



CISA
CYBER+INFRASTRUCTURE

ELECTION SECURITY INITIATIVE

ESI-101



CISA
CYBER+INFRASTRUCTURE

Election Systems: Designated Critical Infrastructure

Mission Statement: To ensure the Election Stakeholder Community – infrastructure owners and operators, partisan organizations, and the electorate – has the necessary information to adequately assess risks and protect, detect, and recover from those risks.

The 2017 designation of election infrastructure as critical infrastructure provides a basis for the Department of Homeland Security and other federal agencies to:

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



CISA's Support to Election Community

- **Election Security remains a top priority for DHS and CISA in 2020**
- Increase engagement and support provided to local election officials
- Raise awareness regarding the need for regular investment in election infrastructure
- Further develop CISA's understanding and conversations about risks to election infrastructure
- Improve communications and information sharing across the subsector
- Make CISA resources available to election officials and technology providers to #PROTECT2020
- Increase support to election system private sector



Threats to Election Infrastructure

Potential Adversaries:

- Nation-state actors
- Black Hat Hackers
- Criminals
- Politically Motivated Groups
- Insiders
- Terrorists

Possible Motivations:

- Undermine Trust in Democracy
- Foreign Policy Goals
- Sow Social Division
- Financial Gain
- Subvert Political Opposition
- Fame and Reputation
- Foment Chaos/Anarchy
- Retribution for Perceived Grievances

Potential Targets:

- Voter registration databases
- Voting systems
- Election reporting systems
- Storage facilities and polling places
- Public confidence in the integrity of the election



Growth of CISA's Election Security Mission

2016

Reactive Response to Incidents in the 2016 Election

- Triggered by cyber incidents in two states and a breach of a political organization.
- DHS tried to rapidly engage the election stakeholder community.
- Unsure of the best lines of communication and reached out to state CIOs instead of election officials.

2017

Recovering from a Deficit of Trust

- Critical Infrastructure designation issued on January 6, 2017.
- Notified 21 states that they had been scanned by an adversary.
- Stood up the Election Task Force, began meeting with state election officials, established the Government Coordinating Council (GCC).

2018

Proactively building trust and elevating security

- Funded the creation of the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC).
- Provided classified and unclassified threat briefings.
- Hosted Tabletop the Vote 2018.
- Creation of the Countering Foreign Influence Task Force

2019-2020

Partnering for more secure elections

- Increased engagement at local level via Last Mile initiative.
- #Protect2020 Strategic Plan with four Lines of Effort (LOE) ahead of the 2020 Election Cycle.



David Kuennen
December 10, 2020

CISA 2020 Priorities - #Protect2020 Strategic Plan

1. **Election Infrastructure:** Ensure state and local election officials and private sector partners have the information they need to assess and manage risks to their networks.
2. **Campaigns & Political Infrastructure:** 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.
3. **The American Electorate:** 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.
4. **Warning and Response:** Provide accurate and actionable threat intelligence to the election community, reinforcing the other three lines of effort.



David Kuennen
December 10, 2020

LOE 1: Protect Election Infrastructure

- Build Stakeholder Capacity
- Provide Assessments and Services
- Facilitate Information Sharing
- **COVID-19 Response**



Build Stakeholder Capacity – Education

Top Recommendations for Election Infrastructure Stakeholders

- Mitigate Internet Vulnerabilities in a Timely Manner
- Strengthen Password Policy and Auditing Processes
- Implement Network Segmentation
- Have a Plan and Implement Backups
- Replace Unmaintainable Equipment

Election Infrastructure Resource Library available at

<https://www.cisa.gov/protect2020>

Key Steps for Election Officials to Take to Improve Their Cybersecurity Posture

Election officials can improve their cybersecurity posture by taking advantage of any of the following cybersecurity services that are provided by the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA). All of these services are free.

Step 1: Join the EHSAC

Information to protect infrastructure community geared toward the EHSAC infrastructure private sector:

- 24 x 7
- Election
- Threat

Membership organization <https://eam.cisa.gov>

Step 2: Know your vulnerability place to mitigate risk

For assistance, contact your state or local election officials. As a volunteer, you can help increase the security of your system. Administer secure web hosts, and cybersecurity vulnerability scanning.

Ransomware

Ransomware is malicious software designed to deny access to computer systems or data. In a ransomware attack, systems and/or data are encrypted and a payment is requested to decrypt. Paying the ransom does not guarantee a user will regain access to their systems or data and this information can be permanently lost. For elections, a ransomware attack could deny access to voter registration data, election results, and other sensitive information. It could also inhibit access to important election systems during critical operational periods such as registration and candidate filing deadlines.

Protect Your Systems and Data Against Ransomware

Committing organizational resources which emphasize cyber hygiene and cybersecurity best practices are the best defenses against ransomware attacks. CISA recommends the following precautions and best practices to protect users against the threat of ransomware:

- Update software and operating systems with the latest patches. Outdated applications and unpatched operating systems are the most frequent targets of ransomware attacks.
- Apply the principle of least privilege to all systems and services. Restricting user and third-party permissions to install and run software applications can help prevent malware from executing and spreading. Application whitelisting—specifying an index of approved software applications that are permitted to be present and active on a system—can be effective in preventing unauthorized programs from running on a network.
- Authenticate inbound email to prevent receipt of spoofed emails. CISA recommends implementing Domain-Based Message Authentication, Reporting, and Conformance (DMARC) and adopting a policy to, at least, quarantine emails that fail the DMARC check. DMARC can reduce the likelihood of your domain being spoofed and enable you to reduce the likelihood of clicking on a spoofed email. For more information, see https://www.dhs.gov/sites/default/files/publications/19_0419_cisa-domain-based-message-authentication-reporting-and-conformance.pdf.
- Scan incoming and outgoing emails to detect threats and filter executable files from reaching end users. Enable strong spam filters to prevent phishing emails from reaching end users.
- Consider leveraging network security devices to provide defense in depth. For example, an intrusion detection system (IDS) can identify infections before they cause too much damage. Ensure any solutions you implement monitor your entire election infrastructure.
- Secure end users against phishing and social engineering via ongoing awareness campaigns and assessments. Ensure staff members are aware of the risks associated with opening suspicious emails, clicking links, or opening unsolicited attachments. Advise them to report any abnormal or suspicious system behavior to your IT or security teams immediately. Implement multi-factor authentication where possible.

Plan for a Ransomware Incident

Ransomware infections typically occur through user-initiated actions like clicking on malicious email links, visiting infected websites, or opening files with embedded macros or scripts. Some types of ransomware may spread to shared storage drives and other systems on the same network. To prepare for a potential ransomware incident:

- Develop an incident response plan that details mitigation steps for business continuity and recovery should a ransomware event occur. In addition to addressing events that affect your systems and assets directly, the plan should account for ransomware infections on other state or local government systems that may indirectly affect your jurisdiction's election infrastructure.
- Confirm you have up-to-date points of contact on file if the EHSAC or a commercial security provider monitors your networks or email. Know how to notify responders as quickly as possible.

2019-09-30

Leveraging the .gov Top-level Domain

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

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

Why should I use a .gov domain?

Since a .gov domain is a top-level domain (TLD) that was established to make it easy to identify US-based government organizations on the internet, it is a trusted and credible website, email, and social media presence.

There are also several benefits to using a .gov domain:

- The .gov domain is a top-level domain (TLD) that was established to make it easy to identify US-based government organizations on the internet.
- Web browser
- The .gov domain is a top-level domain (TLD) that was established to make it easy to identify US-based government organizations on the internet.

How do I get a .gov domain?

To obtain a .gov domain, you must be a federal, state, or local government official or employee. For more information, visit <https://www.dhs.gov/electoral-voting>.

An organization that is not a government entity cannot register a .gov domain. To register a .gov domain, you must be a federal, state, or local government official or employee. For more information, visit <https://www.dhs.gov/electoral-voting>.

Displaying non-secure content is not allowed, and not recommended.

Cybersecurity Best Practices for Election Officials

What steps can election officials take to increase the security of their infrastructure?

Stay Informed of New and Emerging Cyber Threats and Vulnerabilities

Ensure that your organization receives timely and relevant cyber threat indicators and technical vulnerability information. Joining the Elections Infrastructure Information Sharing and Analysis Center (EHSAC) is one recommended solution. This information sharing center was created to serve the election community by providing near real time threat and risk sharing as well as cybersecurity best practices geared towards election officials. Membership in the EHSAC is open to all state, local, tribal, and territorial government organizations and associations that support elections in the United States. To join the EHSAC for free, visit <https://eam.cisa.gov/electoral-voting>.

Mitigate Vulnerabilities in a Timely Manner

Your organization should mitigate all internet-accessible vulnerabilities, such as unpatched web applications, in a timely manner. For context, the federal government requires its departments and agencies to mitigate all vulnerabilities at the critical severity level within 15 calendar days and to mitigate vulnerabilities with lower severity levels within 30-60 calendar days.

For assistance with identifying vulnerabilities, consider enrolling in CISA's Vulnerability Scanning, which is a voluntary, free scanning of internet-accessible systems for known vulnerabilities on a continual basis. As potential issues are identified, CISA notifies customers so they may proactively mitigate risks to their systems prior to exploitation. To enroll in Vulnerability Scanning, contact govcustomerservice@hhs.dhs.gov. Your organization should have an established Patch Management Policy and utilize equipment that is maintainable with current security patching. Exceptions should be minimized and isolated to limit risk.

Control Access to Your Infrastructure

Your organization should utilize multi-factor authentication and perform regular audits of password policies. Password best practices include ensuring that default passwords are changed, that strong passwords are required, and that administrators utilize encrypted password vaults. For additional information on password best practices, visit <https://pages.nist.gov/800-63-3/sp800-63b.html>. For additional information on multi-factor authentication, visit <https://www.dhs.gov/publication/election-security-resource-library>.

Internal network architecture should protect and control access to your most sensitive systems. User workstations should be less trusted and connections to external networks should be isolated, controlled, and monitored. For example, employees with access to voter registration data should utilize a separate workstation for email and internet access.

Have a Plan and Implement Backups

Your organization should have an Incident Response Plan and a Continuity of Operations Plan. The Continuity of Operations Plan should identify a restoration point based on what makes sense for your system, determine the frequency of backups, and include a strong patching methodology for operating systems and third-party products. For best practices on Continuity of Operations Plans and a template for an Incident Response Plan, visit <https://www.dhs.gov/publication/election-security-resource-library>.

2019-06-05



David Kuennen
December 10, 2020

Build Stakeholder Capacity – Partnership

Election Infrastructure Subsector Government Coordinating Council (EIS GCC)

- Formation in 2017 was a milestone in multi-level government cooperation that bolstered election infrastructure security and resilience.
- Enables sharing of information, resources, capabilities, and collective expertise.
- Consists of 27 members, 24 of which are state and local election officials.
- Is led by a five-member Executive Committee (DHS/CISA; EAC; a Secretary of State; a state Election Director; and a local Election Director).

Election Infrastructure Subsector Coordinating Council (EISCC)

- Formed in 2018 to serve as the primary liaison between the private sector and government on election infrastructure security.
- Facilitates information and intelligence sharing.
- Coordinates with DHS and the EIS GCC to develop, recommend, and review subsector-wide plans and procedures.

Election Infrastructure Subsector-Specific Plan (SSP)

- Jointly authored and approved in February 2020
- Describes voluntary framework for subsector partners to collaborate on election infrastructure security



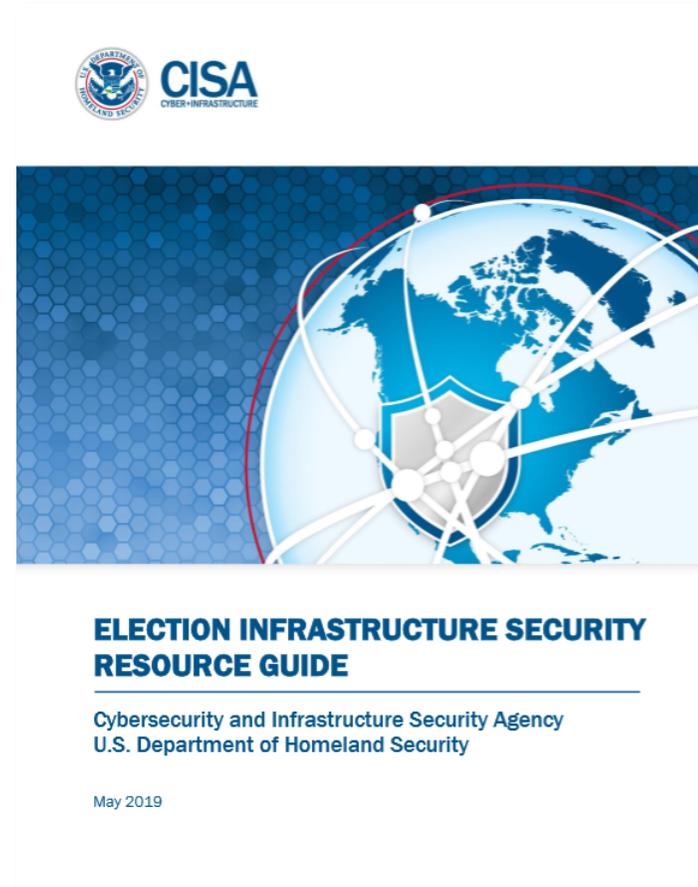
Assessments and Services

Voluntary, no-cost suite of services available to Election Infrastructure partners from CISA

CISA field personnel help to promote and coordinate delivery of these capabilities

Top recommended CISA cyber services for election officials:

- Vulnerability Scanning
- Remote Penetration Testing
- Phishing Campaign Assessment
- Incident Response capabilities (remote or onsite)



Information Sharing

What We Share

Strategic Threat Intelligence

CISA works with I&A, the Intelligence Community, the FBI, and private sector security firms to provide election officials with broader threat intelligence to inform their prioritization of security practices.

Specific Intelligence Notifications

CISA and I&A have requested specific intelligence products be approved for notification purposes. DHS and FBI are considered notifying entities.

Alerts and Warnings

CISA and the EI-ISAC provide alerts provide timely information about current security issues, vulnerabilities, and exploits.

Operational Cyber Threat Indicators

CISA works with IC and private sector partners to disseminate known malicious indicators and signatures for network defenders to action on their networks.

How We Share

Provide Security Clearances and host Classified Briefings

CISA manages a program that provides security clearances to state and local election officials and GCC and SCC members.

Framework for Notifying Regarding Foreign Interference in United States Elections

An IC-led and NSC approved framework for determining whether and to what extent intelligence should be shared with stakeholders and the public.

Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)

In February 2018, the EIS GCC and DHS partnered to form the EI-ISAC, which is funded in part by a cooperative agreement with CISA. As of Apr. 2020, it has more than 2,500 members, including all 50 states.

Push indicators to Albert Sensors supporting Election Infrastructure

Through the EI-ISAC, CISA has funded a network of sensors on all 50 states which capture internet traffic and alert on known malicious indicators.

Election Day Situation Room

Each Election Day, DHS hosts the National Cybersecurity Situational Awareness Room—an online information sharing portal that provides election officials and vendors with virtual access to the NCCIC.



Information Sharing

The Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) is a dedicated resource that gathers, analyzes, and shares information on critical infrastructure and facilitates two-way cybersecurity threat information sharing between the public and the private sectors.

The EI-ISAC supports the election community through:

- 24 x 7 x 365 network monitoring
- Election-specific threat intelligence
- Threat and vulnerability monitoring
- Incident response and remediation
- Training sessions and webinars
- Promotion of security best practices



Progress since 2018

Establishment of the EI-ISAC

- In February 2018, the EIS GCC established the EI-ISAC, which is now the fastest growing ISAC ever with more than 2,400 members as of February 2020.

Funding Considerations

- In March 2020, the EIS GCC released updated guidance with potential short- and long-term funding considerations to support elections officials making decisions on how they could use newly available funding to help secure election infrastructure.

Communications Protocols

- In January 2020, the EIS GCC approved updated Threat Information Sharing and Incident Reporting Protocols to improve the efficiency and effectiveness of information sharing between election officials and the federal government.

New Trainings and Assessments

- Driven by feedback from election officials, CISA now offers capabilities like Remote Penetration Testing as well as “The Election Official as IT Manager” online course.

Exercises

- CISA hosts “Tabletop the Vote,” an annual, national-level virtual TTX with 44+ states, the District of Columbia, and 10+ Federal agencies.
- In January 2020, released a Elections-specific “TTX in a Box.”

Classified Briefings

- CISA has partnered with the Intelligence Community to share classified information on several occasions. DHS provides security clearances for state election officials and GCC & SCC members.

Election Day Situation Room

- Each Election Day, CISA hosts the National Cybersecurity Situational Awareness Room. This online portal for election officials and vendors facilitates rapid information sharing and provided election officials with virtual access to CISA’s 24/7 operational watch floor.



COVID-19 Response

- **CISA remains engaged with Election Infrastructure Subsector partners in a remote support posture**
- Partnered with U.S. Election Assistance Commission on COVID-19 Response Working Group under GCC/SCC structure, including election officials, private sector, and SMEs. Focused on identifying and promulgating considerations and best practices in two primary topic areas:
 - Expanded implementation of vote-by-mail
 - Enhanced measures for voter and election worker health and safety
- Facilitated briefings/coordination with USPS and CDC
- Developing updated Risk Postures to share with the interagency
- CISA Essential Critical Infrastructure Worker Guidance
 - Recognizes the criticality of Election Workers (including public and private sector organizations)
- “COVID-19 & Elections” website: <https://www.cisa.gov/covid-19-and-elections>
- Published a disinformation toolkit for use by state and local governments and an overview of COVID-19 disinformation and steps to avoid amplifying disinformation



LOE 2: Support Campaigns and Political Organizations

Build Partisan Stakeholder Capacity

- Published “Campaign Security Checklist”
 - https://www.dhs.gov/sites/default/files/publications/DHS%20Campaign%20Checklist_FINAL%20October.pdf

Provide Assessments and Services to Partisan Stakeholders

- Same suite of services that are available to Election Infrastructure partners

Facilitate Information Sharing

- Participated with FBI and ODNI in a joint briefing to FEC-registered Presidential campaigns in May 2019
 - Inform them of threat landscape
 - Promote security practices
 - Broaden awareness of incident response capabilities
- CISA met with all declared 2020 Presidential Campaigns
- Working with parties at national and state level around caucuses



LOE 3: Support the American Electorate

Foreign Influence

- Malign actions taken by foreign actors (e.g. governments) to spread disinformation designed to manipulate the public, sow discord and ill will, discredit the electoral process, disrupt markets, and undermine the interests of the American people.
- FBI is the lead agency for countering foreign interference. DHS supports through convening authorities and the ability to broaden awareness.
- CISA's focuses on raising public awareness of, and resilience to, tactics and techniques of foreign interference.

Countering Foreign Influence

- Understand and evaluate the threat
 - Partner with SMEs and federal counterparts
 - Identify targeted audiences
 - Identify possible foreign narratives and efforts
- Build Public Awareness
 - Develop informational products and toolkits
 - Engage trusted voices
 - Amplify election officials
- Facilitate Information Sharing
 - Connect partners from various sectors and levels of government



CISA
CYBER+INFRASTRUCTURE

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY
June 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 passions 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.**

Pizza is for Peppercorn | JOIN YOUR FELLOW PIZZA LOVERS AT THE TOWN CENTER TO MARCH FOR PINEAPPLE! | Pizza is for Pineapple!

David Kuennen
December 10, 2020

Public Resilience Messaging

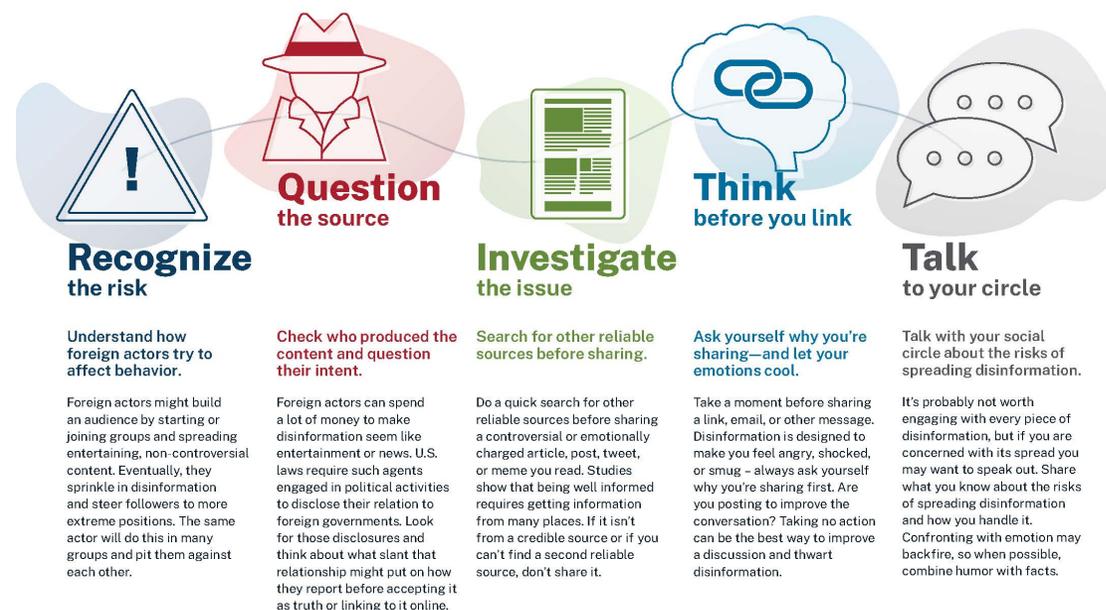
CISA develops public products to educate and enhance resilience of Americans to Disinformation

Resilience Products

- Understanding Foreign Interference
- Foreign Interference Taxonomy
- War on Pineapple: Understanding Foreign Influence in 5 Steps
- Disinfo Toolkit – “Disinformation Stops With You” and topic sheets
- Social Media Bots Overview
- Various External Resources on Mis/Disinformation
- Additional products, links to government reading, and external resources can be found at www.dhs.gov/cisa/protect2020

Disinformation Stops With You

You have the power to stop foreign influence operations.



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



David Kuennen
December 10, 2020

LOE 4: Warning & Response

Partner with the Private Sector

- Improve warning and response by facilitating cooperation between election system vendors, election officials, and private sector

Cooperate Across the Federal Interagency

- Develop common understanding of threats to Election Infrastructure
- Coordinate with IC and LE to enrich understanding of incidents and trends affecting Election Infrastructure

Monitor threat Activity

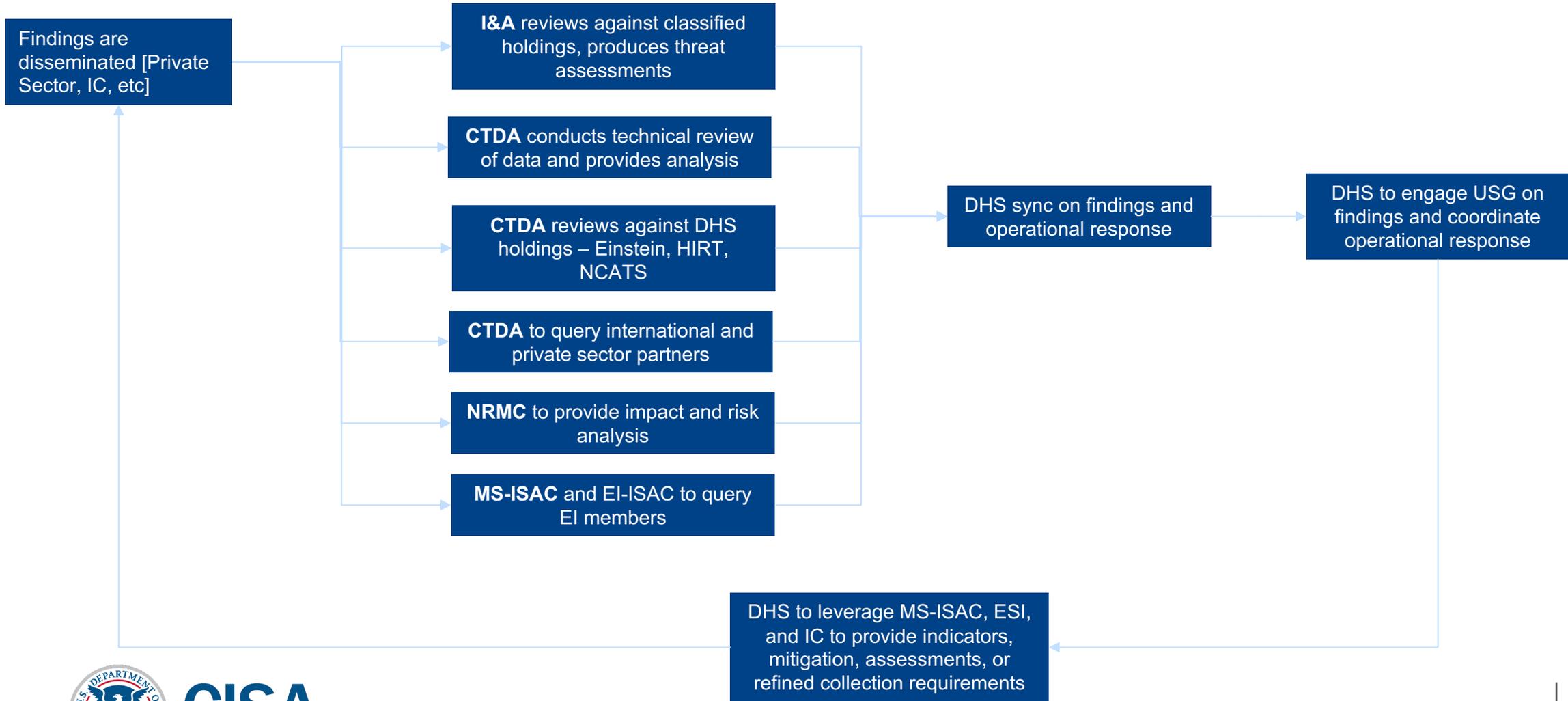
- Identify emerging threats using federal and private sector partner capabilities
- Synchronize info from multiple sources to understand the full threat picture

Facilitate Rapid Information Sharing with Election Infrastructure Stakeholders

- Emphasize speed and actionability
- Share EI stakeholder feedback within federal interagency community to facilitate network defense improvements



LOE 4: Warning & Response



CISA Election Security 101



CISA
CYBER+INFRASTRUCTURE

David Kuennen
IT Cybersecurity Specialist
Cybersecurity & Infrastructure Security Agency
david.kuennen@@cisa.dhs.gov