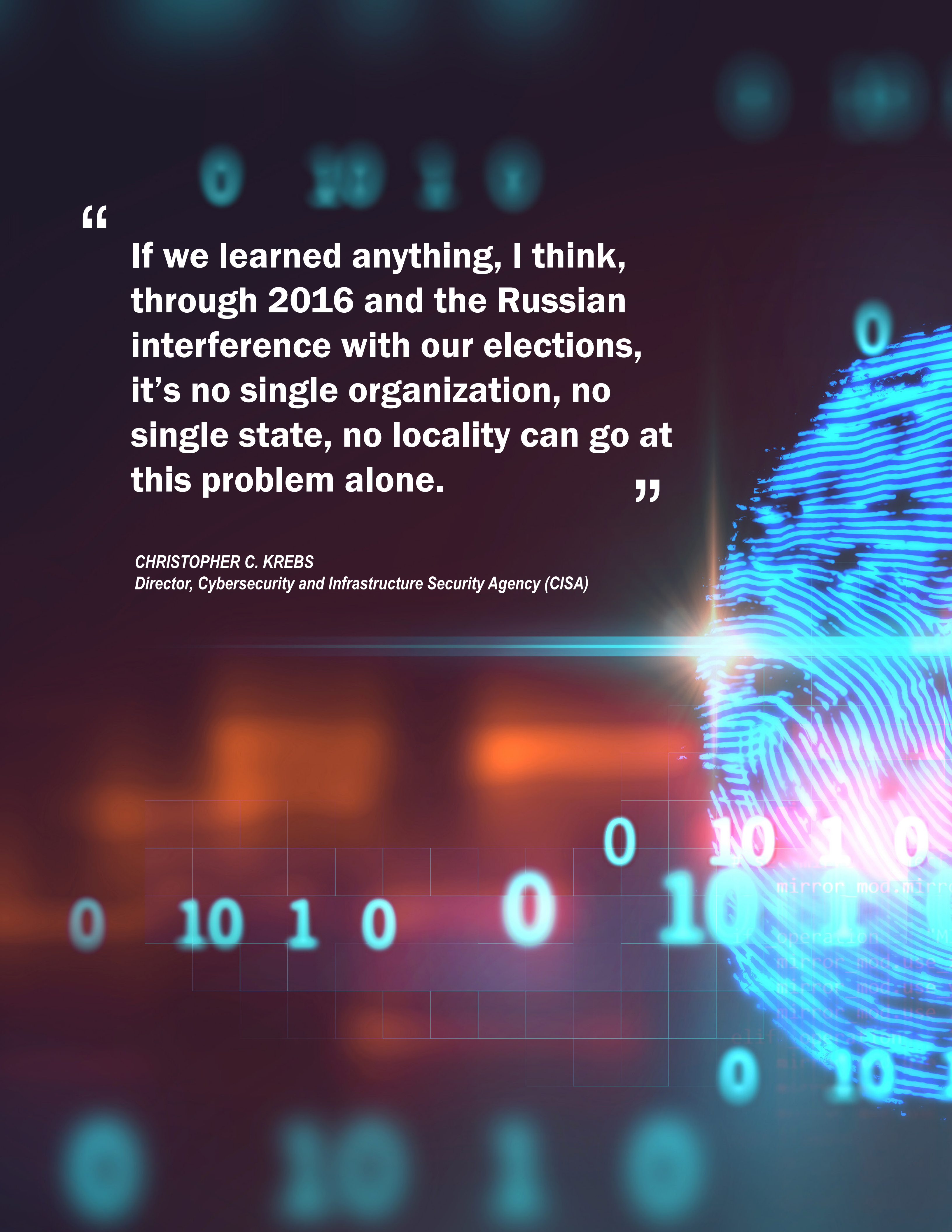
# #Protect2020 Strategic Plan

FEBRUARY2020

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

> **“If we learned anything, I think, through 2016 and the Russian interference with our elections, it’s no single organization, no single state, no locality can go at this problem alone.”**

*CHRISTOPHER C. KREBS*
*Director, Cybersecurity and Infrastructure Security Agency (CISA)*



# CONTENTS

# Message From the Director

CHRISTOPHER C. KREBS
*Director, Cybersecurity and Infrastructure Security Agency (CISA)*

Election security is a top priority for the U.S. Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA). As the lead federal agency responsible for securing the Nation's elections infrastructure, CISA works closely with the intelligence community, law enforcement officials, private sector partners, and others across the Federal Government to ensure we are doing everything possible to defend our electoral systems. But this needs to be a whole of nation effort. State and local election officials are on the front lines, and the role of the Federal Government is to make sure that they are prepared.

Ultimately, CISA's efforts depend on the trust and cooperation of state and local officials. Those relationships are strong and growing stronger. CISA's #Protect2020 initiative will engage officials from all fifty states, District of Columbia, and partisan organizations. 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

# Strategic Planning Overview

### CISA Strategic Intent

Introduces the vision and operational priorities for CISA, and establishes a common framework of goals and high-level outcomes

### #Protect 2020 Strategic Plan

Defines lines of effort and objectives for achieving election security mission to secure election infrastructure ahead of the 2020 election cycle

### CISA 2020 Election Security Operational Plan

Describes key organizational functions, processes, and resources employed to carry out the CISA mission

## Vision

Secure and resilient elections trusted by all Americans

## Mission

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

> **“There’s no question that our election process is more resilient and secure than it was in 2016, and heading into 2020 it will certainly be more secure than it was in 2018.”**
>
> ***Matt Masterson***
> *Election Security Initiative,*
> *Senior Cybersecurity Advisor*

### Vigilant

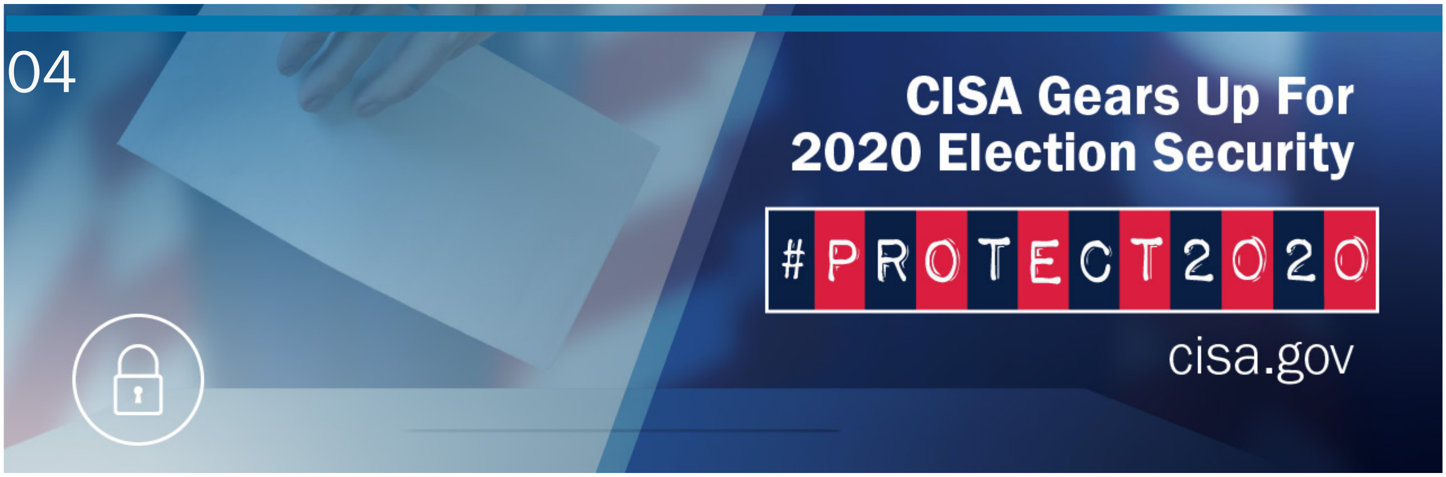
Continuously monitoring threat trends and forecasting future vulnerabilities to provide timely services and information

### Trustworthy

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

### Transparent

Sharing information quickly and effectively



# Background & Authority

In January 2017, DHS designated the infrastructure used to administer the Nation's elections as critical infrastructure. This designation recognizes that the United States' election infrastructure is of such vital importance to the American way of life that its incapacitation or destruction would have a devastating effect on the country. It gave federal agencies authority to assist in election security, but strictly in a supporting role. Under the Constitution, the responsibility for carrying out elections rests with state and local officials.

The President directed DHS to lead federal efforts to protect election infrastructure. DHS provides voluntary assistance and support to state and local officials in the form of advice, intelligence, technical support, and incident response planning—with the ultimate goal of building a more resilient, redundant, and secure election enterprise.

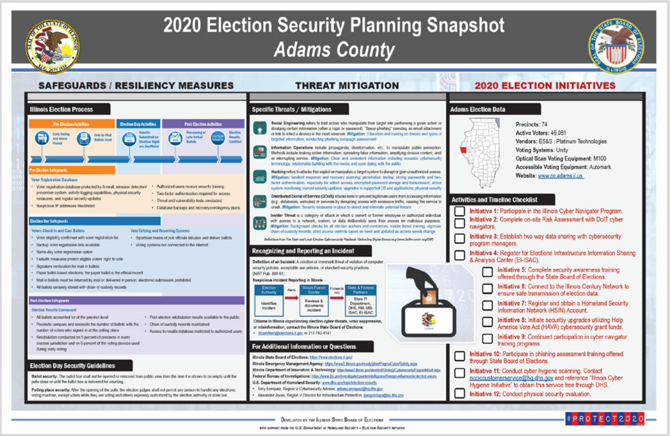
During the 2018 midterm Election cycle, DHS established the Election Task Force (ETF) and the Countering Foreign Influence Task Force (CFITF) to coordinate federal support to the election community. ETF and CFITF have now been institutionalized as the Election Security Initiative (ESI) within CISA. CISA works in coordination with various federal partners, such as DHS' Office of Intelligence and Analysis (I&A) and the Federal Bureau of Investigation (FBI), as well as non-federal election stakeholders.

Through #Protect2020, CISA leverages a wide range of offerings and services to build outreach programs and engage local election officials in the over 8,000 election jurisdictions across the country. CISA builds these crucial relationships within the election community by supporting election officials in their efforts to identify and plan for potential vulnerabilities to elections infrastructure ahead of and during the 2020 election cycle. CISA engages political campaigns by supporting the development of non-partisan informational products and conducting voluntary assessments, partners with the private sector to collaborate on best practices and vendor security, and works towards raising public awareness about foreign interference efforts.

An example of a successful direct engagement with state officials is CISA's Last Mile Project, featured on the following page. Launched in 2018, the Last Mile effort creates and distributes election security products to various stakeholders, tailoring the products to stakeholder needs and priorities. Fifteen states have worked with CISA to complete customized Last Mile products that have been distributed to over 1,000 jurisdictions. Officials from 20 additional states have already expressed interest in Last Mile products for the 2020 elections.

# CISA #Protect2020
# “The Last Mile” Products

Thousands of local jurisdictions, vendors, and political campaigns make up the majority of the U.S. elections stakeholder community, and together represent the biggest opportunities and vulnerabilities for election security. The independence and resource disparity among these entities create significant challenges to information sharing and implementation of best practices. Engaging these local stakeholders and the voters they serve represents the “Last Mile” in reducing risks to election security. CISA’s Last Mile products are scalable, customizable tools that local stakeholders can use immediately to improve security and awareness of additional services available. These products aim to strengthen the relationships among national, state, and local partners, which are essential for effective information sharing and continual engagement on critical election security issues.



2020 Election Security Planning Snapshot
*Adams County*

SAFEGUARDS / RESILIENCY MEASURES

Illinois Election Process

Pre-Election Activities
Early Voting and Grace Period
Vote by Mail Ballots Sent
Election Day Activities
Results Submitted on Election Night are Unofficial
Post-Election Activities
Processing of Late Arrival Ballots
Election Results Certified

Pre-Election Safeguards

Voter Registration Database

- Voter registration database protected by firewall, intrusion detection/ prevention system, activity logging capabilities, physical security measures, and regular security updates
- Suspicious IP addresses blacklisted
- Authorized users receive security training
- Two-factor authentication required for access
- Threat and vulnerability tests conducted
- Database backups and recovery/contingency plans

Election Day Safeguards

Voters Check In and Cast Ballots

- Voter eligibility confirmed with voter registration list
- Backup voter registration lists available
- Same-day voter registration option
- Failsafe measures protect eligible voters' right to vote
- Signature verification for mail in ballots
- Paper ballot-based elections; the paper ballot is the official record
- Mail-in ballots must be returned by mail or delivered in person; electronic submission prohibited
- All ballots securely stored with chain of custody records

Vote Tallying and Reporting Systems

- Bipartisan teams of poll officials tabulate and deliver ballots
- Voting systems not connected to the internet

Post-Election Safeguards

Election Results Canvassed

- All ballots accounted for at the precinct level
- Precincts compare and reconcile the number of ballots with the number of voters who signed in at the polling place
- Retabulation conducted on 5 percent of precincts in every election jurisdiction and on 5 percent of the voting devices used during early voting
- Post election retabulation results available to the public
- Chain of custody records maintained
- Access to results database restricted to authorized users

Election Day Security Guidelines

**Ballot security:** The ballot box shall not be opened or removed from public view from the time it is shown to be empty until the polls close or until the ballot box is delivered for counting.

**Polling place security:** After the opening of the polls, the election judges shall not permit any person to handle any electronic voting machine, except voters while they are voting and others expressly authorized by the election authority or state law.

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 and 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:*** Security measures in place to detect and eliminate potential threats

**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)

**Suspicious Incident Reporting in Illinois**

**Citizens in Illinois experiencing election cyber threats, voter suppression, or misinformation, contact the Illinois State Board of Elections:**

- ScamAlert@elections.il.gov or 217-782-4141

For Additional Information or Questions

**Illinois State Board of Elections:** https://www.elections.il.gov/
**Illinois Emergency Management Agency:** https://www2.illinois.gov/ready/plan/Pages/CyberSafety.aspx
**Illinois Department of Innovation & Technology:** https://www2.illinois.gov/sites/doit/Strategy/Cybersecurity/Pages/default.aspx
**Federal Bureau of Investigations:** https://www.fbi.gov/investigate/counterintelligence/foreign-influence/protected-voices
**U.S. Department of Homeland Security:** www.dhs.gov/topic/election-security

- Tony Enriquez, Region V Cybersecurity Advisor, antonio.enriquez@hq.dhs.gov
- Alexander Joves, Region V Director for Infrastructure Protection, ipregion5ops@hq.dhs.gov

2020 ELECTION INITIATIVES

Adams Election Data

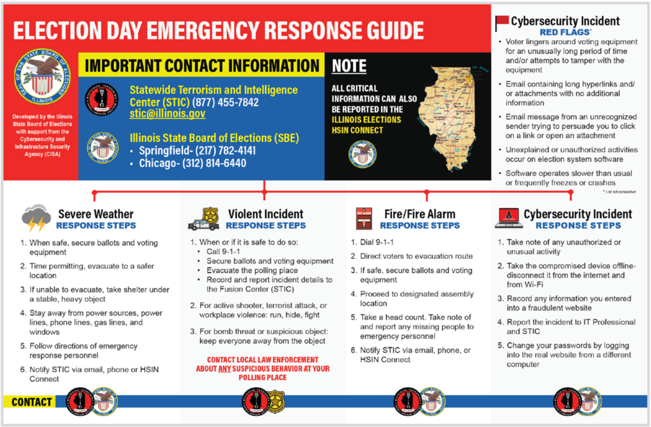
**Precincts:** 74
**Active Voters:** 46,081
**Vendors:** ES&S ; Platinum Technologies
**Voting Systems:** Unity
**Optical Scan Voting Equipment:** M100
**Accessible Voting Equipment:** Automark
**Website:** www.co.adams.il.us

Activities and Timeline Checklist

□ **Initiative 1:** Participate in the Illinois Cyber Navigator Program.
□ **Initiative 2:** Complete on-site Risk Assessment with DoIT cyber navigators.
□ **Initiative 3:** Establish two-way data sharing with cybersecurity program managers.
□ **Initiative 4:** Register for Elections Infrastructure Information Sharing & Analysis Center (EI-ISAC).
□ **Initiative 5:** Complete security awareness training offered through the State Board of Elections.
□ **Initiative 6:** Connect to the Illinois Century Network to ensure safe transmission of election data.
□ **Initiative 7:** Register and obtain a Homeland Security Information Network (HSIN) Account.
□ **Initiative 8:** Initiate securitiy upgrades utilizing Help America Vote Act (HAVA) cybersecurity grant funds.
□ **Initiative 9:** Continued participation in cyber navigator training programs.
□ **Initiative 10:** Participate in phishing assessment training offered through State Board of Elections.
□ **Initiative 11:** Conduct cyber hygiene scanning. Contact ncciccustomerservice@hq.dhs.gov and reference “Illinois Cyber Hygiene Initiative” to obtain this service free through DHS.
□ **Initiative 12:** Conduct physical security evaluation.

Developed by the Illinois State Board of Elections
with support from the U.S. Department of Homeland Security – Election Security Initiative

#PROTECT2020



ELECTION DAY EMERGENCY RESPONSE GUIDE

Developed by the Illinois State Board of Elections with support from the Cybersecurity and Infrastructure Security Agency (CISA)

IMPORTANT CONTACT INFORMATION

Statewide Terrorism and Intelligence Center (STIC) (877) 455-7842
stic@illinois.gov

Illinois State Board of Elections (SBE)

- Springfield- (217) 782-4141
- Chicago- (312) 814-6440

NOTE

ALL CRITICAL INFORMATION CAN ALSO BE REPORTED IN THE ILLINOIS ELECTIONS HSIN CONNECT

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

* List not exhaustive

Severe Weather
RESPONSE STEPS

1. When safe, secure ballots and voting equipment
2. Time permitting, evacuate to a safer location
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. Notify STIC via email, phone or HSIN Connect

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 polling place
   - Record and report incident details to the Fusion Center (STIC)
2. For active shooter, terrorist attack, or workplace violence: run, hide, fight
3. For bomb threat or suspicious object: keep everyone away from the object

CONTACT LOCAL LAW ENFORCEMENT ABOUT ANY SUSPICIOUS BEHAVIOR AT YOUR POLLING PLACE

Fire/Fire Alarm
RESPONSE STEPS

1. Dial 9-1-1
2. Direct voters to evacuation route
3. If safe, secure ballots and voting equipment
4. Proceed to designated assembly location
5. Take a head count. Take note of and report any missing people to emergency personnel
6. Notify STIC via email, phone, or HSIN Connect

Cybersecurity Incident
RESPONSE STEPS

1. Take note of any unauthorized or unusual activity
2. Take the compromised device offline- disconnect it from the internet and from Wi-Fi
3. Record any information you entered into a fraudulent website
4. Report the incident to IT Professional and STIC
5. Change your passwords by logging into the real website from a different computer

CONTACT

*See Appendix A for samples of Last Mile Products and other election security deliverables*

## SPOTLIGHT:
## ELECTION SECURITY PLANNING SNAPSHOT POSTER

The Election Security Planning Snapshot posters highlight the measures state and local election authorities are taking and plan to implement to strengthen the security of their election systems. CISA collaborates with state election officials to customize the Snapshot posters for each state and locality. The Snapshot posters promote election security initiatives and bolster confidence among voters, lawmakers, and election personnel in the security of their jurisdiction’s elections. The Snapshot posters help cover the Last Mile by demonstrating to localities that election security is a top priority for state governments and CISA, and by encouraging localities to leverage the free resources CISA offers.

## SPOTLIGHT:
## ELECTION DAY EMERGENCY RESPONSE GUIDE POSTER

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. The Election Day Emergency Response Guide posters address this capability gap by providing local election personnel with a simple yet eye-catching tool for determining what steps to take when an incident occurs and who to report the incident to. CISA works with state election officials to determine which response steps and contacts are most appropriate for their jurisdictions.

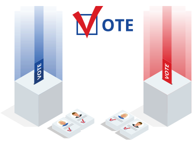
# Who We Support

The election community is made up of a variety of independent actors. CISA must constantly work to ensure stakeholder buy-in and to build trust within the community. Without each of these groups' voluntary engagement, CISA could not work to promote election security.

## State and Local Election Authorities

**State and Local Authorities:** Elections are organized and executed by citizens at all levels of government from a State's Chief Election Official to precinct poll workers. These are the operators on the front lines of drafting election security policies and overseeing their implementation.

**Coordinating Bodies:** Stakeholders in the election community often voluntarily come together in formal organizations to share information and best practices and to serve as a central communication point between the Federal Government and individual actors.



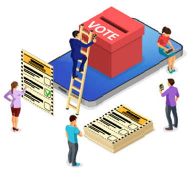
## Election Technology Vendors

Elections take place on technology and infrastructure developed, deployed, and sometimes operated by private sector companies. These companies play a critical role in ensuring the overall security of the election system.

## Campaigns and Political Infrastructure

**Campaigns:** The security practices of candidates and staffers can affect how easily an adversary can penetrate their networks and attempt to disrupt U.S. elections through leaked materials.

**National Political Party Committees:** Partisan organizations are potential targets for adversaries searching for sensitive political information. They also provide resources to assist campaigns in strengthening their cybersecurity posture.



## American Electorate

Voting citizens are the lifeblood of the election system and the ultimate targets of any attempts to interfere in the elections process.

### SPOTLIGHT:
### COORDINATING BODIES

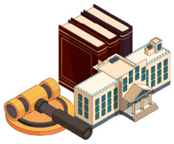
EI✓SCC

ELECTION INFRASTRUCTURE SECTOR COORDINATING COUNCIL

### The Government Coordinating Council (GCC) & Sector Coordinating Council (SCC)

The GCC and SCC are made up of state and local election officials and private sector election stakeholders, respectively. They are the primary coordinating bodies through which their respective stakeholder groups and the Federal Government collaborate to address the entire range of security and resilience efforts and policies in the subsector.

# Who We Partner With



## Federal Partners

**Federal Partners:** A number of federal agencies play a role in election security. Some have a direct election-related mandate while others have adapted from their traditional roles to support election security efforts. Through coordination across the federal interagency, election security stakeholders are provided the best possible intelligence, information, and security services.

## Non-Governmental Organizations (NGOs)

NGOs work with stakeholders at all levels to increase the election community's resilience to disruption.

## Think Tanks & Academia

Academic institutions, think tanks, and private researchers play a pivotal role in creating and promoting best practices for election security.

## Media & Social Media Companies

Traditional media outlets and social media platforms are critical nodes for reporting on elections and can be abused by malign actors to manipulate or erode confidence in the electoral system.

## Cybersecurity Firms

Private sector firms are often responsible for providing election officials with risk consultations, threat monitoring services, and incident response teams.

**SPOTLIGHT:**
**EI-ISAC**

Elections Infrastructure ISAC™

### The Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)

The EI-ISAC facilitates the sharing of cyber and critical election infrastructure data among members and others as appropriate, in order to promote communication regarding election-related disinformation and cyber and election infrastructure readiness and response efforts.

08

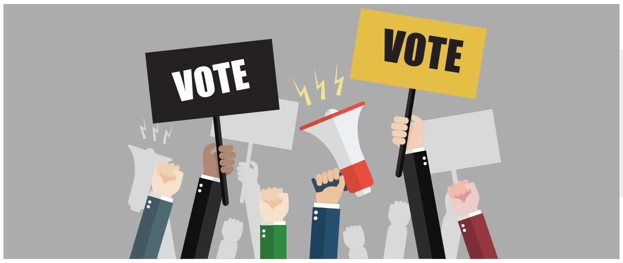
# CISA Lines of Effort

CISA's #Protect2020 campaign supports the election infrastructure community, campaigns, political infrastructure stakeholders, and the American electorate, with a combination of technical expertise and relationship building to ensure they have a solid understanding of the risks they face and access to the resources they need to manage them. To aid this effort, CISA engages with public and private sector threat intelligence sources to identify risks to the election community. CISA's #Protect2020 lines of effort work toward making the 2020 elections the safest and most secure in our Nation's history and toward building a sturdy and sustainable framework for defending all future elections.

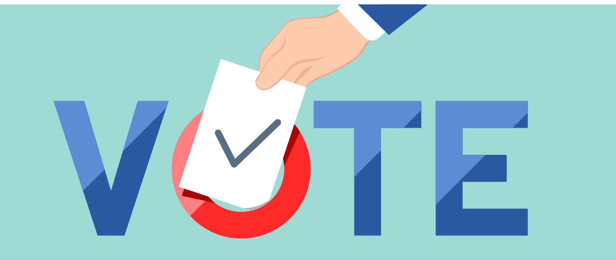
This Strategic Plan is organized by the lines of effort shown above. For each line of effort, CISA has defined associated objectives, key actions, and measures of success.

## Elections Infrastructure

## Campaigns & Political Infrastructure



## The American Electorate



## Warning and Response

**SAFE & SECURE ELECTIONS** ✓

# Line of Effort 1:

# Election Infrastructure

Ensuring state and local election officials and private sector partners have the information they need to assess and manage risks to their networks. CISA assists with efforts to secure election infrastructure, which includes storage facilities, polling places, and centralized vote tabulation locations used to support the election process. Additionally, CISA assists with information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and to report and display results on behalf of state and local governments.

## Objectives

### 1 Build Stakeholder Capacity

1.1 Promote security practices among key audiences
1.2 Advise and coordinate the creation of incident response & communications plans
1.3 Train stakeholders and exercise security practices

### 2 Provide Assessments and Services

2.1 Coordinate interactions between deployed cyber and physical advisors, and election stakeholders
2.2 Promote the use of CISA's no-cost, voluntary security services & assessments
2.3 Provide Incident Response capabilities, as necessary, by request

### 3 Facilitate Information Sharing

3.1 Convene and interface with stakeholder bodies
3.2 Expand reach among election community
3.3 Promote situational awareness among stakeholders

# Election Infrastructure

## Objectives

### 1. Build Stakeholder Capacity

CISA focuses on making sure that election infrastructure stakeholders have the skills and information necessary to assess and manage the risks they face. State and local officials, volunteer poll workers, and election system vendors are responsible for administering safe and secure elections. However, they face threats from foreign nation-states and criminal organizations. CISA serves to provide them the resources and support necessary to build their capacity to deal with these outside adversaries.

#### KEY ACTIONS

- **1.1 Promote security practices among key audiences**

  CISA partners with state and local election officials and their private sector partners to create and distribute customized products that aim to close the disparity in resources and capabilities among election infrastructure stakeholders.

- **1.2 Advise and coordinate the creation of incident response and communications plans**

  CISA works to produce standardized incident response and crisis communications plans and encourages states to adopt and practice them prior to election day.

- **1.3 Train stakeholders and exercise security practices**

  CISA offers trainings and facilitates exercises at the local, state, and national levels for the election community. The exercises simulate likely election scenarios, such as disinformation campaigns and cyber events, while highlighting best practices and allowing actors to develop and practice their response plans. The exercises serve to reinforce existing communication channels and forge new ones to be used in the event of a crisis.

### SPOTLIGHT: ELECTION INFRASTRUCTURE SUBSECTOR COORDINATING COUNCIL (EISCC) ELECTION SECURITY GUIDE

Election system vendors and their third-party providers establish the technological foundation of American democracy and are therefore integral to CISA's efforts to secure election infrastructure. However, many private sector companies that EISCC members partner with lack the resources and the know-how to meet the security standards expected by the voting public. The *EISCC Election Security Guide* provides election technology providers a tool for promoting the measures they take to secure their products, services, and infrastructure, as well as for providing guidance to their third-party providers for contributing to those efforts. The Guide also details incident response and reporting steps for their own employees and third-party providers to follow, as well as CISA resources they should leverage.

## 2. Provide Assessments and Services

CISA engages with election infrastructure stakeholders continually to give them the technical assistance necessary to monitor and secure their networks and provides them with federal support as they confront cyber threats.

### KEY ACTIONS

- **2.1 Coordinate interactions between deployed cyber and physical advisors, and election stakeholders**

  CISA deploys cybersecurity advisors (CSAs) and protective security advisors (PSAs) to all regions of the country. These advisors engage stakeholders and assist with creating their risk profiles, using federal resources, and implementing best security practices.

- **2.2 Promote the use of CISA's no-cost, voluntary security services & assessments**

  CISA maintains a full catalog of no-cost physical and cybersecurity services. These services inform CISA's understanding of risk to different communities. CISA has specifically promoted services such as vulnerability scanning, physical security assessments, remote penetration testing, and Phishing Campaign Assessments for the election community. Through these services, CISA helps stakeholders assess their risk profile and works with them to develop individualized plans for increasing security.

- **2.3 Provide incident response capabilities, as necessary, by request**

  When cyber incidents occur, CISA offers assistance by request to potentially impacted entities, analyzes the impact across critical infrastructure, and coordinates the national response to significant cyber incidents. CISA works in close coordination with other agencies with complementary cyber missions, as well as private sector and other non-federal owners and operators of critical infrastructure, to ensure greater unity of effort and a whole-of-nation response to cyber incidents.

> **"As the threat environment evolves, DHS will continue to work with federal agencies, state and local partners, and private sector entities to enhance our understanding of the threat; and to make essential physical and cybersecurity tools and resources available to the public and private sectors to increase security and resiliency."**
>
> *Bob Kolasky*
> *Director of National Risk Management Center*

## 3. Facilitate Information Sharing

The election infrastructure community relies on up-to-date threat reporting and best practice sharing to secure America's elections. CISA facilitates this two-way process by coordinating up-to-date intelligence sharing between the Federal Government and private and local partners.

### KEY ACTIONS

- **3.1 Convene and interface with stakeholder bodies**
  CISA is the sector-specific agency for the election infrastructure subsector and takes the lead in managing to guide priorities across the subsector and promote effective communication among state and local officials, industry experts, and the Federal Government.
- **3.2 Expand reach among the election community**
  CISA funds the EI-ISAC to enable rapid communication, information sharing, and situational awareness across the community. CISA has prioritized encouraging localities to sign up for the EI-ISAC.
- **3.3 Promote situational awareness among stakeholders**
  CISA and the EI-ISAC provide a variety of situational awareness capabilities, including hosting a platform prior to, during, and after state and national elections for election stakeholders to swiftly identify, react to, and share real-time events and intelligence.

### SPOTLIGHT: GCC "READY FOR 2020" PRIORITIES

The Election Infrastructure Government Coordinating Council (EI-GCC) identified 5 priorities to support the Election Infrastructure Sector Specific Plan ahead of the 2020 elections:

- Increase engagement and support to local-level election officials.
- Increase awareness of risks associated with inconsistent and insufficient resources.
- Mature risk initiatives with Sector-Specific Agencies (SSAs) through coordination with Sector Coordinating Councils.
- Apply lessons learned from 2018 to review and refine the communications mechanisms and content supporting the subsector.
- Drive improved security practices in future election infrastructure.

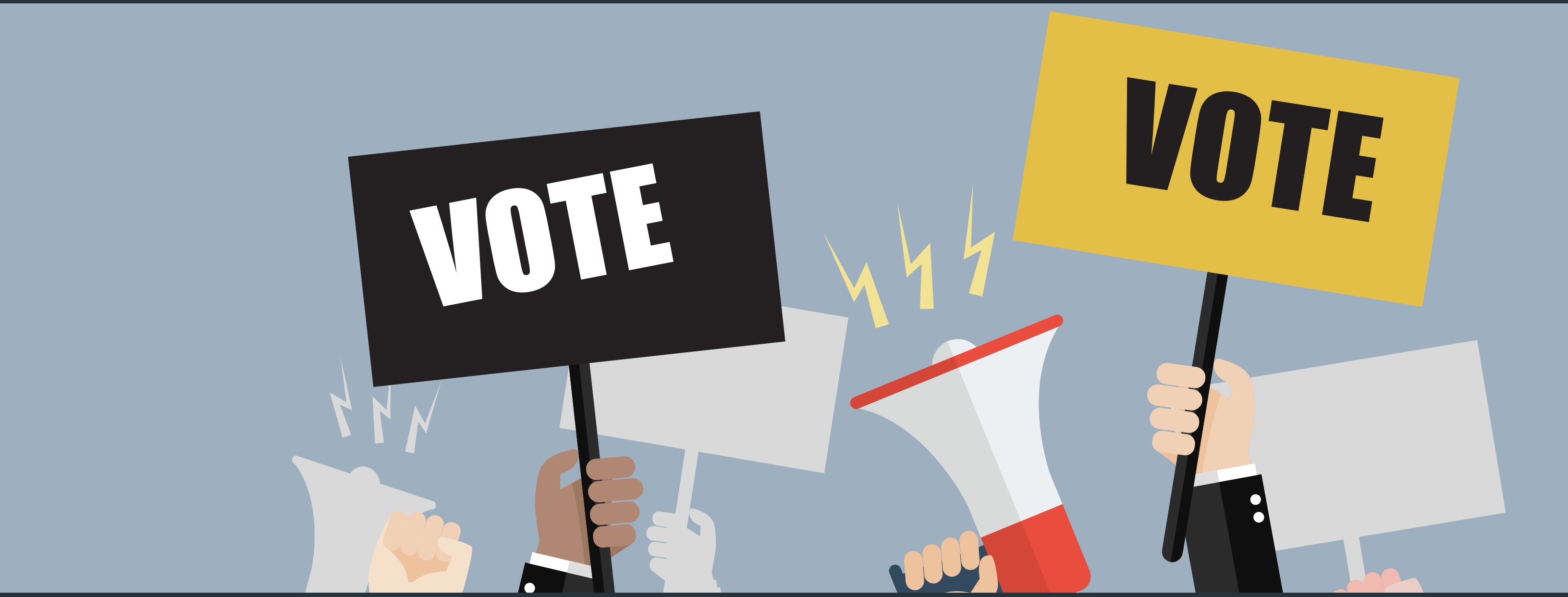
### SUCCESS INDICATORS

- Advance election technology security from voter registration databases to vote casting devices and ballot tabulation processes.
- Prepare election infrastructure stakeholders to perform their duties securely and manage incident response scenarios.
- Encourage more secure publicly facing platforms that display voting information and report election night results.

## Line of Effort 2:

# Campaigns & Political Infrastructure

To provide political campaigns and partisan organizations with access to the information they need to assess and manage risks. CISA assists efforts to secure political infrastructure and critical communications systems.



## Objectives

### 4 Build Partisan Stakeholder Capacity

4.1 Foster the creation of an engaged stakeholder community

### 5 Provide Assessments and Services to Partisan Stakeholders

5.1 Offer CISA no-cost, voluntary services & assessments

### 6 Facilitate Information Sharing with Partisan Stakeholders

6.1 Brief campaigns on the latest threat intelligence

6.2 Meet with national-level campaigns and party committees

## 14 *Line of Effort 2*

# Campaigns & Political Infrastructure

## Objectives

### 4. Build Partisan Stakeholder Capacity

Traditionally, campaigns and national political parties are hyper focused on raising money, amplifying political messages, and turning out voters, but 2016 showed that they are vulnerable stakeholders in the election community. CISA works with them to build their capacities and increase their resilience.

#### KEY ACTIONS

- **4.1 Foster the creation of an engaged stakeholder community**

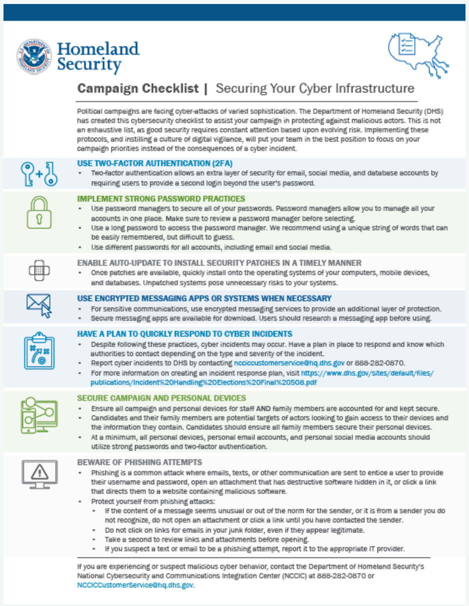
  CISA works with political infrastructure stakeholders to create a culture of active information sharing and collaborative best practice sharing.

### 5. Provide Assessments and Services to Partisan Stakeholders

Campaigns and political parties host sensitive voter information, private communications, and privileged policy proposals on a wide array of networks and devices. CISA works with them to identify and mitigate vulnerabilities within these information technology systems.

### SPOTLIGHT: CAMPAIGN CHECKLIST

In 2018, CISA built a campaign checklist to circulate to candidates and their staff to assist them in implementing cybersecurity best practices in order to protect them against malicious actors.



Homeland Security

**Campaign Checklist |** Securing Your Cyber Infrastructure

Political campaigns are facing cyber-attacks of varied sophistication. The Department of Homeland Security (DHS) has created this cybersecurity checklist to assist your campaign in protecting against malicious actors. This is not an exhaustive list, as good security requires constant attention based upon evolving risk. Implementing these protocols, and instilling a culture of digital vigilance, will put your team in the best position to focus on your campaign priorities instead of the consequences of a cyber incident.

**USE TWO-FACTOR AUTHENTICATION (2FA)**
- Two-factor authentication allows an extra layer of security for email, social media, and database accounts by requiring users to provide a second login beyond the user's password.

**IMPLEMENT STRONG PASSWORD PRACTICES**
- Use password managers to secure all of your passwords. Password managers allow you to manage all your accounts in one place. Make sure to review a password manager before selecting.
- Use a long password to access the password manager. We recommend using a unique string of words that can be easily remembered, but difficult to guess.
- Use different passwords for all accounts, including email and social media.

**ENABLE AUTO-UPDATE TO INSTALL SECURITY PATCHES IN A TIMELY MANNER**
- Once patches are available, quickly install onto the operating systems of your computers, mobile devices, and databases. Unpatched systems pose unnecessary risks to your systems.

**USE ENCRYPTED MESSAGING APPS OR SYSTEMS WHEN NECESSARY**
- For sensitive communications, use encrypted messaging services to provide an additional layer of protection.
- Secure messaging apps are available for download. Users should research a messaging app before using.

**HAVE A PLAN TO QUICKLY RESPOND TO CYBER INCIDENTS**
- Despite following these practices, cyber incidents may occur. Have a plan in place to respond and know which authorities to contact depending on the type and severity of the incident.
- Report cyber incidents to DHS by contacting nccicсustomerservice@hq.dhs.gov or 888-282-0870.
- For more information on creating an incident response plan, visit https://www.dhs.gov/sites/default/files/publications/Incident%20Handling%20Elections%20Final%20508.pdf

**SECURE CAMPAIGN AND PERSONAL DEVICES**
- Ensure all campaign and personal devices for staff **AND** family members are accounted for and kept secure.
- Candidates and their family members are potential targets of actors looking to gain access to their devices and the information they contain. Candidates should ensure all family members secure their personal devices.
- At a minimum, all personal devices, personal email accounts, and personal social media accounts should utilize strong passwords and two-factor authentication.

**BEWARE OF PHISHING ATTEMPTS**
- Phishing is a common attack where emails, texts, or other communication are sent to entice a user to provide their username and password, open an attachment that has destructive software hidden in it, or click a link that directs them to a website containing malicious software.
- Protect yourself from phishing attacks:
  - If the content of a message seems unusual or out of the norm for the sender, or it is from a sender you do not recognize, do not open an attachment or click a link until you have contacted the sender.
  - Do not click on links for emails in your junk folder, even if they appear legitimate.
  - Take a second to review links and attachments before opening.
  - If you suspect a text or email to be a phishing attempt, report it to the appropriate IT provider.

If you are experiencing or suspect malicious cyber behavior, contact the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC) at 888-282-0870 or NCCICCustomerService@hq.dhs.gov.

#### KEY ACTIONS

- **5.1 Offer CISA no-cost, voluntary services and assessments**

  CISA offers campaign staff, candidates, and national party committees the same services and assessments available to election infrastructure stakeholders. However, due to its critical infrastructure status, any services or assessments requested by election infrastructure stakeholders would receive priority over campaigns and political infrastructure requests. CISA also provides incident response capabilities, by request.

## 6. Facilitate Information Sharing with Partisan Stakeholders

In a heated political contest, information sharing between partisan entities is difficult. CISA works with campaigns and political parties to provide them real-time threat and vulnerability information from the Federal Government. Even though campaign and partisan actors are not designated as elections infrastructure, CISA offers cybersecurity assistance to these entities, ensuring that the same assistance is offered to all similarly-situated entities and is not offered for the purpose of conferring any political advantage or disadvantage on those entities.

### KEY ACTIONS

- **6.1 Brief campaigns on the latest threat intelligence**
  CISA collaborates with the FBI and the intelligence community to offer campaigns joint briefings on potential threats to their systems or active hostile campaigns.
- **6.2 Meet with national-level campaigns and party committees**
  CISA holds introductory meetings with national-level political campaigns and partisan organizations to provide information on CISA services and points of contact for incident response and other needs.

### SUCCESS INDICATORS

- Increase engagement between partisan actors and the Federal Government.
- Promote a greater emphasis on cybersecurity and risk mitigation throughout the political infrastructure community.

> **We recognize the fundamental link between public trust in our election infrastructure and the confidence the American public places in basic democratic functions. Ensuring the security of our electoral process is a vital national interest and one of our highest priorities at DHS.**
>
> ***Bob Kolasky***
> *Director of National Risk Management Center*

## SPOTLIGHT:
## COUNTERING FOREIGN INFLUENCE TASK FORCE (CFITF)

In early 2018, former Secretary Kirstjen Nielsen established a Countering Foreign Influence Task Force (CFITF) within the Department of Homeland Security. The Task Force is now formally a part of CISA. It works in close coordination with the FBI Foreign Influence Task Force, the government lead on foreign interference.

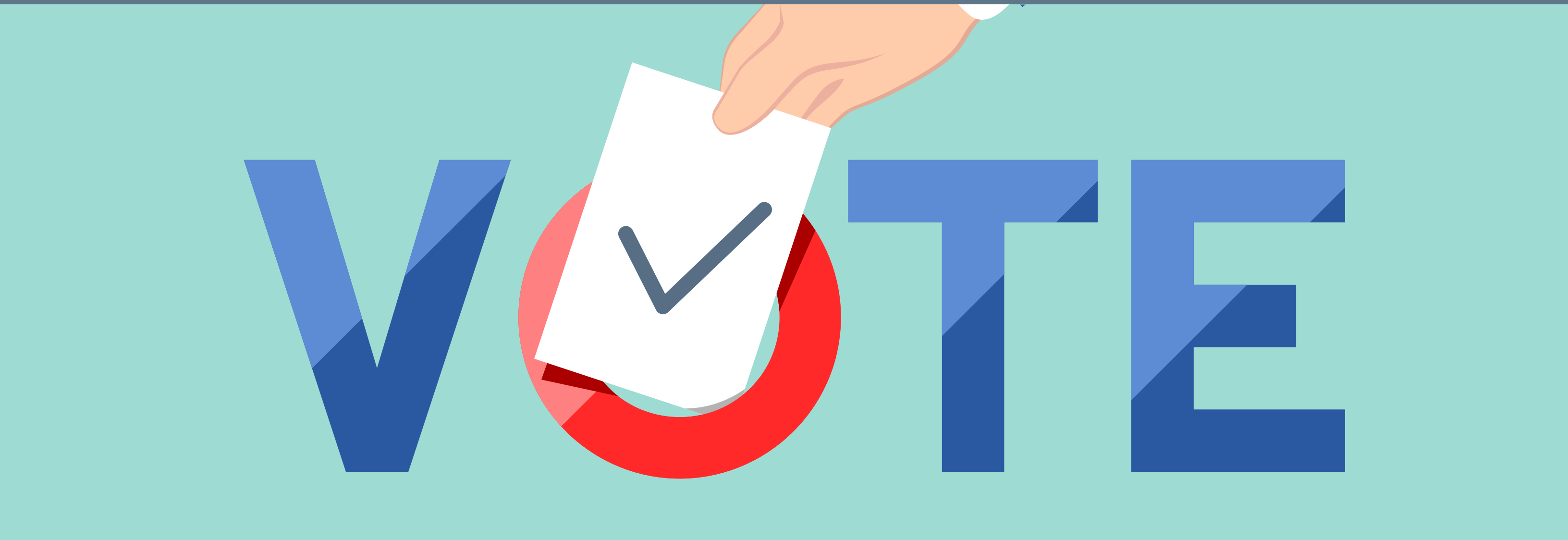
CFITF is charged with helping CISA's leadership understand the scope and scale of this challenge; identifying the policy options available to the government; and working with social media companies, academia, international partners and across the executive branch on a variety of projects to build resilience against foreign influence operations.

Based on its governing authorities, CISA plays a significant role in enabling stakeholders to make effective risk management decisions. Applying that role to the foreign influence context, the Task Force supports election stakeholders by helping them to understand the scope and scale of the challenge and by enabling them to take actions they deem appropriate. CFITF and the FBI Foreign Influence Task Force coordinate closely on public outreach and education efforts.

## Line of Effort 3:

# The American Electorate

Americans regularly believe, engage with, and share content online and through their personal networks, that has been designed by foreign adversaries to undermine U.S. democratic institutions, disrupt U.S. markets, and sow societal discord. CISA aims to build societal resilience to the persuasion and dissuasion created or amplified by foreign influence activities, including disinformation and misinformation, to ensure the integrity and autonomy of the American electorate.



## Objectives

### 7 Understand and Evaluate the Threat

7.1 Partner With Subject Matter Experts
7.2 Partner With Federal Counterparts

### 8 Build Public Awareness & Educate the Public on Best Practices

8.1 Develop Informational Products
8.2 Engage Trusted Voices

### 9 Facilitate Information Sharing

9.1 Expand the Reporting Community
9.2 Host Domestic and International Disinformation Switchboard

# The American Electorate

## Objectives

### 7. Understand and Evaluate the Threat

In order to come up with policy recommendations and adequately support stakeholder populations, CISA needs to understand the nature and scope of the threat and common tactics used in foreign influence operations. Rather than starting from the drawing board, CISA engages the expertise of external and federal partners who have studied or tracked information operations beyond the election sphere, as well as regional and national security experts familiar with the tactics of U.S. adversaries active in the disinformation space.

### KEY ACTIONS

- **7.1 Partner with Subject Matter Experts (SMEs)**
  CISA engages with SMEs, including researchers, academics, think tanks, and marketing experts, to better understand the threat and how to develop messaging to mitigate the impact of foreign influence operations.
- **7.2 Partner with federal counterparts**
  CISA works in close collaboration with the FBI's Foreign Influence Task Force, the State Department's Global Engagement Center, the Department of Defense, and intelligence community to recognize, understand, and help manage the threat of foreign influence on the American people.

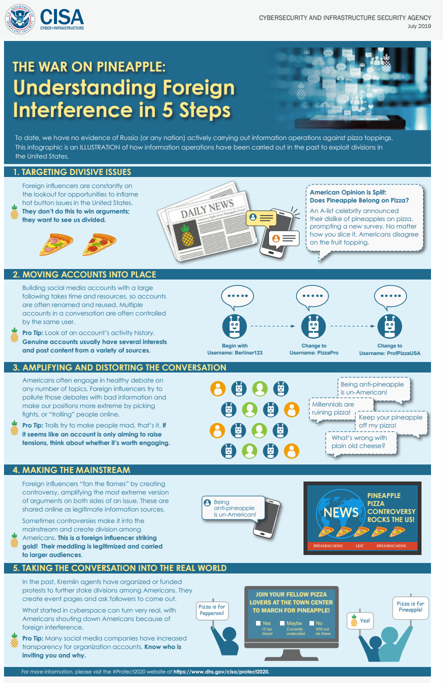
> **One of the highest-profile threats we face today is attempts by nation-state actors to maliciously interfere in our democratic elections.**

***CHRISTOPHER C. KREBS***
***Director, Cybersecurity and Infrastructure Security Agency (CISA)***

**SPOTLIGHT:**

### THE WAR ON PINEAPPLE

In 2019, CISA launched a public awareness campaign to educate the electorate about ways foreign actors may try to interfere with democratic processes by sowing discord and pitting American against American. The first product of this initiative was an infographic taking an innocuous example — whether pineapple belongs on pizza — and showing a potential strategy a foreign actor could use to spread divisiveness on the issue.



CISA CYBER+INFRASTRUCTURE

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: ProfPizzaUSA

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!

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.**

JOIN YOUR FELLOW PIZZA LOVERS AT THE TOWN CENTER TO MARCH FOR PINEAPPLE!
□ Yes I'll be there! □ Maybe Currently undecided □ No Will not be there

Pizza is for Pepperoni!
Yes!
Pizza is for Pineapple!

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

## 8. Build Public Awareness & Educate the Public on Best Practices

Findings from academics and researchers show that much of the manipulative power of disinformation can be undermined through awareness. As the public becomes more aware of the tactics and procedures used to covertly manipulate their opinion forming, they become more resistant to them. For this reason, CISA prioritized building public awareness and providing educational materials on best practices as a key strategy in its efforts to foster public resilience to disinformation.

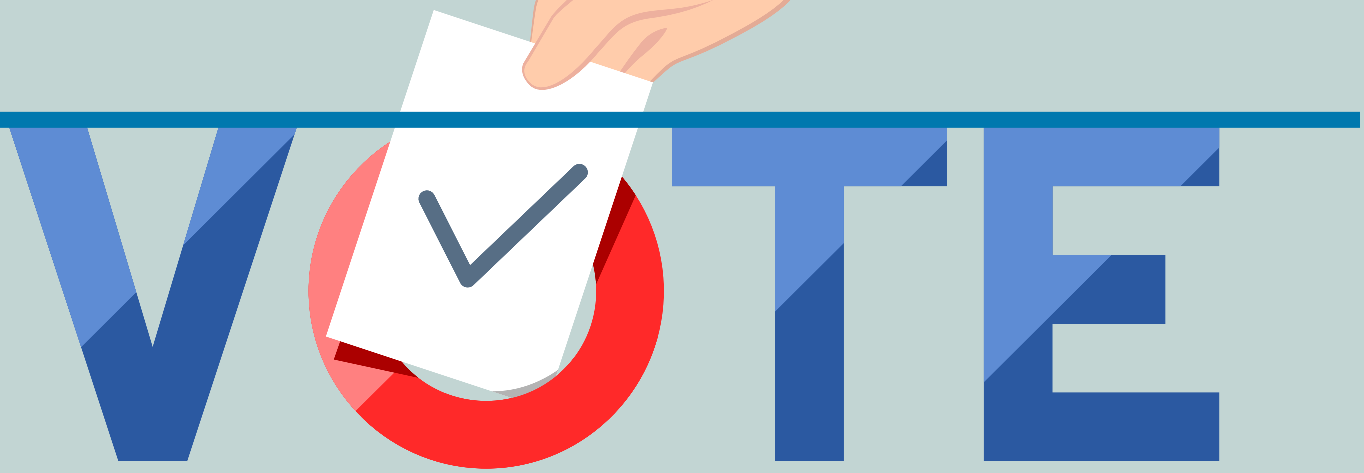
### KEY ACTIONS

- **8.1 Develop informational products**

  CISA is developing a number of products to share with the public and influencer organizations. These products aim to build public awareness about the disinformation threat and educate the public on ways to mitigate it. In addition, CISA promotes third-party products that align with its mission statement.

- **8.2 Engage trusted voices**

  CISA engages "trusted voices," influential groups such as the American Association of Retired Persons (AARP) and the National Association for the Advancement of Colored People (NAACP), to amplify resilience messaging and reach a broader stakeholder base.



## 9. Facilitate Information Sharing

CISA coordinates the sharing of information between the Federal Government, private sector, and state election officials to make sure that the American electorate has access to accurate and up-to-date information on all aspects of the election process.

### SUCCESS INDICATORS

- Limit electorate's exposure to foreign disinformation on social media platforms.
- Mitigate the effect of foreign disinformation on targeted audiences.

### KEY ACTIONS

- **9.1 Expand the Reporting Community**

  CISA will build upon 2018 midterm Election Information Sharing efforts by expanding the number of entities that can report incidents to CISA and expanding the number of platforms with agreements to receive reporting from CISA.

- **9.2 Host Domestic and International Disinformation Switchboard**

  Following its success in the 2018 U.S. midterm elections, CISA again plans to operate as a switchboard for routing disinformation concerns of state and local election officials to appropriate social media platforms and law enforcement agencies. Additionally, CISA plans to share information and best practices with international partners who are experiencing similar concerns within their own elections.

> **"We can patch cyber vulnerabilities and defend our databases, but if we don't also prepare the American people for the onslaught of foreign interference they face daily, then we will have failed."**

*BRIAN SCULLY*
*Countering Foreign Influence Lead,*
*Election Security Initiative*

# Line of Effort 4:
# Warning and Response

Warning and response reinforces CISA's three previous lines of effort, capacity building and support for election officials, campaigns, and the American electorate. It aims to provide accurate and actionable threat intelligence to the election community.

## Objectives

### 10 Partner with the Private Sector

10.1 Improve warning and response by facilitating cooperation between vendors, election officials, and private sector experts

10.2 Engage the cybersecurity community

### 11 Cooperate Across the Federal Interagency

11.1 Foster a sense of community and support common understanding across the federal interagency on election threats

11.2 Coordinate with the intelligence community and law enforcement to enrich their understanding of cybersecurity incidents and identify trends impacting election infrastructure

### 12 Monitor Threat Activity

12.1 Identify emerging threats using CISA, EI-ISAC, and federal partner & private sector capabilities

12.2 Synchronize information from a variety of sources to understand the full threat picture

### 13 Facilitate Rapid Information Sharing with Elections Infrastructure Stakeholders

13.1 Share cyber threat intelligence, context on cyber incident trends, and mitigation advice with elections infrastructure owners, operators, and vendors in a rapid, actionable manner

13.2 Facilitate provision of feedback on shared threat information to improve the intelligence cycle and ensure mitigation advice is actionable

# *Line of Effort 4*

# Warning and Response

## Objectives

### 10. Partner with the Private Sector

Many private sector firms conduct research and perform assessments relevant to election security. In order to have access to the most up-to-date information and avoid duplicating efforts, CISA partners with recognized security experts from across the private sector to understand the threats and provide warning and mitigation actions to election stakeholders.

#### KEY ACTIONS

- **10.1 Improve warning and response by facilitating cooperation between vendors, election officials, and private sector experts**

  CISA coordinates between election technology vendors, state and local officials, and private cyber threat intelligence firms to develop indicators and warnings.

- **10.2 Engage the cybersecurity community**

  CISA works with cybersecurity communities to identify ongoing attacks and coordinate response measures.

### 11. Cooperate Across the Federal Interagency

As with previous lines of effort, to develop a warning and response protocol requires cooperation with federal counterparts and information sharing across the intelligence community to stay up-to-date on the most urgent threats and vulnerabilities across the election community.

#### KEY ACTIONS

- **11.1 Foster a sense of community and support common understanding across the federal interagency on election threats**

  CISA advocates creating a joint Sense of the Community Memorandum to consolidate and highlight current knowledge on election threat intelligence.

- **11.2 Coordinate with the intelligence community and law enforcement to enrich their understanding of cybersecurity incidents and identify trends impacting election infrastructure**

  CISA works closely with interagency partners to ensure the government has an accurate and complete picture of the threat landscape from which to engage the election community.

## 12. Monitor Threat Activity

CISA relies heavily on partner capabilities, including the intelligence community and EI-ISAC, to track and monitor emerging threats to elections.

### KEY ACTIONS

- **12.1 Identify emerging threats using CISA, EI-ISAC, and federal partner & private sector capabilities**
  CISA uses passive measures to monitor relevant networks to spot malign activity and reveal key trends.
- **12.2 Synchronize information from a variety of sources to understand the full threat picture**
  CISA reviews and analyzes third-party vendor information, unclassified open source reporting, and threat information received from stakeholders to understand the scope of malicious cyber activity and foreign influence activities targeting elections.

## 13. Facilitate Rapid Information Sharing with Elections Infrastructure Stakeholders

CISA analyzes various information sources to develop a continuously updated picture of the threats to election infrastructure and provides information to elections stakeholders in order to facilitate risk mitigation activities.

### KEY ACTIONS

- **13.1 Share cyber threat intelligence, context on cyber incident trends, and mitigation advice with elections infrastructure owners, operators, and vendors in a rapid, actionable manner**
  CISA works to ensure relevant and actionable threat information is declassified when necessary and shared with the appropriate network owners and operators for cyber defense purposes. CISA also develops and publishes mitigation advice when appropriate and shares it with elections stakeholders as rapidly as possible.
- **13.2 Facilitate provision of feedback on shared threat information to improve the intelligence cycle and ensure mitigation advice is actionable**
  CISA will ensure that feedback from election infrastructure stakeholders is shared with interagency partners to facilitate improvements for network defense purposes.

**SUCCESS INDICATORS**

- Identify potential and realized threats to the election community.
- Improve sharing of timely and actionable threat information with election community.
- Improve processes and mechanisms for information sharing across federal entities.

# Measuring and Achieving Results

The Federal Government has made significant improvements in its efforts to promote safe and secure elections since the Secretary of Homeland Security designated elections infrastructure as a critical infrastructure subsector on January 6, 2017. Initially, there was much confusion over what the designation meant, and stakeholders criticized DHS for not involving them in this decision, for not explaining it effectively, and for continuing to describe threats to election infrastructure without engaging the states. CISA recognized a need to better serve this community and surged resources to establish the Election Task Force and build critical infrastructure governance bodies.

CISA's mission for the 2018 midterm elections focused on proactively building trust with the election community, elevating security of election infrastructure, and facilitating information sharing across stakeholders, including social media and technology companies, law enforcement and intelligence, and state and local election officials. In the lead up to the 2020 elections, CISA will continue the prioritization of support to election administrators and vendors and will continue to build relationships to support and advise partisan organizations. It aims to enhance awareness of and participation by the public and to partner with third-party organizations and subject matter experts to help develop and amplify effective public messaging. Additionally, CISA will work to enhance federal, private, and ISAC operational alliance to improve rapid bi-directional information sharing and expand engagements with threat intelligence firms and the intelligence community to ensure that the election community has access to accurate and actionable threat analysis.

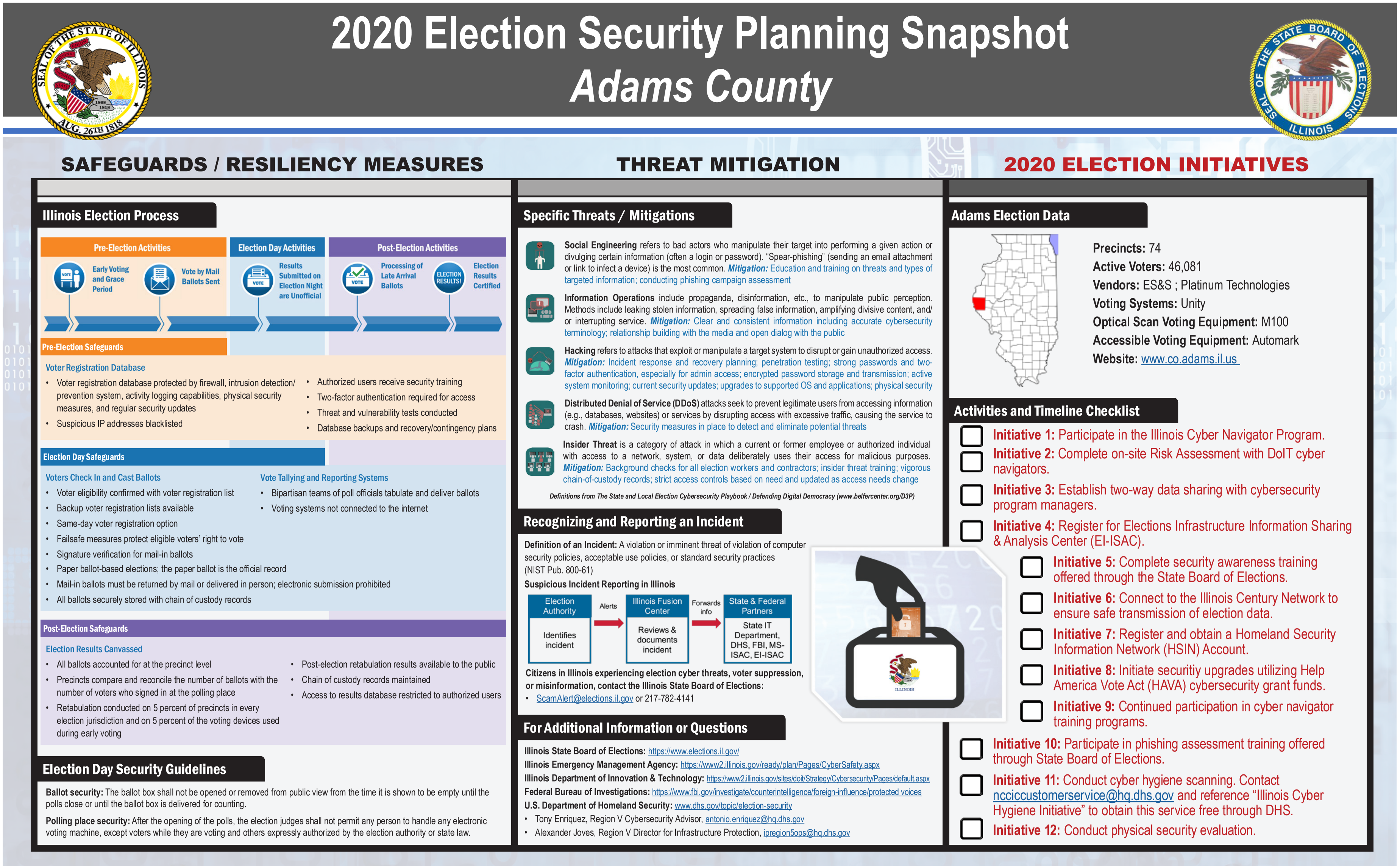
# Conclusion

#Protect2020 is more than just a slogan; it is a pledge among election security stakeholders—including the Federal cybersecurity community, state and local election officials, vendors, political campaigns, and others—to work together towards a common vision of a safe and secure election trusted by all Americans in 2020. This is an ambitious undertaking. The threat landscape is constantly evolving, and dedicated, malicious actors with virtually unlimited resources will always be able to penetrate some aspect of American networks or to spread disinformation. In the field of election security, it is not possible to identify all system vulnerabilities and defend them in all scenarios. However, it is CISA's mission to elevate the security posture of our Nation's election systems to make these intrusions more difficult, identify them when they occur, and ensure that they do not affect the overall outcome of the election. CISA cannot do this alone.

Ultimately, the security of America's elections rests with the state and local officials who administer them, the private sector vendors who create the technology that makes them possible, the candidates and campaigns who participate in them, and ultimately the electorate who show up to the polls on election day. Securing American elections requires hard work, resources, and persistence among all of these critical actors, and no one entity can do it alone. To this end, CISA's #Protect2020 strategy is all about building strong, resilient, and interconnected stakeholder communities, outfitted with the required capacities, technical assistance, and information necessary to resist adversaries while trusting that the DHS CISA organization will be there to support them in every way that they can.

# Appendix A: Election Security Deliverables

## Election Security Planning Snapshot – “The Last Mile” Poster



# 2020 Election Security Planning Snapshot
*Adams County*

## SAFEGUARDS / RESILIENCY MEASURES

### Illinois Election Process

Pre-Election Activities
Early Voting and Grace Period
Vote by Mail Ballots Sent
Election Day Activities
Results Submitted on Election Night are Unofficial
Post-Election Activities
Processing of Late Arrival Ballots
Election Results Certified
VOTE
ELECTION RESULTS!

#### Pre-Election Safeguards

Voter Registration Database

- Voter registration database protected by firewall, intrusion detection/ prevention system, activity logging capabilities, physical security measures, and regular security updates
- Suspicious IP addresses blacklisted
- Authorized users receive security training
- Two-factor authentication required for access
- Threat and vulnerability tests conducted
- Database backups and recovery/contingency plans

#### Election Day Safeguards

Voters Check In and Cast Ballots

- Voter eligibility confirmed with voter registration list
- Backup voter registration lists available
- Same-day voter registration option
- Failsafe measures protect eligible voters' right to vote
- Signature verification for mail-in ballots
- Paper ballot-based elections; the paper ballot is the official record
- Mail-in ballots must be returned by mail or delivered in person; electronic submission prohibited
- All ballots securely stored with chain of custody records

Vote Tallying and Reporting Systems

- Bipartisan teams of poll officials tabulate and deliver ballots
- Voting systems not connected to the internet

#### Post-Election Safeguards

Election Results Canvassed

- All ballots accounted for at the precinct level
- Precincts compare and reconcile the number of ballots with the number of voters who signed in at the polling place
- Retabulation conducted on 5 percent of precincts in every election jurisdiction and on 5 percent of the voting devices used during early voting
- Post-election retabulation results available to the public
- Chain of custody records maintained
- Access to results database restricted to authorized users

### Election Day Security Guidelines

**Ballot security:** The ballot box shall not be opened or removed from public view from the time it is shown to be empty until the polls close or until the ballot box is delivered for counting.

**Polling place security:** After the opening of the polls, the election judges shall not permit any person to handle any electronic voting machine, except voters while they are voting and others expressly authorized by the election authority or state law.

## 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 and 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:*** Security measures in place to detect and eliminate potential threats

**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)

**Suspicious Incident Reporting in Illinois**

**Citizens in Illinois experiencing election cyber threats, voter suppression, or misinformation, contact the Illinois State Board of Elections:**

- ScamAlert@elections.il.gov or 217-782-4141

### For Additional Information or Questions

**Illinois State Board of Elections:** https://www.elections.il.gov/
**Illinois Emergency Management Agency:** https://www2.illinois.gov/ready/plan/Pages/CyberSafety.aspx
**Illinois Department of Innovation & Technology:** https://www2.illinois.gov/sites/doit/Strategy/Cybersecurity/Pages/default.aspx
**Federal Bureau of Investigations:** https://www.fbi.gov/investigate/counterintelligence/foreign-influence/protected voices
**U.S. Department of Homeland Security:** www.dhs.gov/topic/election-security

- Tony Enriquez, Region V Cybersecurity Advisor, antonio.enriquez@hq.dhs.gov
- Alexander Joves, Region V Director for Infrastructure Protection, ipregion5ops@hq.dhs.gov

## 2020 ELECTION INITIATIVES

### Adams Election Data

**Precincts:** 74
**Active Voters:** 46,081
**Vendors:** ES&S ; Platinum Technologies
**Voting Systems:** Unity
**Optical Scan Voting Equipment:** M100
**Accessible Voting Equipment:** Automark
**Website:** www.co.adams.il.us

### Activities and Timeline Checklist

- □ **Initiative 1:** Participate in the Illinois Cyber Navigator Program.
- □ **Initiative 2:** Complete on-site Risk Assessment with DoIT cyber navigators.
- □ **Initiative 3:** Establish two-way data sharing with cybersecurity program managers.
- □ **Initiative 4:** Register for Elections Infrastructure Information Sharing & Analysis Center (EI-ISAC).
  - □ **Initiative 5:** Complete security awareness training offered through the State Board of Elections.
  - □ **Initiative 6:** Connect to the Illinois Century Network to ensure safe transmission of election data.
  - □ **Initiative 7:** Register and obtain a Homeland Security Information Network (HSIN) Account.
  - □ **Initiative 8:** Initiate securitiy upgrades utilizing Help America Vote Act (HAVA) cybersecurity grant funds.
  - □ **Initiative 9:** Continued participation in cyber navigator training programs.
- □ **Initiative 10:** Participate in phishing assessment training offered through State Board of Elections.
- □ **Initiative 11:** Conduct cyber hygiene scanning. Contact ncciccustomerservice@hq.dhs.gov and reference “Illinois Cyber Hygiene Initiative” to obtain this service free through DHS.
- □ **Initiative 12:** Conduct physical security evaluation.

Developed by the Illinois State Board of Elections

*with support from the U.S. Department of Homeland Security – Election Security Initiative*

#PROTECT2020

# Election Day Emergency Response Guide– “EDERG” Poster

## ELECTION DAY EMERGENCY RESPONSE GUIDE

Developed by the Illinois State Board of Elections with support from the Cybersecurity and Infrastructure Security Agency (CISA)

### IMPORTANT CONTACT INFORMATION

**Statewide Terrorism and Intelligence Center (STIC)** (877) 455-7842
stic@illinois.gov

**Illinois State Board of Elections (SBE)**
- Springfield- (217) 782-4141
- Chicago- (312) 814-6440

### NOTE

ALL CRITICAL INFORMATION CAN ALSO BE REPORTED IN THE **ILLINOIS ELECTIONS HSIN CONNECT**

### 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

* List not exhaustive

### Severe Weather
**RESPONSE STEPS**

1. When safe, secure ballots and voting equipment
2. Time permitting, evacuate to a safer location
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. Notify STIC via email, phone or HSIN Connect

### 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 polling place
   - Record and report incident details to the Fusion Center (STIC)
2. For active shooter, terrorist attack, or workplace violence: run, hide, fight
3. For bomb threat or suspicious object: keep everyone away from the object

**CONTACT LOCAL LAW ENFORCEMENT ABOUT ANY SUSPICIOUS BEHAVIOR AT YOUR POLLING PLACE**

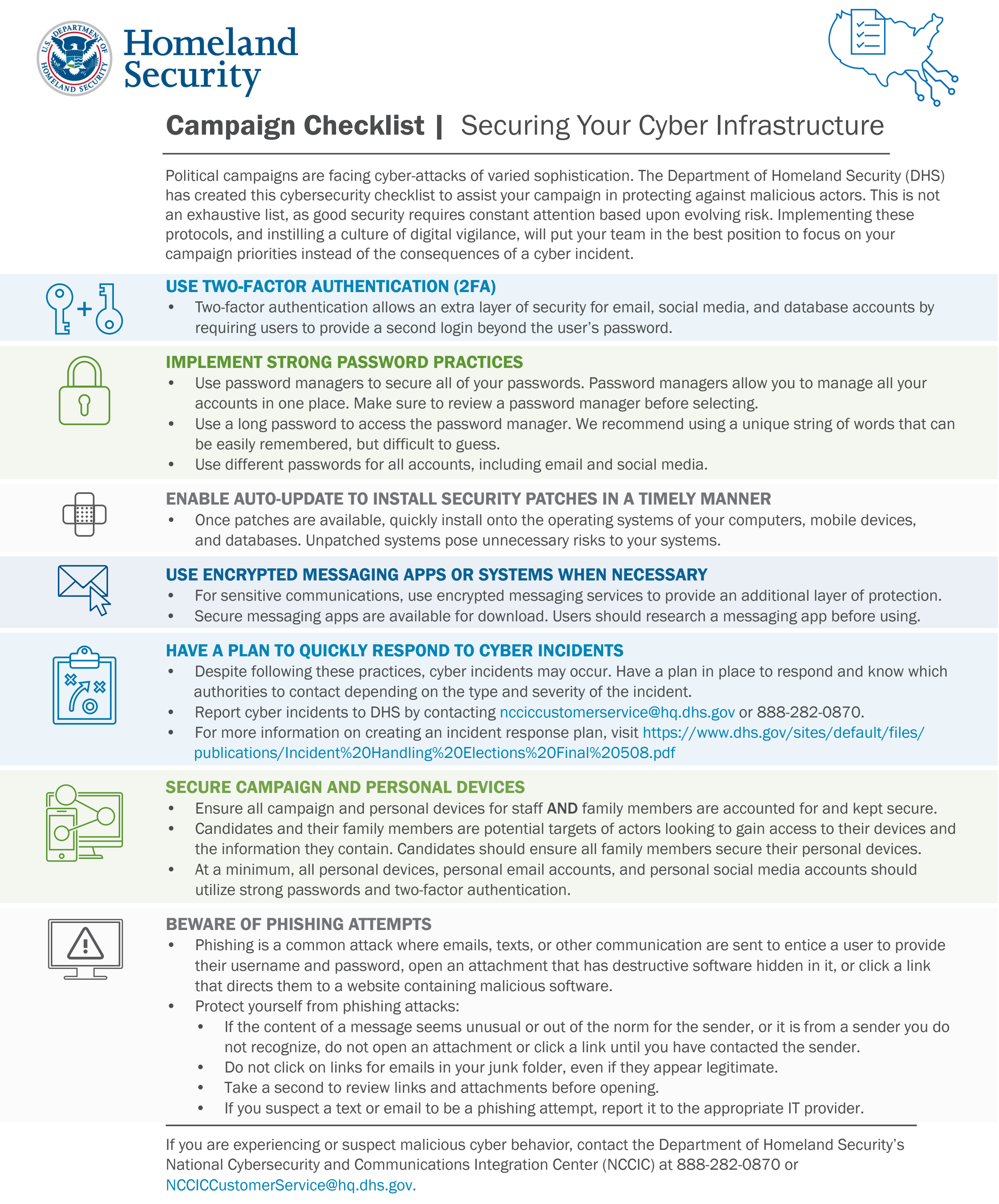
### Fire/Fire Alarm
**RESPONSE STEPS**

1. Dial 9-1-1
2. Direct voters to evacuation route
3. If safe, secure ballots and voting equipment
4. Proceed to designated assembly location
5. Take a head count. Take note of and report any missing people to emergency personnel
6. Notify STIC via email, phone, or HSIN Connect

### Cybersecurity Incident
**RESPONSE STEPS**

1. Take note of any unauthorized or unusual activity
2. Take the compromised device offline-disconnect it from the internet and from Wi-Fi
3. Record any information you entered into a fraudulent website
4. Report the incident to IT Professional and STIC
5. Change your passwords by logging into the real website from a different computer

**CONTACT**



Homeland Security

## Campaign Checklist | Securing Your Cyber Infrastructure

Political campaigns are facing cyber-attacks of varied sophistication. The Department of Homeland Security (DHS) has created this cybersecurity checklist to assist your campaign in protecting against malicious actors. This is not an exhaustive list, as good security requires constant attention based upon evolving risk. Implementing these protocols, and instilling a culture of digital vigilance, will put your team in the best position to focus on your campaign priorities instead of the consequences of a cyber incident.

### USE TWO-FACTOR AUTHENTICATION (2FA)

- Two-factor authentication allows an extra layer of security for email, social media, and database accounts by requiring users to provide a second login beyond the user's password.

### IMPLEMENT STRONG PASSWORD PRACTICES

- Use password managers to secure all of your passwords. Password managers allow you to manage all your accounts in one place. Make sure to review a password manager before selecting.
- Use a long password to access the password manager. We recommend using a unique string of words that can be easily remembered, but difficult to guess.
- Use different passwords for all accounts, including email and social media.

### ENABLE AUTO-UPDATE TO INSTALL SECURITY PATCHES IN A TIMELY MANNER

- Once patches are available, quickly install onto the operating systems of your computers, mobile devices, and databases. Unpatched systems pose unnecessary risks to your systems.

### USE ENCRYPTED MESSAGING APPS OR SYSTEMS WHEN NECESSARY

- For sensitive communications, use encrypted messaging services to provide an additional layer of protection.
- Secure messaging apps are available for download. Users should research a messaging app before using.

### HAVE A PLAN TO QUICKLY RESPOND TO CYBER INCIDENTS

- Despite following these practices, cyber incidents may occur. Have a plan in place to respond and know which authorities to contact depending on the type and severity of the incident.
- Report cyber incidents to DHS by contacting ncciccustomerservice@hq.dhs.gov or 888-282-0870.
- For more information on creating an incident response plan, visit https://www.dhs.gov/sites/default/files/publications/Incident%20Handling%20Elections%20Final%20508.pdf

### SECURE CAMPAIGN AND PERSONAL DEVICES

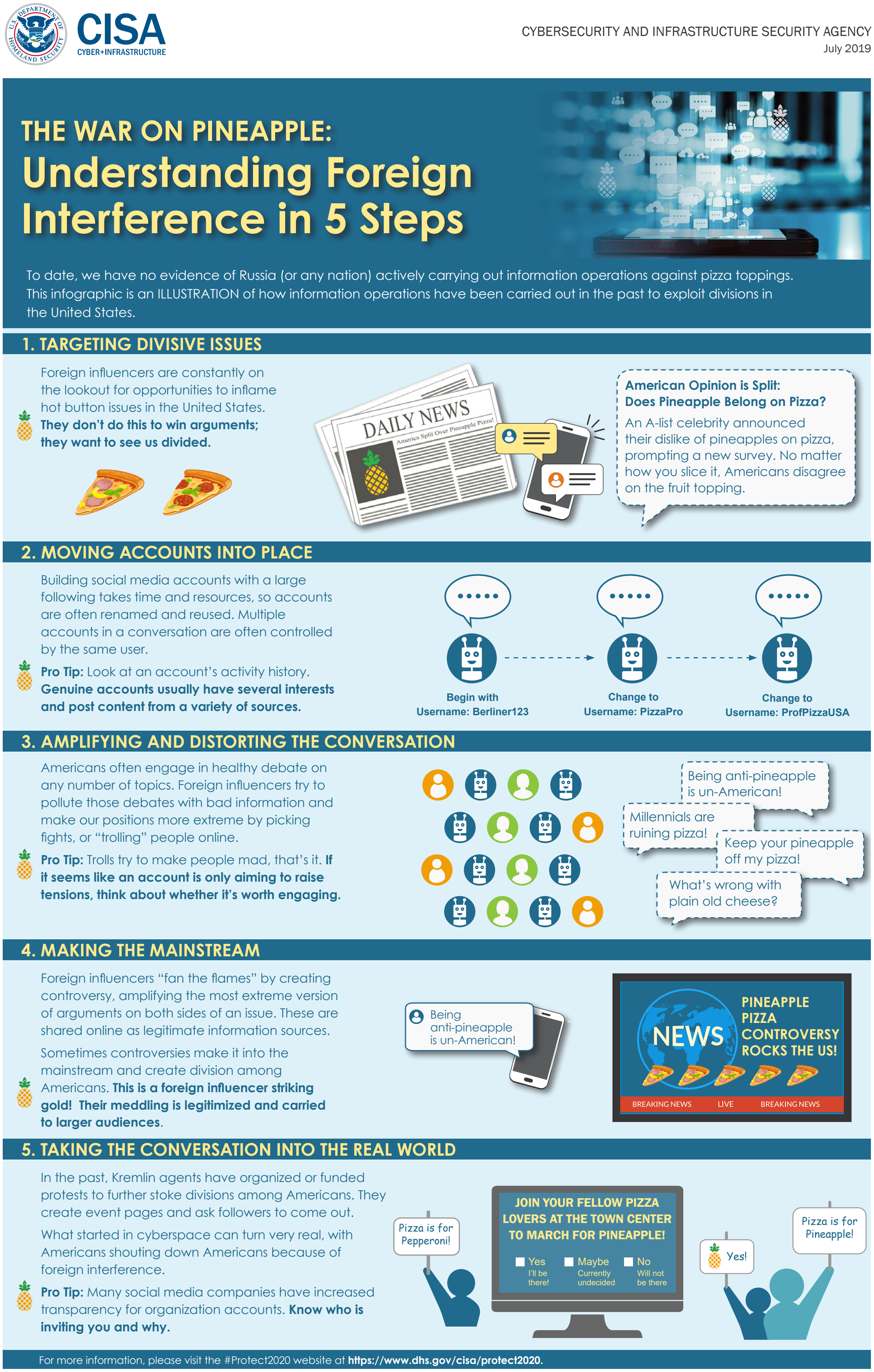
- Ensure all campaign and personal devices for staff **AND** family members are accounted for and kept secure.
- Candidates and their family members are potential targets of actors looking to gain access to their devices and the information they contain. Candidates should ensure all family members secure their personal devices.
- At a minimum, all personal devices, personal email accounts, and personal social media accounts should utilize strong passwords and two-factor authentication.

### BEWARE OF PHISHING ATTEMPTS

- Phishing is a common attack where emails, texts, or other communication are sent to entice a user to provide their username and password, open an attachment that has destructive software hidden in it, or click a link that directs them to a website containing malicious software.
- Protect yourself from phishing attacks:
  - If the content of a message seems unusual or out of the norm for the sender, or it is from a sender you do not recognize, do not open an attachment or click a link until you have contacted the sender.
  - Do not click on links for emails in your junk folder, even if they appear legitimate.
  - Take a second to review links and attachments before opening.
  - If you suspect a text or email to be a phishing attempt, report it to the appropriate IT provider.

If you are experiencing or suspect malicious cyber behavior, contact the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC) at 888-282-0870 or NCCICCustomerService@hq.dhs.gov.

# 29 The War on Pineapple Infographic



CISA
CYBER+INFRASTRUCTURE

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.**

DAILY NEWS
America Split Over Pineapple Pizza!

**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: ProfPizzaUSA

### 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!
BREAKING NEWS LIVE BREAKING NEWS

### 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 I'll be there! □ Maybe Currently undecided □ No Will not be there

Yes!

Pizza is for Pineapple!

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

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