CISA

CYBER+INFRASTRUCTURE

ELECTION SECURITY INITIATIVE

ESI-101

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.

CISA
CYBER+INFRASTRUCTURE

David Kuennen
December 10, 2020

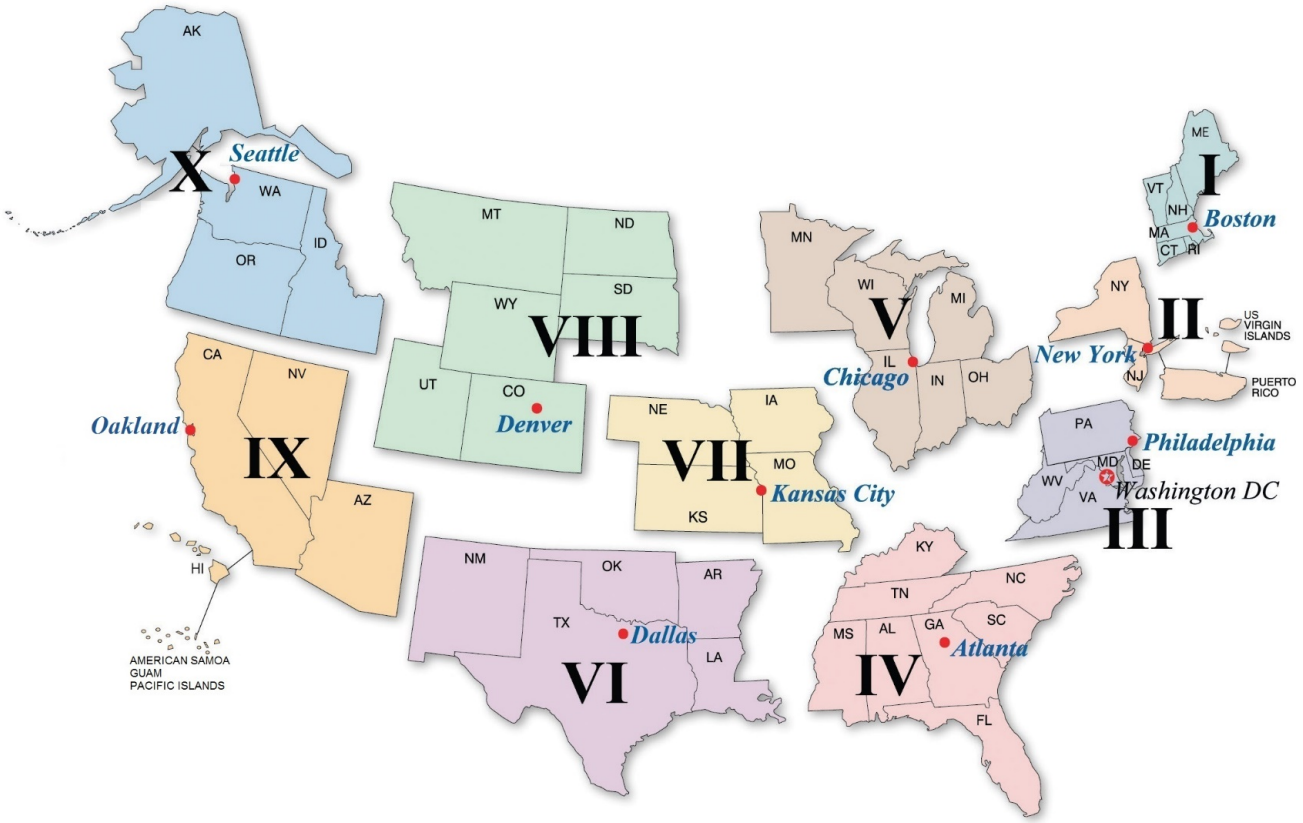
CISA 2020 Priorities - #Protect2020 Strategic Plan

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.

CISA
CYBER+INFRASTRUCTURE

LOE 1: Protect Election Infrastructure

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



CISA
CYBER+INFRASTRUCTURE

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

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

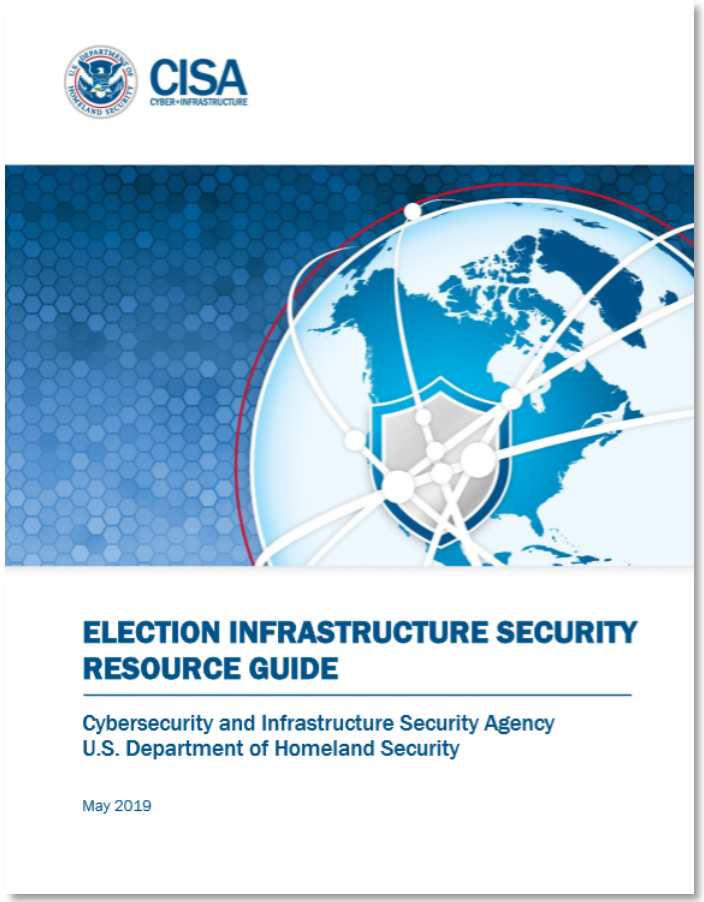
Assessments and Services

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

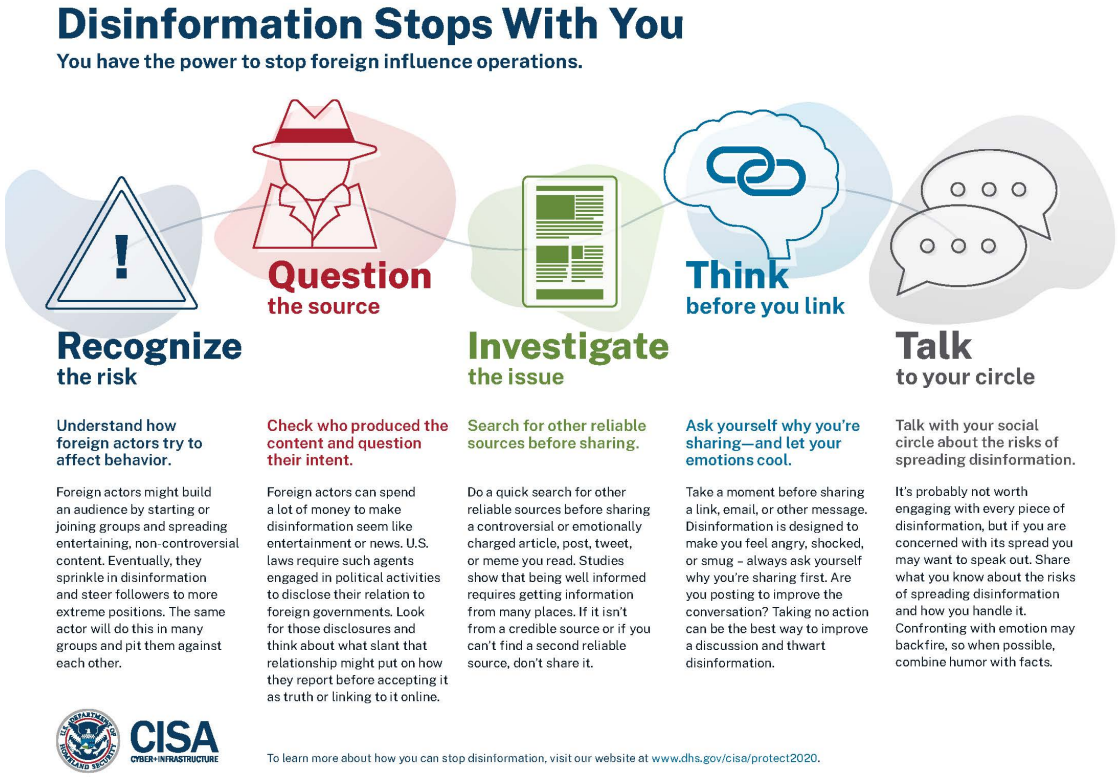
- Understand and evaluate the threat
  - Partner with SMEs and federal counterparts
  - Identify targeted audiences
  - Identify possible foreign narratives and efforts
- Build Public Awareness
  - Develop informational products and toolkits
  - Engage trusted voices
  - Amplify election officials
-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

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



CISA
CYBER+INFRASTRUCTURE

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

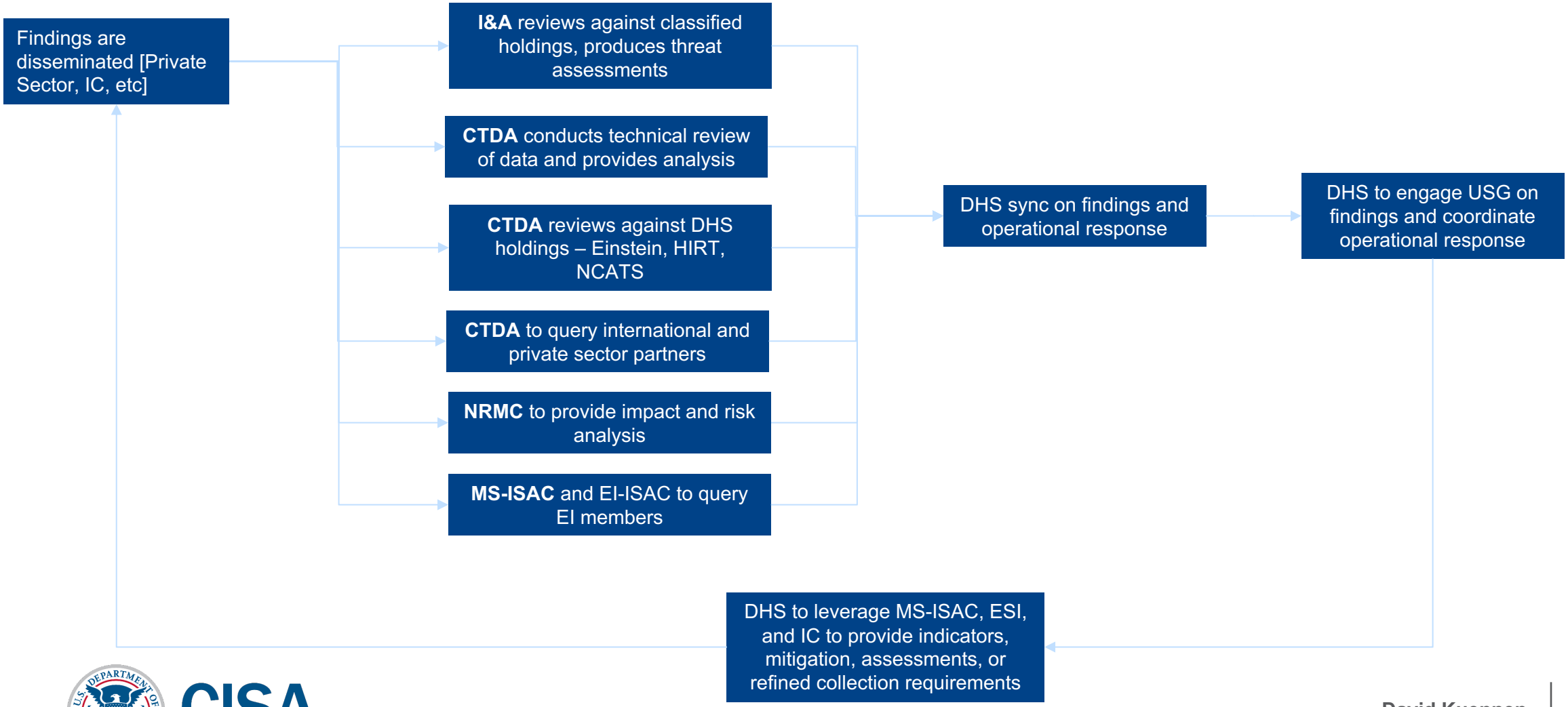
Monitor threat Activity

- 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
CYBER+INFRASTRUCTURE

CISA
CYBER+INFRASTRUCTURE

CISA Election Security 101

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