ELECTION SECURITY OVERVIEW
2021 NASS SUMMER CONFERENCE

Opening Remarks

CISA Leadership

Jen Easterly, Director

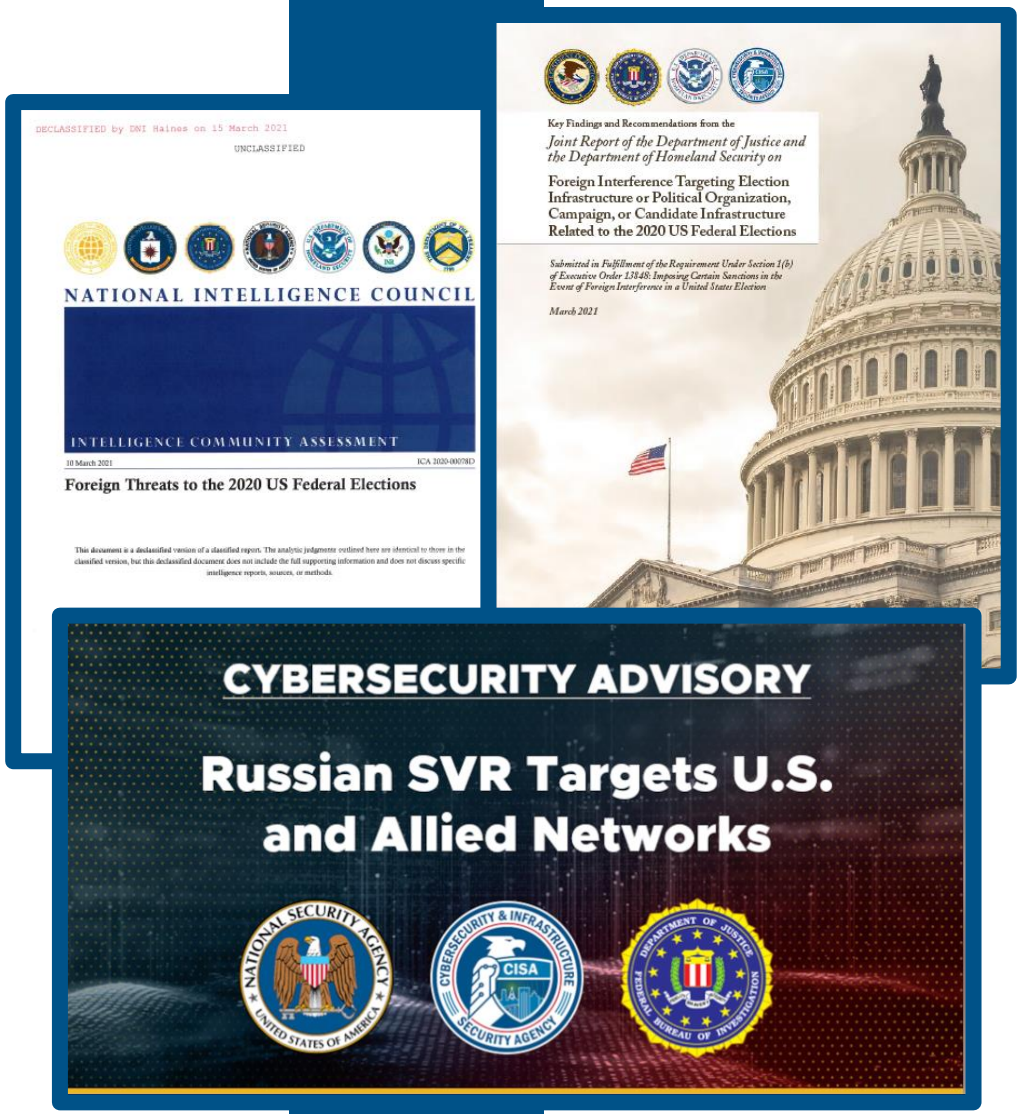
Threat Landscape

2016

- Russian APT cyber and influence activity

2020/2021

- E-Day: “Just another Tuesday on the Internet”
- Russian APT cyber and influence activity
- Iranian APT cyber and influence activity
- Enemies of the People
- Mis- and Disinformation
- SolarWinds
- Microsoft Exchange Server
- Colonial pipeline ransomware
- Kaseya ransomware



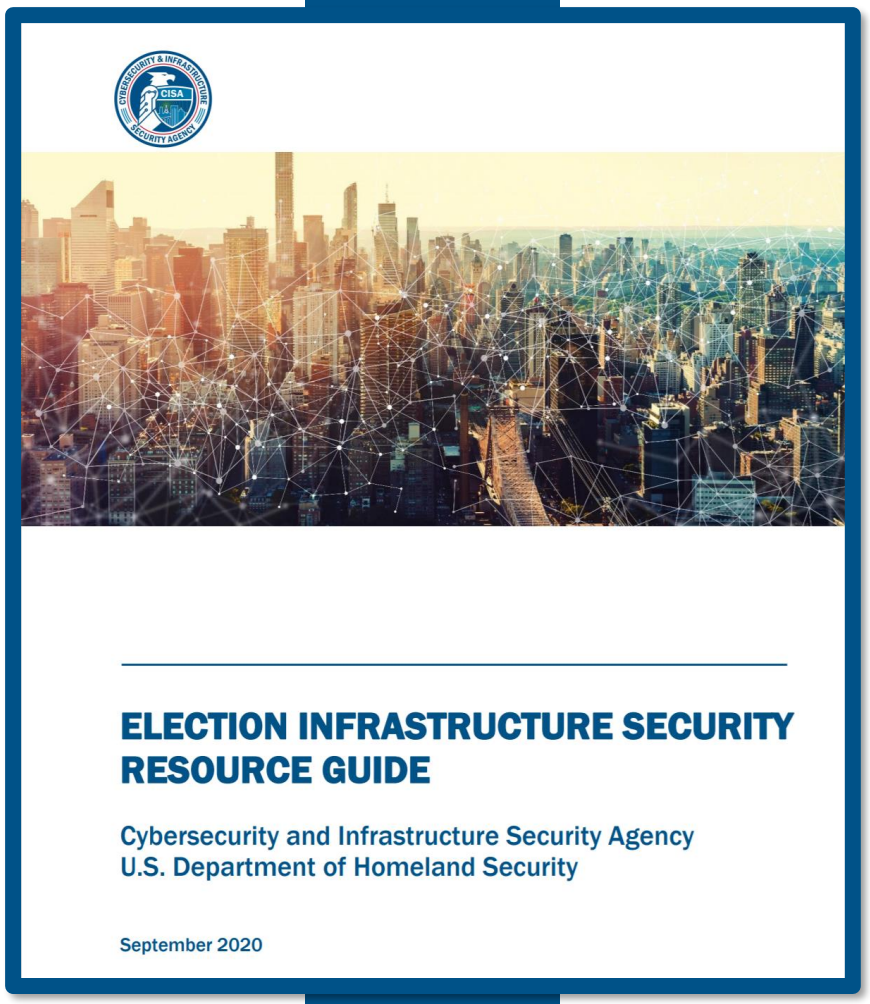
Cybersecurity Services

CISA Services

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

CISA Election Security Trainings

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



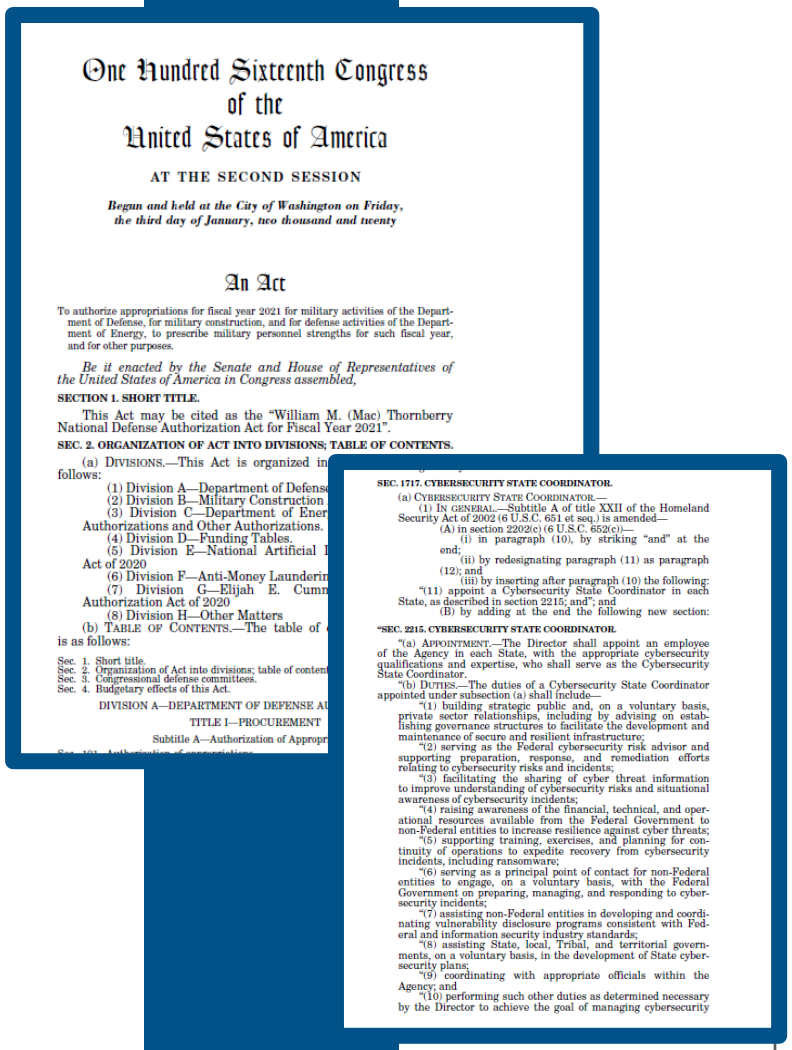
Cybersecurity State Coordinators (CSC)

CSC Key Roles Outlined in the FY21 NDAA

- Serve as Federal cybersecurity risk advisor in the state
- Facilitate cyber threat info-sharing
- Raise awareness of Federal cybersecurity resources
- Support trainings and exercises
- Assist in developing vulnerability disclosure programs

Cybersecurity Advisors (CSAs) Roles Remain Unchanged

- Provide assistance to SLTT governments and CI owners/operators
- Introduce organizations to CISA products and services
- Provide preparedness, assessments, resources, messaging, incident coordination, etc.



One Hundred Sixteenth Congress
of the
United States of America

AT THE SECOND SESSION

Begun and held at the City of Washington on Friday, the third day of January, two thousand and twenty

An Act

To authorize appropriations for fiscal year 2021 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021".

SEC. 2. ORGANIZATION OF ACT INTO DIVISIONS; TABLE OF CONTENTS.

(a) DIVISIONS.—This Act is organized in
follows:
(1) Division A—Department of Defens
(2) Division B—Military Construction
(3) Division C—Department of Ener
Authorizations and Other Authorizations.
(4) Division D—Funding Tables.
(5) Division E—National Artificial I
Act of 2020
(6) Division F—Anti-Money Launderin
(7) Division G—Elijah E. Cumm
Authorization Act of 2020
(8) Division H—Other Matters
(b) TABLE OF CONTENTS.—The table of
is as follows:

Sec. 1. Short title.
Sec. 2. Organization of Act into divisions; table of content
Sec. 3. Congressional defense committees.
Sec. 4. Budgetary effects of this Act.

DIVISION A—DEPARTMENT OF DEFENSE A

TITLE I—PROCUREMENT

Subtitle A—Authorization of Appropr

SEC. 1717. CYBERSECURITY STATE COORDINATOR.

(a) CYBERSECURITY STATE COORDINATOR.—
(1) IN GENERAL.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—
(A) in section 2202(c) (6 U.S.C. 652(c))—
(i) in paragraph (10), by striking "and" at the end;
(ii) by redesignating paragraph (11) as paragraph (12); and
(iii) by inserting after paragraph (10) the following:
"(11) appoint a Cybersecurity State Coordinator in each State, as described in section 2215; and"; and
(B) by adding at the end the following new section:

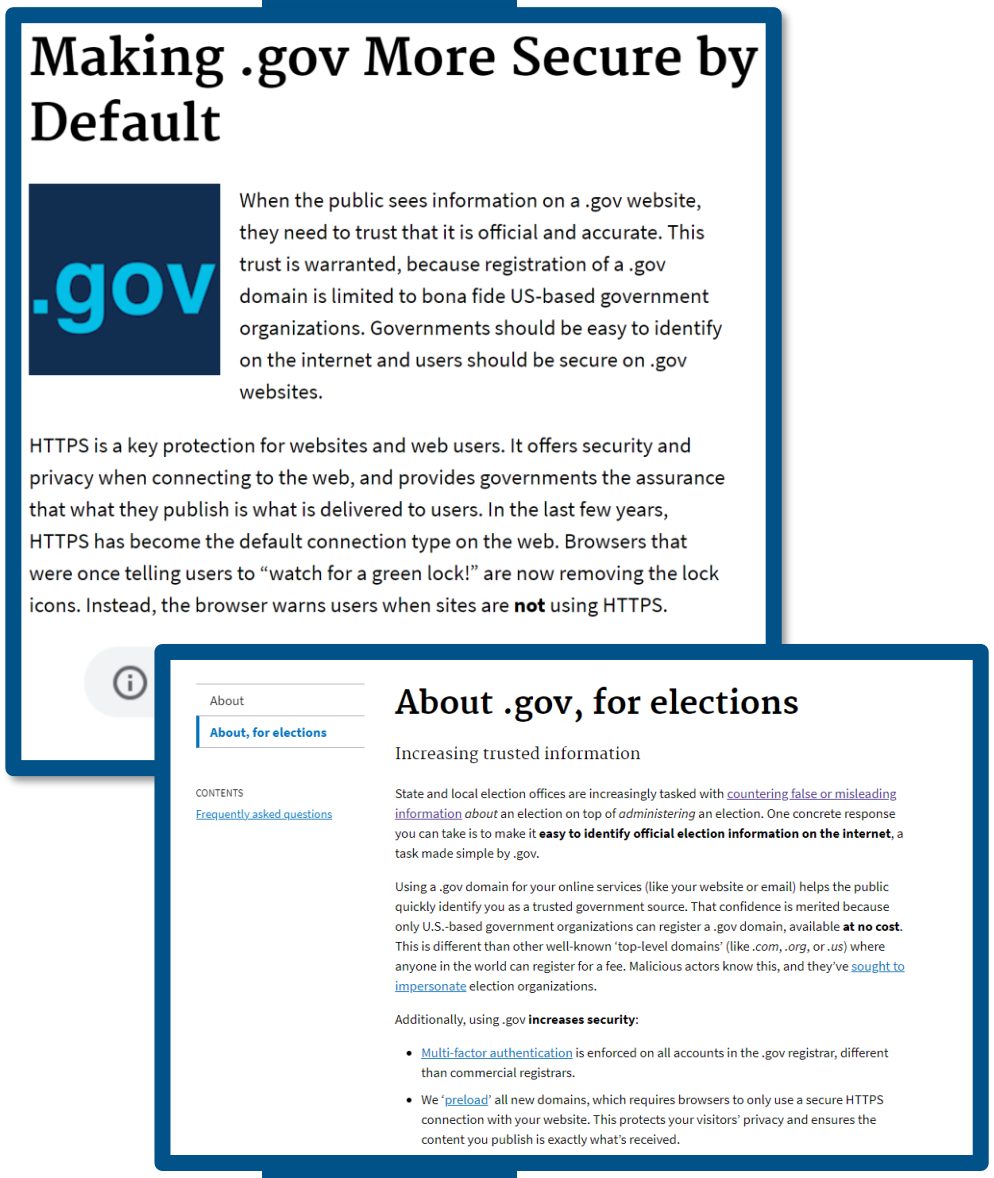
"SEC. 2215. CYBERSECURITY STATE COORDINATOR.

"(a) APPOINTMENT.—The Director shall appoint an employee of the Agency in each State, with the appropriate cybersecurity qualifications and expertise, who shall serve as the Cybersecurity State Coordinator.
"(b) DUTIES.—The duties of a Cybersecurity State Coordinator appointed under subsection (a) shall include—
"(1) building strategic public and, on a voluntary basis, private sector relationships, including by advising on establishing governance structures to facilitate the development and maintenance of secure and resilient infrastructure;
"(2) serving as the Federal cybersecurity risk advisor and supporting preparation, response, and remediation efforts relating to cybersecurity risks and incidents;
"(3) facilitating the sharing of cyber threat information to improve understanding of cybersecurity risks and situational awareness of cybersecurity incidents;
"(4) raising awareness of the financial, technical, and operational resources available from the Federal Government to non-Federal entities to increase resilience against cyber threats;
"(5) supporting training, exercises, and planning for continuity of operations to expedite recovery from cybersecurity incidents, including ransomware;
"(6) serving as a principal point of contact for non-Federal entities to engage, on a voluntary basis, with the Federal Government on preparing, managing, and responding to cybersecurity incidents;
"(7) assisting non-Federal entities in developing and coordinating vulnerability disclosure programs consistent with Federal and information security industry standards;
"(8) assisting State, local, Tribal, and territorial governments, on a voluntary basis, in the development of State cybersecurity plans;
"(9) coordinating with appropriate officials within the Agency; and
"(10) performing such other duties as determined necessary by the Director to achieve the goal of managing cybersecurity

.GOV Top-Level Domain

DOTGOV Act of 2020

- Under CISA, .gov domains are available at **no cost** for qualifying organizations
- Increased use of .gov domains will **improve cybersecurity and trust** in public services across the United States
- It should be easy for the public to know they are engaged with a government agency
- Released new "**About. gov, for elections**" page on the DotGov website: https://home.dotgov.gov/about/elections/



Making .gov More Secure by Default

.gov

When the public sees information on a .gov website, they need to trust that it is official and accurate. This trust is warranted, because registration of a .gov domain is limited to bona fide US-based government organizations. Governments should be easy to identify on the internet and users should be secure on .gov websites.

HTTPS is a key protection for websites and web users. It offers security and privacy when connecting to the web, and provides governments the assurance that what they publish is what is delivered to users. In the last few years, HTTPS has become the default connection type on the web. Browsers that were once telling users to "watch for a green lock!" are now removing the lock icons. Instead, the browser warns users when sites are **not** using HTTPS.

About

About, for elections

CONTENTS

Frequently asked questions

About .gov, for elections

Increasing trusted information

State and local election offices are increasingly tasked with countering false or misleading information *about* an election on top of *administering* an election. One concrete response you can take is to make it **easy to identify official election information on the internet**, a task made simple by .gov.

Using a .gov domain for your online services (like your website or email) helps the public quickly identify you as a trusted government source. That confidence is merited because only U.S.-based government organizations can register a .gov domain, available **at no cost**. This is different than other well-known 'top-level domains' (like *.com*, *.org*, or *.us*) where anyone in the world can register for a fee. Malicious actors know this, and they've sought to impersonate election organizations.

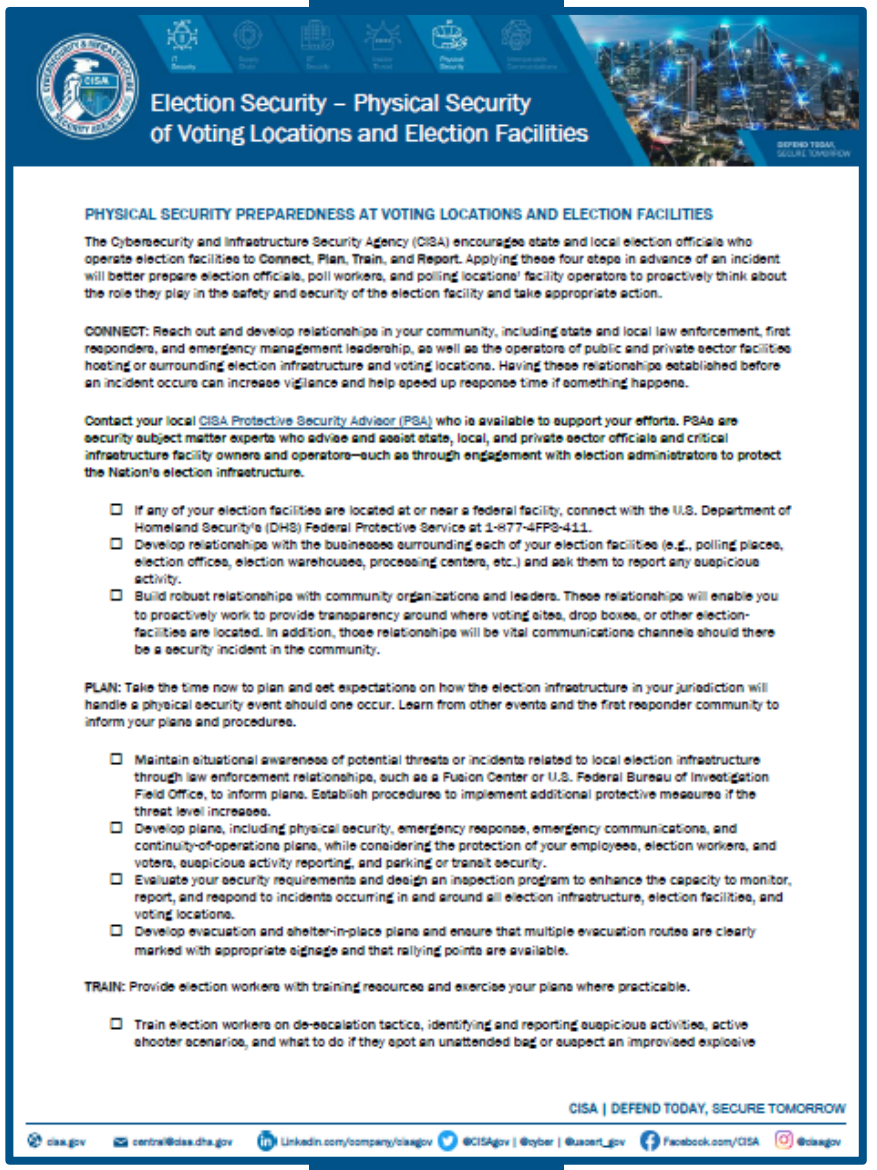
Additionally, using .gov **increases security**:

- Multi-factor authentication is enforced on all accounts in the .gov registrar, different than commercial registrars.
- We 'preload' all new domains, which requires browsers to only use a secure HTTPS connection with your website. This protects your visitors' privacy and ensures the content you publish is exactly what's received.

Physical Security

CISA resources available to election officials

- Protective Security Advisors
- Physical Security Assessments
- Physical Security at Voting Locations and Election Facilities Guide
- Hometown Security page and resources: https://www.cisa.gov/hometown-security
- Mitigating the Impacts of Doxing on Critical Infrastructure Guidance



Election Security – Physical Security of Voting Locations and Election Facilities

PHYSICAL SECURITY PREPAREDNESS AT VOTING LOCATIONS AND ELECTION FACILITIES

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

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

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

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

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

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

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

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

CISA | DEFEND TODAY, SECURE TOMORROW

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

Physical Security

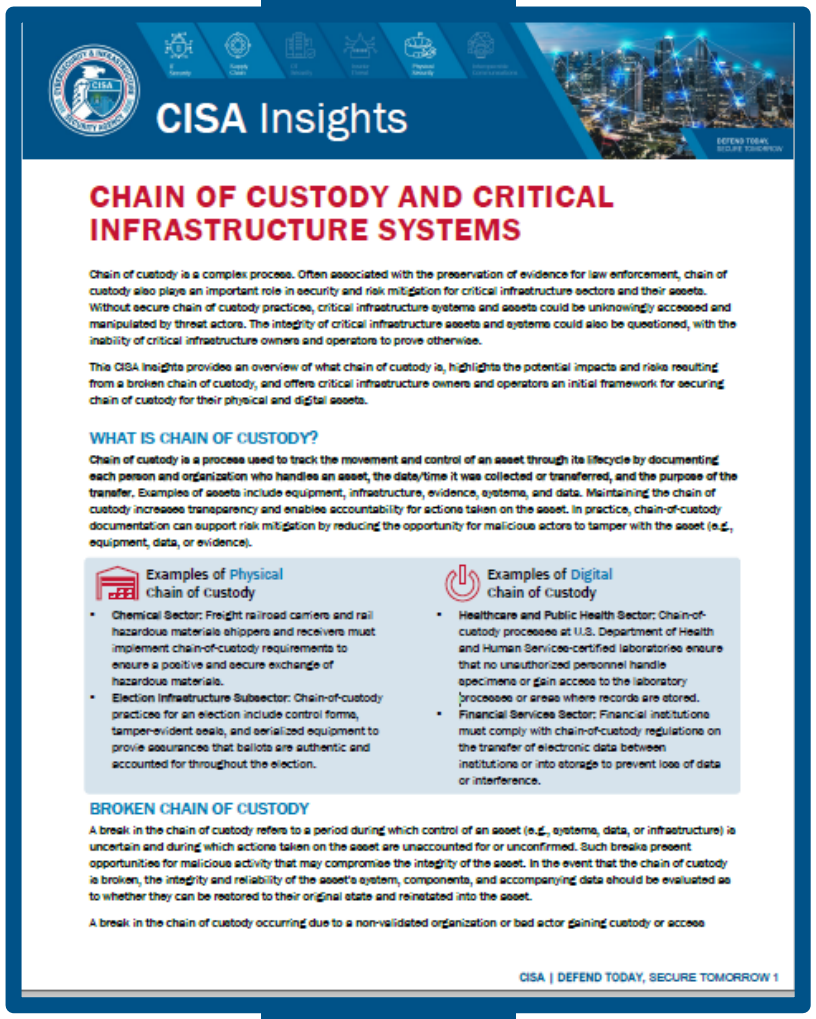
Coordinated Federal Support

- Report immediate threats to local law enforcement (9-1-1)
- Report threats and violent acts to the FBI at 1-CALL-FBI (225-5324), prompt 1, then prompt 3
- DOJ, DHS, FBI, and others are working together in recognition of increasing threats against election workers/administrators/officials

Chain of Custody Guidance

Released by CISA in August 2021

- Chain of custody is a security consideration across critical infrastructure
- Tracking control of data and assets to ensure transparency, accountability, and trust
- Highlights **impacts and risks** from a broken chain of custody
  - The integrity of the system and its data will be deemed untrustworthy
  - A court of law can render the system and data inadmissible
  - Inability to definitively determine if an actor has manipulated your systems or data



CISA Insights

CHAIN OF CUSTODY AND CRITICAL INFRASTRUCTURE SYSTEMS

Chain of custody is a complex process. Often associated with the preservation of evidence for law enforcement, chain of custody also plays an important role in security and risk mitigation for critical infrastructure sectors and their assets. Without secure chain of custody practices, critical infrastructure systems and assets could be unknowingly accessed and manipulated by threat actors. The integrity of critical infrastructure assets and systems could also be questioned, with the inability of critical infrastructure owners and operators to prove otherwise.

This CISA Insights provides an overview of what chain of custody is, highlights the potential impacts and risks resulting from a broken chain of custody, and offers critical infrastructure owners and operators an initial framework for securing chain of custody for their physical and digital assets.

WHAT IS CHAIN OF CUSTODY?

Chain of custody is a process used to track the movement and control of an asset through its lifecycle by documenting each person and organization who handles an asset, the date/time it was collected or transferred, and the purpose of the transfer. Examples of assets include equipment, infrastructure, evidence, systems, and data. Maintaining the chain of custody increases transparency and enables accountability for actions taken on the asset. In practice, chain-of-custody documentation can support risk mitigation by reducing the opportunity for malicious actors to tamper with the asset (e.g., equipment, data, or evidence).

Examples of Physical Chain of Custody

- Chemical Sector: Freight railroad carriers and rail hazardous materials shippers and receivers must implement chain-of-custody requirements to ensure a positive and secure exchange of hazardous materials.
- Election Infrastructure Subsector: Chain-of-custody practices for an election include control forms, tamper-evident seals, and serialized equipment to provide assurances that ballots are authentic and accounted for throughout the election.

Examples of Digital Chain of Custody

- Healthcare and Public Health Sector: Chain-of-custody processes at U.S. Department of Health and Human Services-certified laboratories ensure that no unauthorized personnel handle specimens or gain access to the laboratory processes or areas where records are stored.
- Financial Services Sector: Financial institutions must comply with chain-of-custody regulations on the transfer of electronic data between institutions or into storage to prevent loss of data or interference.

BROKEN CHAIN OF CUSTODY

A break in the chain of custody refers to a period during which control of an asset (e.g., systems, data, or infrastructure) is uncertain and during which actions taken on the asset are unaccounted for or unconfirmed. Such breaks present opportunities for malicious activity that may compromise the integrity of the asset. In the event that the chain of custody is broken, the integrity and reliability of the asset's system, components, and accompanying data should be evaluated as to whether they can be restored to their original state and reinstated into the asset.

A break in the chain of custody occurring due to a non-validated organization or bad actor gaining custody or access

CISA | DEFEND TODAY, SECURE TOMORROW 1

Chain of Custody Guidance

A Complex Topic Vastly Oversimplified

Identify

- What do you care about?
- Who is authorized to access and control it?

Protect

- What can they do to the things you care about?
- How do you keep non-authorized people from accessing it?

Detect

- Is there enough evidence to know something happened?
- Can you tell if something occurred and what it was?

Respond

- How will you determine the impact?
- How will you prevent further consequences?
- Do you know what to do next?

Recover

- What will it take to trust the asset again?


CYBERSECURITY & INFRASTRUCTURE
SECURITY AGENCY
CISA