MITIGATING RISK – CHAIN OF CUSTODY

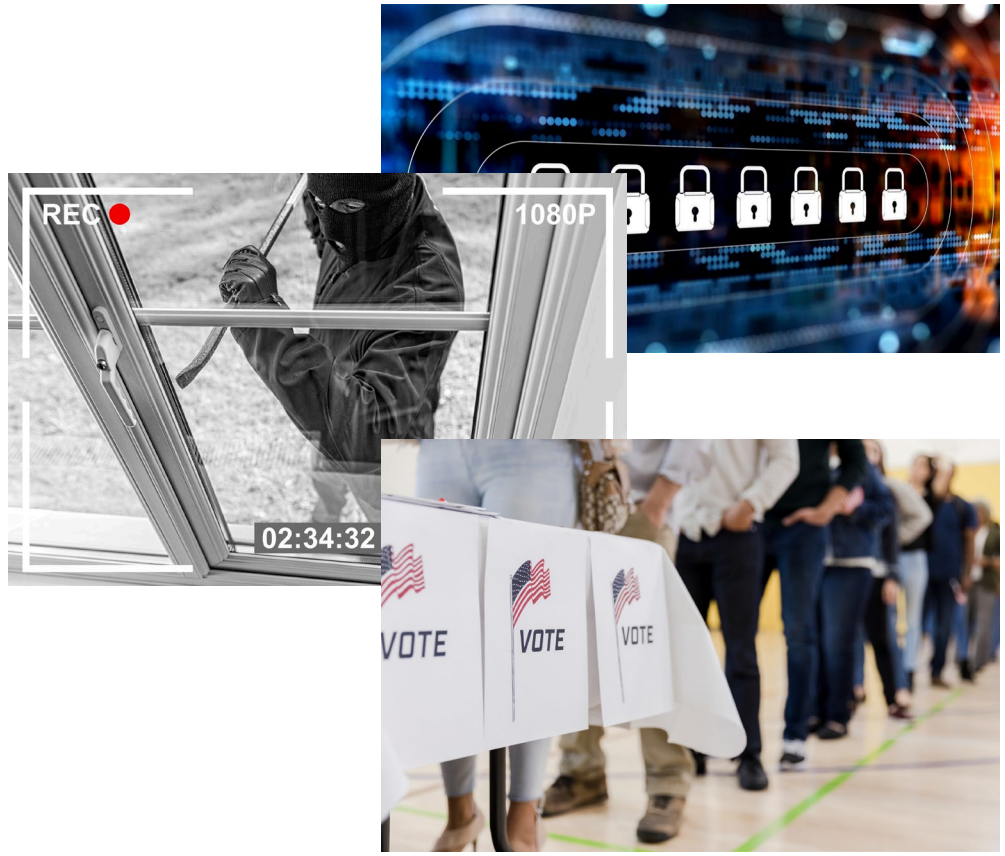
JANUARY 5, 2022

RYAN MACIAS – SME ELECTION SECURITY CONSULTANT, CISA

Risks to Election Infrastructure

- As the nation's **risk advisor**, the Cybersecurity and Infrastructure Security Agency's (CISA) mission is to ensure the security and resiliency of our critical infrastructure

- **Major Risks Facing Election Officials**:
  - Cyber
  - Physical
  - Operational
  - Mis-, Dis-, & Malinformation (MDM)



Chain of Custody Guidance

Released by CISA in August 2021

- Chain of custody is a security consideration across all **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

Chain of custody is a process to track the movement and control of assets by documenting each person and organization who handled an asset, the date/time it was collected or transferred, and the purpose for the transfer.

- **Chain of custody** 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 if critical infrastructure owners and operators are unable to prove otherwise

Chain of Custody Framework

To address risk and improve security and resilience, owners and operators of critical infrastructure can utilize the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) to establish chain-of-custody standards, guidelines, and practices.

Identify: Develop an organizational understanding to manage physical and cybersecurity risk to systems, people, assets, data, and capabilities.

Protect: Develop and implement appropriate safeguards to ensure delivery and security of critical services, systems, and data. Protective measures keep people out.

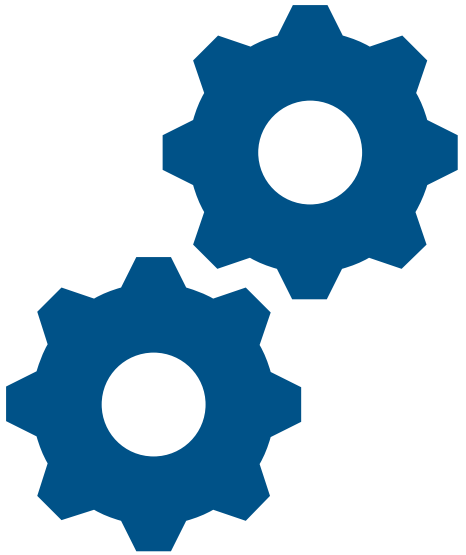
Detect: Develop and implement appropriate activities to identify the occurrence of a chain of custody breach. Detective measures provide evidence that a breach has occurred.

Respond: Develop and implement appropriate activities to act regarding a detected breach of chain of custody.

Recover: Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to the chain of custody breach or cybersecurity incident.

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**
- Breaks present opportunities for **malicious activity** that may **compromise the integrity** of the asset
- The inability to provide evidence that a system has **NOT been compromised** results in the inability to determine if a malicious actor (or any actor for that matter) has gained access to and/or manipulated the systems and data



When a break in the chain of custody occurs, the integrity of the system can no longer be trusted. The reliability, accuracy, and security of records in question – physical or digital – cannot be guaranteed and the systems and data may be rendered inadmissible in a court of law.

Auditing Chain of Custody

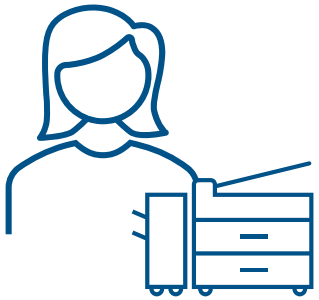
- Routinely audit chain of custody processes to prove that the **authenticity of the data collected has been maintained** across all stages
- Audits should look for **evidence that demonstrates the effectiveness and durability** of the procedures, processes, systems, and training
- Trialing chain of custody processes also provides owners and operators the opportunity to ensure there are no gaps in the chain of custody process, and that **sufficient evidence exists** to maintain a defensible trail of collected data for a litigation or investigation

Elections: Broken Chain of Custody

The loss of chain of custody can lead to doubt about the integrity of elections, fuel mis-, dis-, and malinformation, and result in the release of critical data.

Theft
Taken from the custody of the election

Lost
Missing equipment or data



Maintenance
Transferred to a vendor

Voting
Stored at vote locations

Testing
Provided to a laboratory

Insider Threat Mitigation

Individuals entrusted with access to or knowledge of election infrastructure represent potential risks to the confidentiality, integrity, and availability of elections.

- This includes current and former employees, part-time or temporary workers (e.g., poll workers) vendors, and other individuals with access, understanding, or privilege to election systems (e.g., observers).

Unintentional insider threats are caused by **negligence or accidents**. The risk of unintentional threats can be minimized and mitigated, but never completely prevented.

Examples of Unintentional Threats:

- Allowing someone to "piggyback" through a secure entry point
- Misplacing or losing a portable storage device
- Ignoring messages to install new updates or patches
- Unknowingly or inadvertently clicking on a hyperlink or phishing email

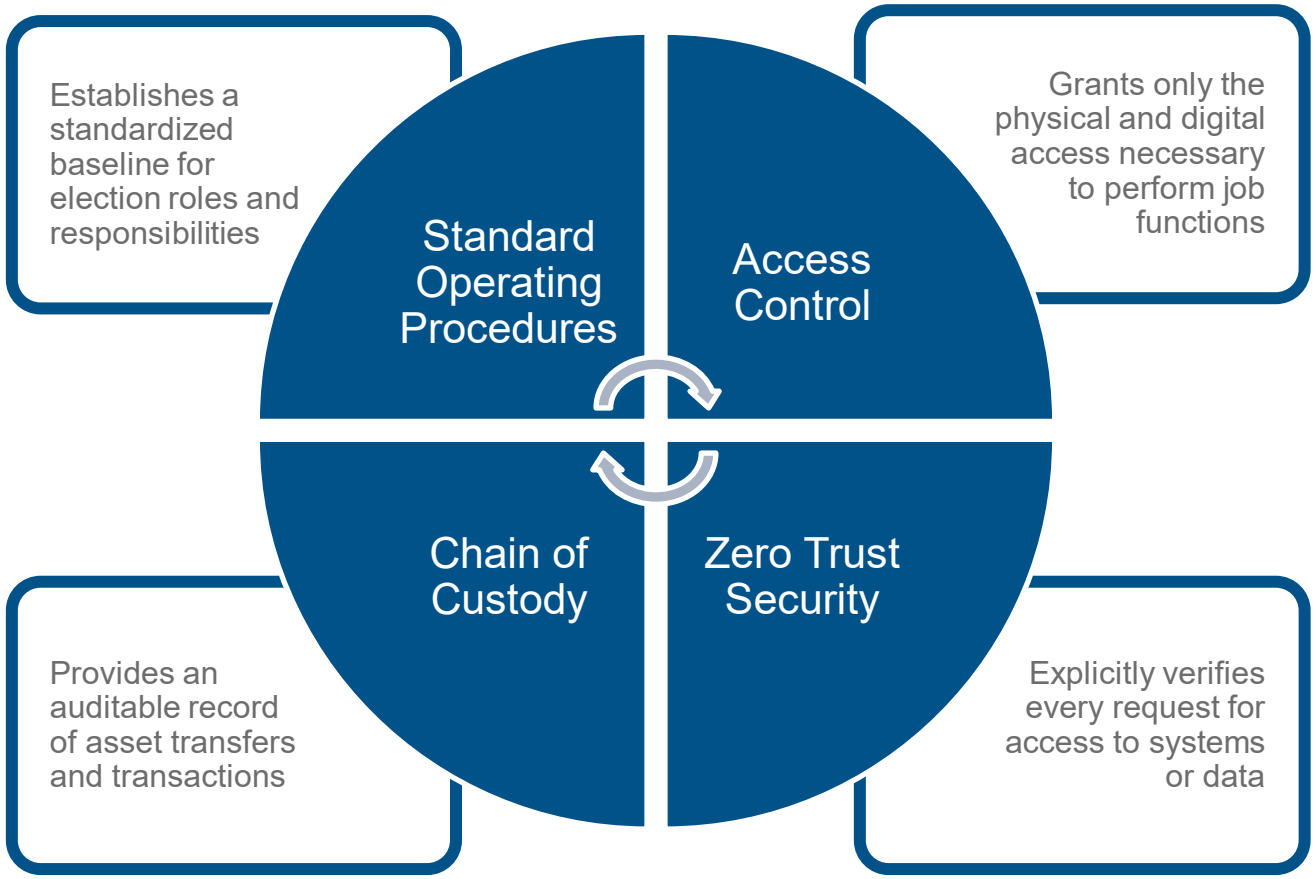
Intentional insider threats occur through **collusion or third-party contractor** threats.

Examples of Intentional Threats:

- Allowing an unauthorized person to access election equipment or systems
- Turning off security cameras or access control systems
- Stealing election equipment
- Leaking confidential information to the press or public
- Intimidating or threatening other staff members

Preventative and Protective Measures

Effective insider threat mitigation programs are built on a strong foundation of accountability, transparency, and trust among all members of the organization.



Detecting and Identifying Threats

Even the most robust preventative and protective measures cannot fully eliminate the risk of insider threats, whether intentional or unintentional. Therefore, it is important to routinely test and audit procedures to identify and respond to evolving threats.

Threat Detection

- **Test election systems and processes** to ensure they are being applied appropriately and audited routinely
- **Monitor systems ongoingly** to identify any errors or unusual activity, including security footage and access logs
- **Conduct internal audits** to validate whether measures such as access control and chain of custody are providing necessary evidence

Threat Assessment

1. Is there evidence to suggest the person of concern poses a threat?
2. What type of threat does the person of concern pose?
3. Is the person of concern moving towards a malicious act?

- Based on the threat assessment, determine whether **emergency** or **non-emergency intervention** is needed
- Non-emergency intervention should involve a deeper investigation to gather information, assess the risk, and determine next steps

Build Your Case - The Three T's

Tracking

- Document your cybersecurity, physical security, and operational security procedures to ensure that the safeguards are enacted and being implemented

Testing

- Verify and audit your processes and procedures, the work of your staff, and the functioning of election infrastructure

Telling (Your Story)

- Provide evidence of why your voters should trust elections and get ahead of likely stories by pre-bunking false narratives before they catch hold, and then quickly rebutting them if they do start to spread
- Use documentation from your Tracking and Testing practices as communication content to share information about secure practices, trustworthy technology, resiliency measures, and general professionalism that stakeholders can trust

Managing Risk: Track

Effective tracking of ballots, voting equipment, and other election assets through robust chain-of-custody and physical security procedures helps election officials manage risk by:

- Reducing the likelihood of malicious actors, including insiders, gaining physical access to voting systems or other election technology assets, and increasing the likelihood that improper access would be detected;
- Enabling robust post-election tabulation audits, which can demonstrate the proper functioning of voting equipment or detect malfunctioning or malware-infected equipment; and
- Provides evidence that demonstrates election security, accuracy, and integrity has been maintained.

Tracking: Critical Assets

Assess your election process to determine which assets are considered critical and highly valuable and can benefit from chain of custody practices.

- Identify and inventory all critical systems, devices, software, data, and people

- Catalog external systems, especially dependent systems, and/or processes outside your control

- Manage access control risk by tracking movement of assets, people, materials, and data

Tracking: What and How

Standard Operating Procedures (SOPs)

Written SOPs can:

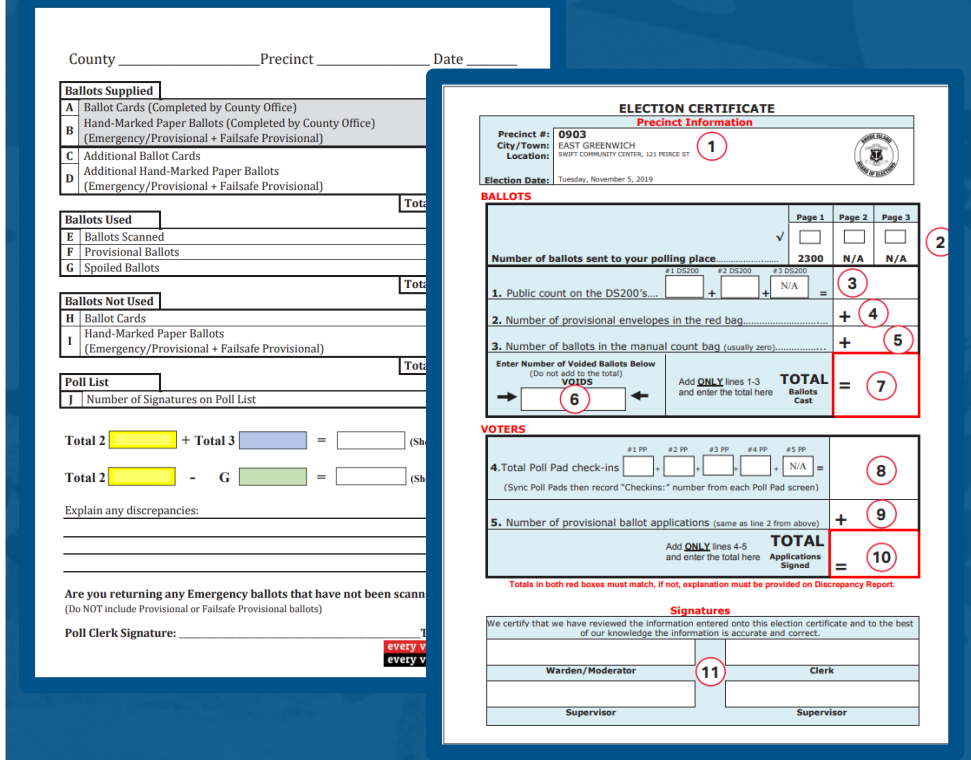
- Limit risks to the operation of election infrastructure
- Limit ad hoc decision making
- Increase quality and consistency of work across staff
- Increase productivity, efficiency and measurement opportunities
- Speed remediation time when following incident response plans

Tracking Control Forms

Control forms capture data at critical points in time to help manage workflow and can provide evidence for audits or incident analysis. Control forms include things like:

- Chain of custody documentation
- Voter registration data entry batch header forms
- Mail ballot envelope batch header forms
- Ballot duplication logs

Examples



Managing Risk: Test

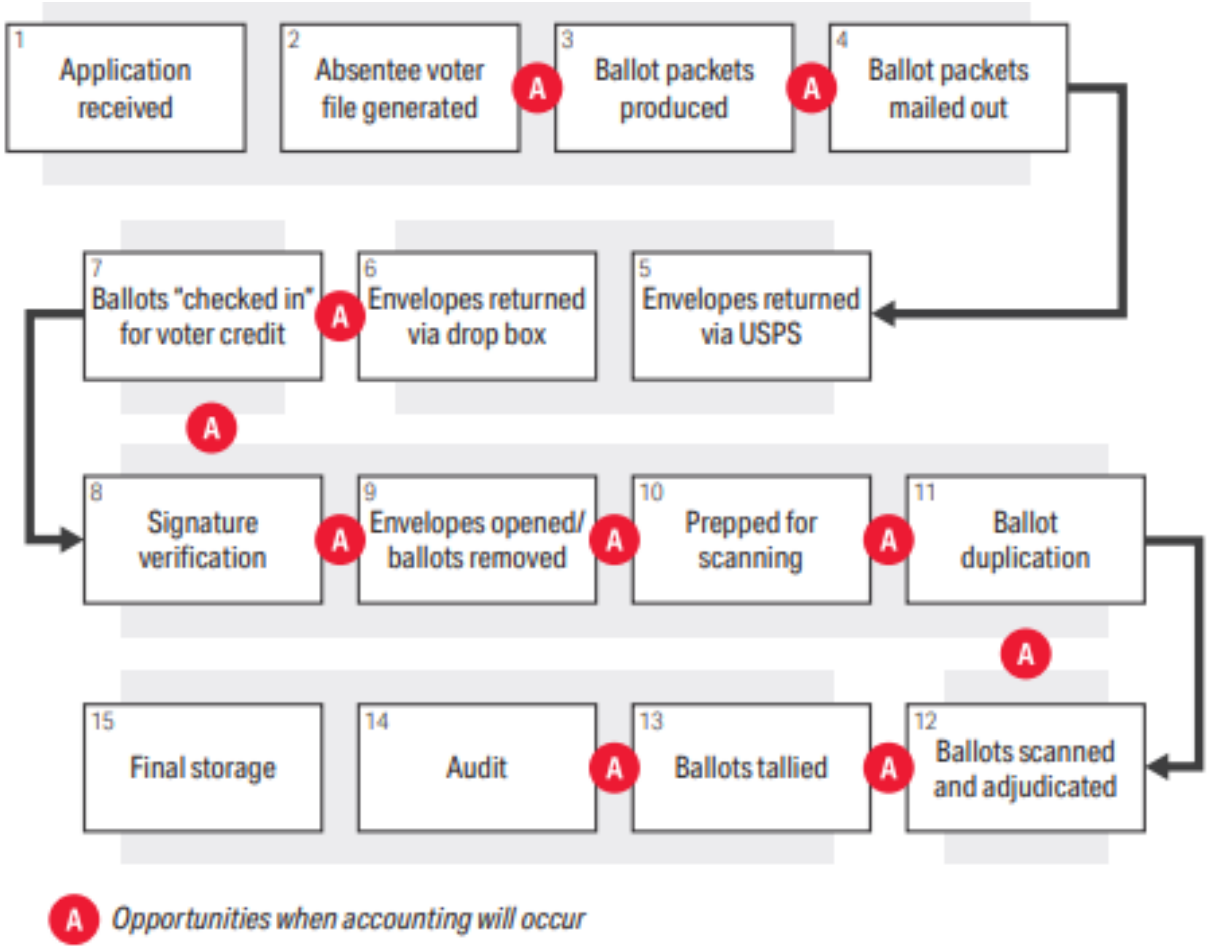
Testing voting equipment and other election assets and processes help election officials manage risk by:

- Demonstrating the proper functioning of voting equipment and other election assets or detecting malfunctioning or malware-infected equipment;
- Identifying strengths and weaknesses in the election office's cybersecurity and physical security risk posture; and
- Ensuring that election workers are operating in the secure manner proscribed in your SOPs.

Testing: Election Audits

Processes to audit include:

- Post-election tabulation audits
- Compliance audits
- Voter registration entry
- Districting using GIS
- Security
- Ballot reconciliation/chain of custody
- Ballot layout and design
- Resource allocation



Managing Risk: Tell

Proactive and responsive communications and transparency measures help election officials manage risk by:

- Bolstering public resilience against MDM narratives and claims;
- Educating voters and the broader public about cybersecurity and physical risks to election infrastructure and the controls put in place to manage such risks; and
- Enabling meaningful public scrutiny of election processes, which can assist with the detection of improper physical access of election assets or malicious cyber activity.

Telling: Who and Why

Who should tell the story of elections?

- Election officials are the absolute authority - they are the trusted source
- Local election officials are closest to the voter
- External validators can add their credibility; political party leadership, local elected officials, and community leaders can spread the good word

Engage the public in the process – encourage public participation

- When feasible, testing and auditing should be open to the public
- Encourage bipartisan participation
- Use the opportunity to educate the public
- Allow for inspection of SOPs, testing logs, audit reports, etc.
- Publicly stream the process so voter can watch from afar and at their convenience

CISA
CYBER+INFRASTRUCTURE

Ryan Macias
SME Election Security Consultant
electionsecurity@hq.dhs.gov

For more information:
www.cisa.gov/election-security
Contact CISA:
Central@cisa.dhs.gov


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY

Election Security Planning Snapshot

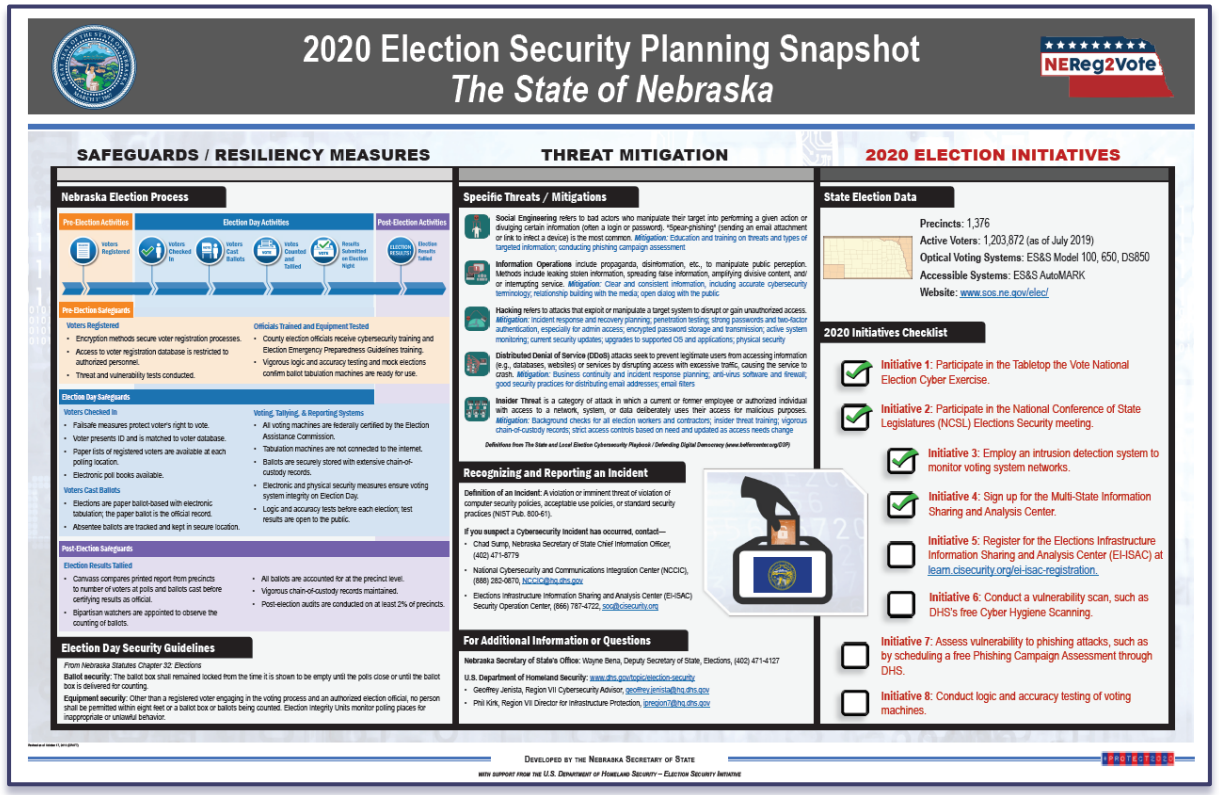
OVERVIEW

What it is

- **High-level snapshot,** highlighting what states and localities are doing to protect their elections
- **Fully customizable product,** created in collaboration with each state to feature the content and layout needed to meet their needs
- **Applicable to State and/or locality level**, tailored to match how the elections are managed and secured

What it is used for

- Educate stakeholders (e.g., staff, leadership, regulators, voters) on existing safeguards and security measures
- Identify mitigative measures employed and develop an action plan of priorities for building resilience
- Inform policymakers and budget holders on the resources needed to continuously manage risk

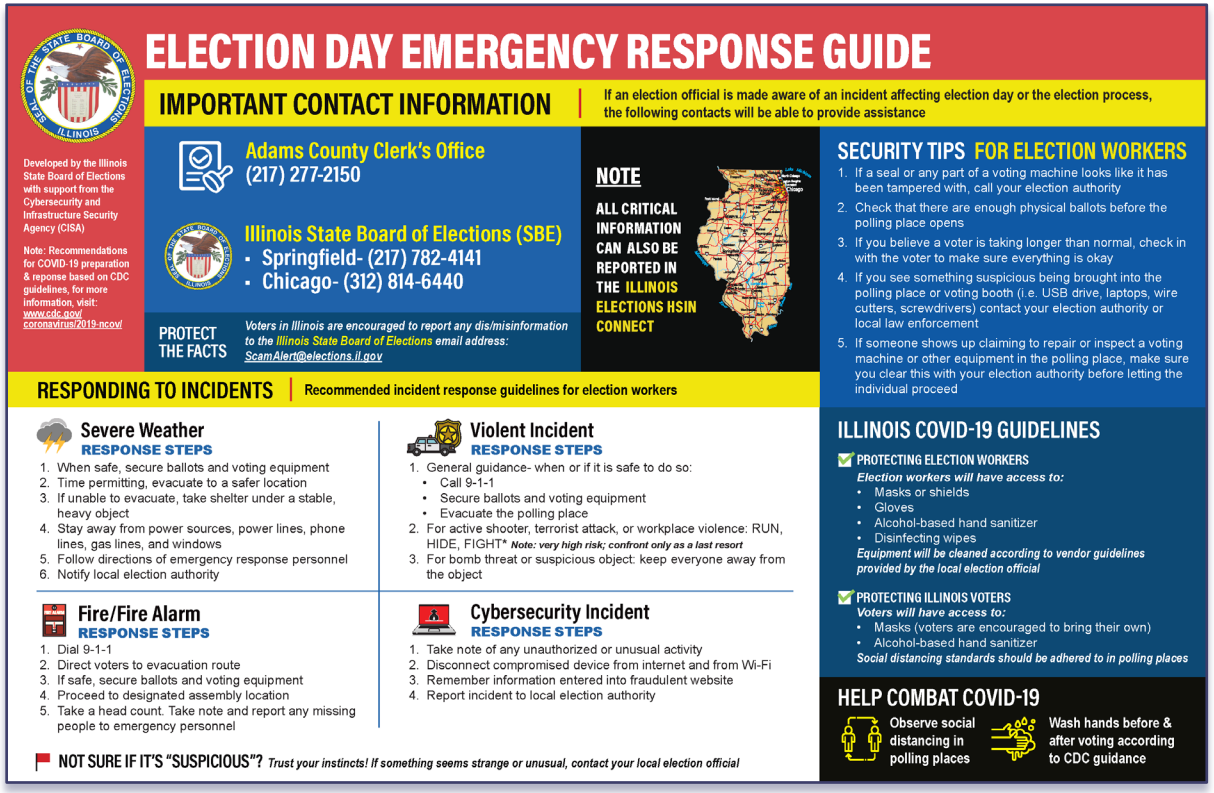


Actual Size: 30" x 20"

Election Emergency Response Guide

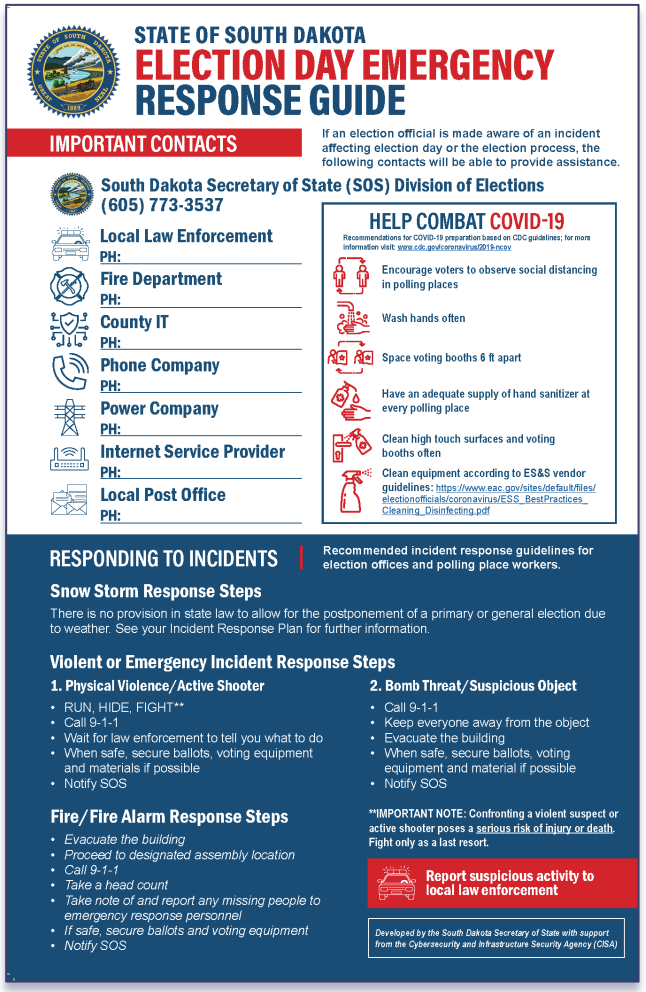
VARIATIONS

The fully customizable nature of the EERG has allowed states to adapt the product to meet evolving election challenges, such as administering an election during the COVID-19 pandemic:



Featuring COVID-19 guidance (11" x 17")

Vertical layout, featuring COVID-19 guidance (11" x 17")



Election Safeguards

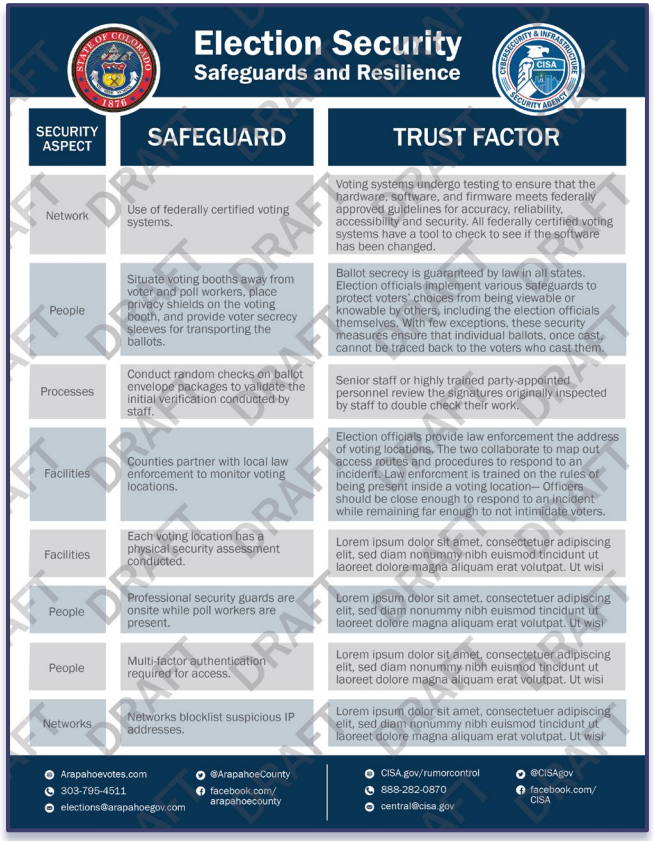
OVERVIEW

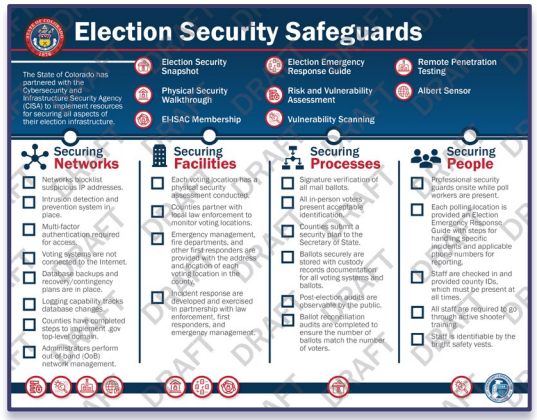
What it is

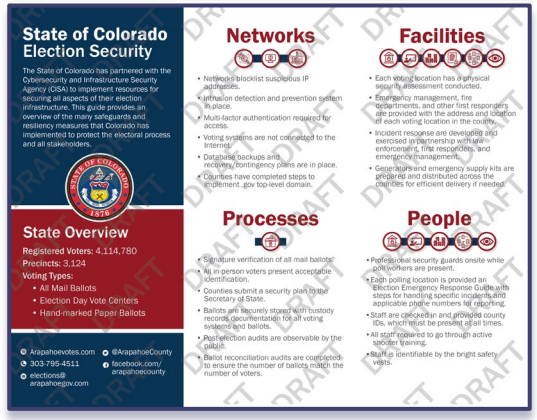
- **Three customizable templates,** tailored to meet the different needs of election administrators and to communicate to different audiences
- **Snapshot of safeguard measures,** identify measures enacted to secure the election infrastructure and to build trust in the process
- **Overview of multiple security aspects**: networks, facilities, processes, and people

What it is used for

- Assess security measures employed and identify potential areas for improvement
- Build trust by communicating safeguards to the public, election workers, and other stakeholders
- Provide information on resources that can be utilized to manage election risks







Three customizable templates