

MITIGATING RISK – CHAIN OF CUSTODY

JANUARY 5, 2022

RYAN MACIAS – SME ELECTION SECURITY CONSULTANT, CISA

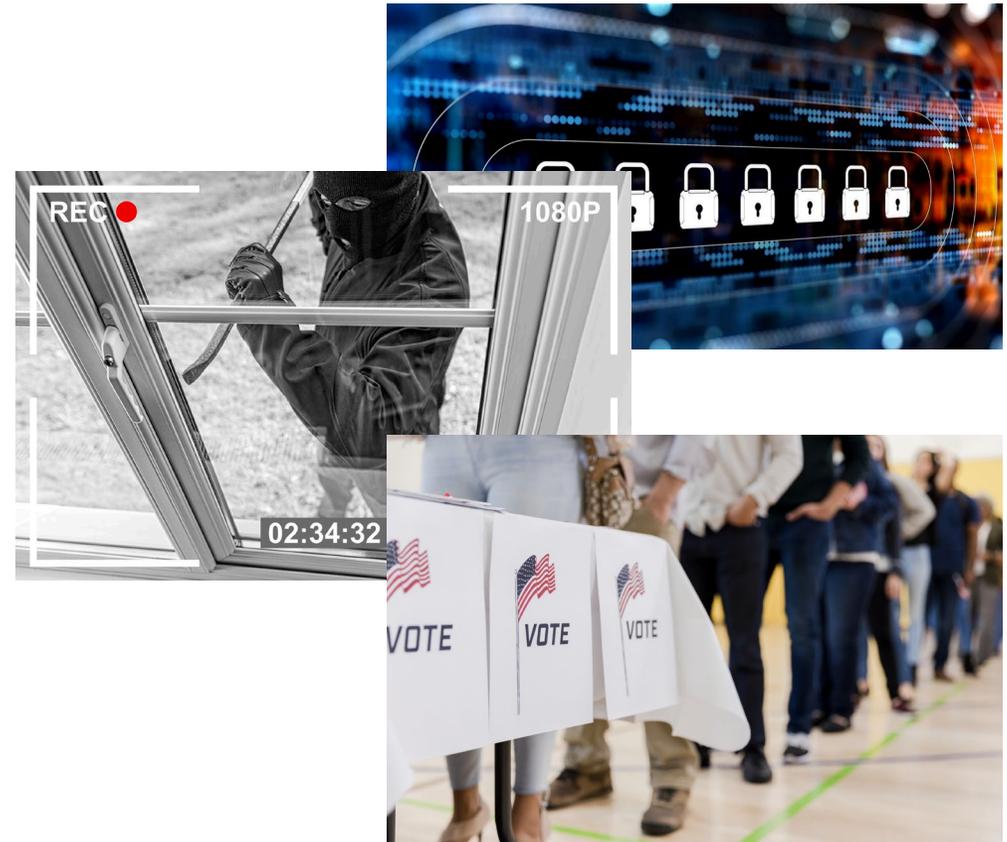


Risks to Election Infrastructure

»» 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	Examples of Digital chain of custody
<ul style="list-style-type: none">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 practice for an election include control forms, tamper-evident seals, and serialized equipment to provide assurance that ballots are authentic and accounted for throughout the election.	<ul style="list-style-type: none">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.

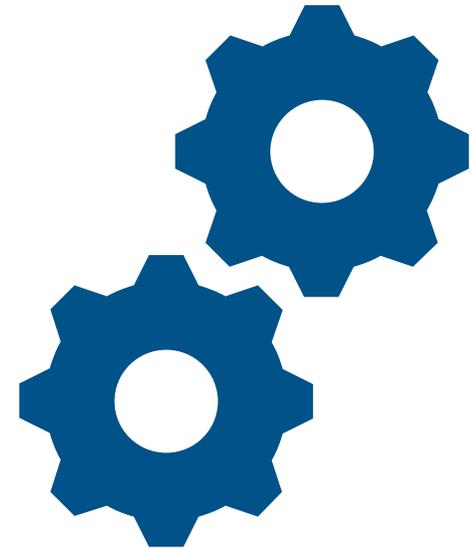


Recover: Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to the chain of custody breach or cybersecurity incident.



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



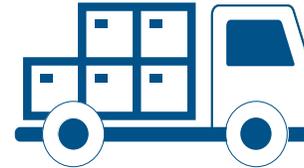
Lost

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.

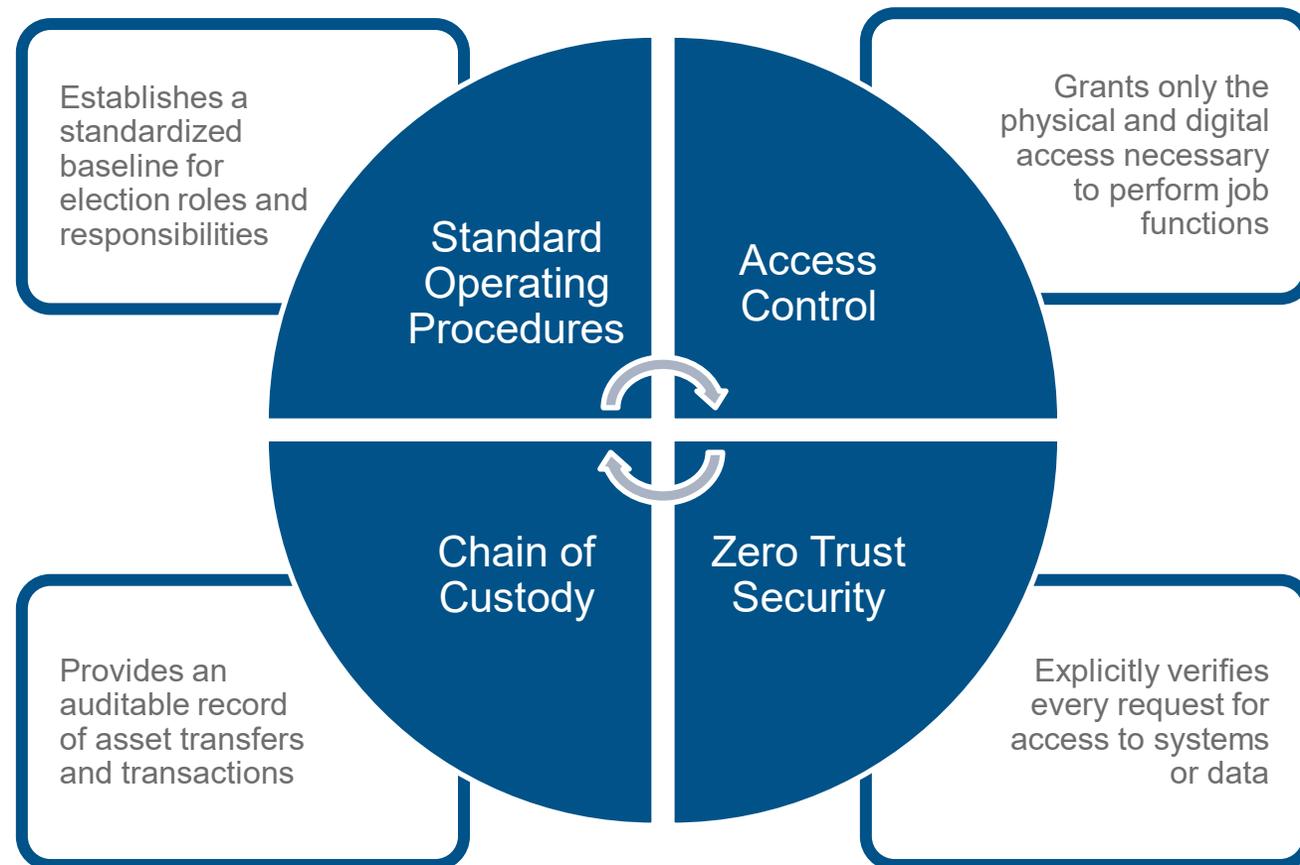
Examples of Intentional Threats:

- 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



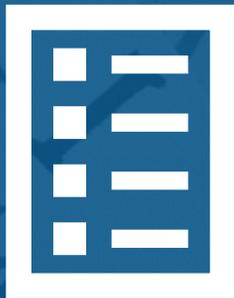
Effective tracking of ballots, voting equipment, and other election assets through robust chain-of-custody and physical security procedures helps election officials manage risk by:

- 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

County _____ Precinct _____ Date _____

Ballots Supplied		Total
A	Ballot Cards (Completed by County Office)	
B	Hand-Marked Paper Ballots (Completed by County Office) (Emergency/Provisional + Failsafe Provisional)	
C	Additional Ballot Cards	
D	Additional Hand-Marked Paper Ballots (Emergency/Provisional + Failsafe Provisional)	
		Total

Ballots Used		Total
E	Ballots Scanned	
F	Provisional Ballots	
G	Spoiled Ballots	
		Total

Ballots Not Used		Total
H	Ballot Cards	
I	Hand-Marked Paper Ballots (Emergency/Provisional + Failsafe Provisional)	
		Total

Poll List	
J	Number of Signatures on Poll List

Total 2 + Total 3 = (Sh

Total 2 - G = (Sh

Explain any discrepancies:

Are you returning any Emergency ballots that have not been scanned (Do NOT include Provisional or Failsafe Provisional ballots)

Poll Clerk Signature: _____ every v

ELECTION CERTIFICATE
Precinct Information

Precinct #: **0903**
City/Town: EAST GREENWICH
Location: SWIFT COMMUNITY CENTER, 121 PEARCE ST **1**

Election Date: Tuesday, November 5, 2019

BALLOTS	Page 1	Page 2	Page 3
	Number of ballots sent to your polling place	2300	N/A
1. Public count on the DS200's...	3		
2. Number of provisional envelopes in the red bag	4		
3. Number of ballots in the manual count bag (usually zero)	5		
Enter Number of Voided Ballots Below (Do not add to the total) VOIDS	6		
TOTAL Ballots Cast	7		

VOTERS	#1 PP	#2 PP	#3 PP	#4 PP	#5 PP
	4. Total Poll Pad check-ins				
5. Number of provisional ballot applications (same as line 2 from above)	9				
TOTAL Applications Signed	10				

Totals in both red boxes must match, if not, explanation must be provided on Discrepancy Report.

Signatures

We certify that we have reviewed the information entered onto this election certificate and to the best of our knowledge the information is accurate and correct.

Warden/Moderator 11	Clerk
Supervisor	Supervisor



Managing Risk: Test



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

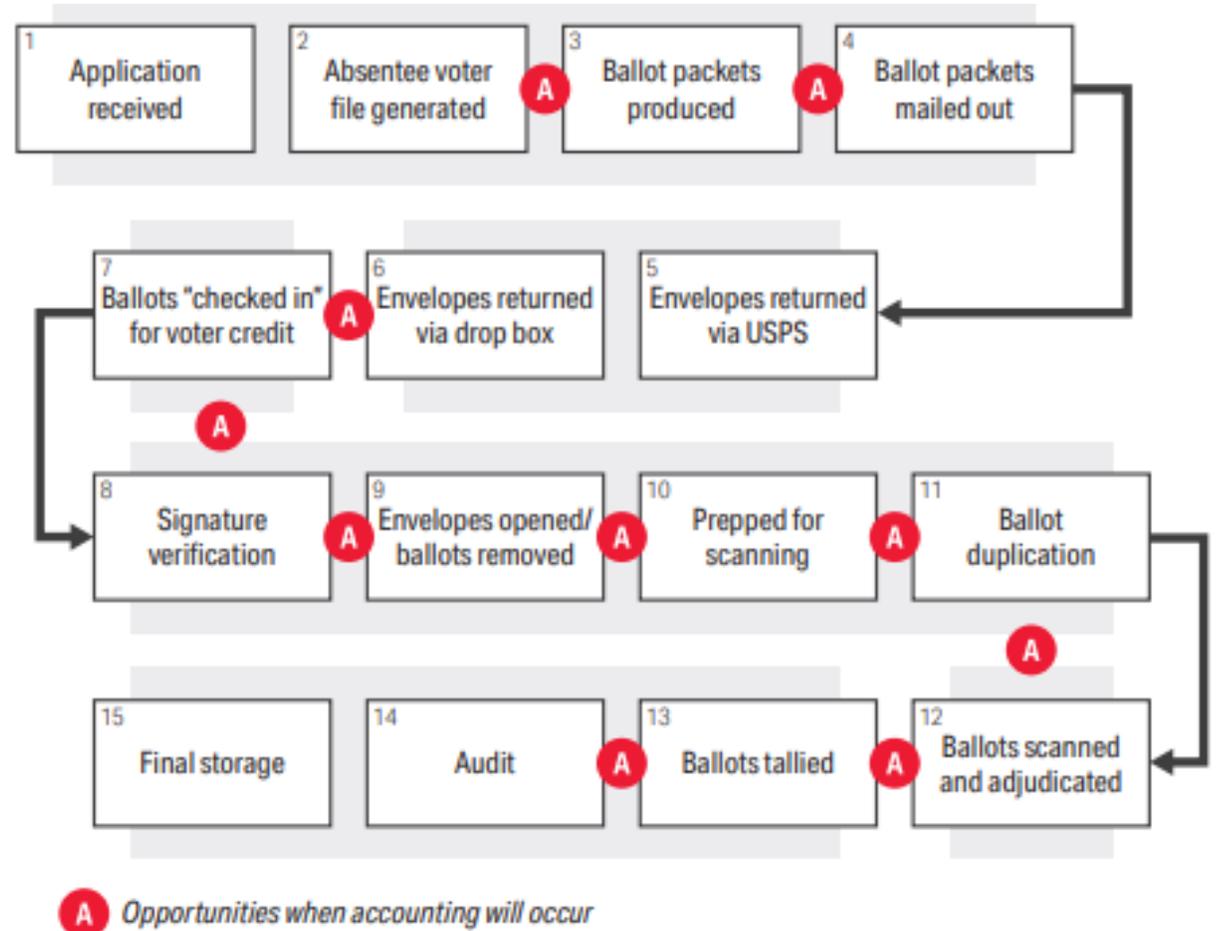
- Demonstrating the proper functioning of voting equipment and other election assets or detecting malfunctioning or malware-infected equipment;
- Identifying strengths and weaknesses in the election office's cybersecurity and physical security risk posture; and
- Ensuring that election workers are operating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





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

2020 Election Security Planning Snapshot
The State of Nebraska

SAFEGUARDS / RESILIENCY MEASURES

Nebraska Election Process

Pre-Election Activities: Voters Registration, Ballot Check-in, Ballot Distribution, Ballot Counting, Results Reporting.

Pre-Election Safeguards:

- Voters Registered:
 - Encryption methods secure voter registration processes.
 - Access to voter registration database is restricted to authorized personnel.
 - Threat and vulnerability tests conducted.
- Officials Trained and Equipment Tested:
 - County election officials receive cybersecurity training and Election Emergency Preparedness Guidelines training.
 - Vigorous logic and accuracy testing and mock elections confirm ballot tabulation machines are ready for use.
- Election Day Safeguards:
 - Voters Checked-In:
 - Fail-safe measures protect voters' right to vote.
 - Voter presents ID and is matched to voter database.
 - Paper lists of registered voters are available at each polling location.
 - Electronic poll books available.
 - Voters Cast Ballots:
 - Elections are paper ballot-based with electronic tabulation; the paper ballot is the official record.
 - Absentee ballots are tracked and kept in secure location.
- Post-Election Safeguards:
 - Election Results Tabulated:
 - Counties compare printed report from precincts to number of votes at polls and ballots cast before certifying results as official.
 - Bipartisan watchers are appointed to observe the counting of ballots.
 - All ballots are accounted for at the precinct level.
 - Vigorous chain-of-custody records maintained.
 - Post-election audits are conducted on at least 2% of precincts.

Election Day Security Guidelines

From Nebraska Statutes Chapter 32: Elections

Ballot security: The ballot box shall remain locked from the time it is shown to be empty until the polls close or until the ballot box is delivered for counting.

Equipment security: Other than a registered voter engaging in the voting process and an authorized election official, no person shall be permitted within eight feet of a ballot box or ballots being counted. Election Integrity Units monitor polling places for inappropriate or unlawful behavior.

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. **Mitros:** 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; 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 administrative access; encrypted password storage and transmission; active system monitoring; current security updates; upgrades to supported OS and applications; physical security.
- 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:** Business continuity and incident response planning, anti-virus software and firewall; good security practices for distributing email addresses; email filters.
- 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.

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).

If you suspect a Cybersecurity Incident has occurred, contact—

- Chad Stump, Nebraska Secretary of State Chief Information Officer, (402) 471-4778
- National Cybersecurity and Communications Integration Center (NCCIC), (888) 282-0870, IC2CIC@hhs.dhs.gov
- Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) Security Operation Center, (866) 787-4722, oc@EISAC.dhs.gov

For Additional Information or Questions

Nebraska Secretary of State's Office: Wayne Bena, Deputy Secretary of State, Elections, (402) 471-4127

U.S. Department of Homeland Security: www.dhs.gov/topics/election-security

- Geoffrey Jenista, Region VII Cybersecurity Advisor, geoffrey.jenista@dhs.gov
- Phil Kirk, Region VII Director for Infrastructure Protection, ipregion@dhs.gov

2020 ELECTION INITIATIVES

State Election Data

- Precincts: 1,376
- Active Voters: 1,203,872 (as of July 2019)
- Optical Voting Systems: ES&S Model 100, 650, DS650
- Accessible Systems: ES&S AutoMARK
- Website: www.sos.ne.gov/elec/

2020 Initiatives Checklist

- Initiative 1: Participate in the Tabletop the Vote National Election Cyber Exercise.
- Initiative 2: Participate in the National Conference of State Legislatures (NCSL) Elections Security meeting.
- Initiative 3: Employ an intrusion detection system to monitor voting system networks.
- Initiative 4: Sign up for the Multi-State Information Sharing and Analysis Center.
- Initiative 5: Register for the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) at learn.eisecurity.org/ei-isac-registration.
- Initiative 6: Conduct a vulnerability scan, such as DHS's free Cyber Hygiene Scanning.
- Initiative 7: Assess vulnerability to phishing attacks, such as by scheduling a free Phishing Campaign Assessment through DHS.
- Initiative 8: Conduct logic and accuracy testing of voting machines.

DEVELOPED BY THE NEBRASKA SECRETARY OF STATE
WITH SUPPORT FROM THE U.S. DEPARTMENT OF HOMELAND SECURITY - ELECTION SECURITY INITIATIVE

Actual Size: 30" x 20"



Presenter's Name
January 5, 2022



Election Emergency Response Guide

VARIATIONS

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

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:

ELECTION DAY EMERGENCY RESPONSE GUIDE



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

Note: Recommendations for COVID-19 preparation & response based on CDC guidelines, for more information visit: www.cdc.gov/coronavirus/2019-ncov/

IMPORTANT CONTACT INFORMATION

If an election official is made aware of an incident affecting election day or the election process, the following contacts will be able to provide assistance

Adams County Clerk's Office
(217) 277-2150

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



PROTECT THE FACTS

Voters in Illinois are encouraged to report any dis/misinformation to the Illinois State Board of Elections email address: ScamAlert@elections.il.gov

RESPONDING TO INCIDENTS

Recommended incident response guidelines for election workers

<p>Severe Weather RESPONSE STEPS</p> <ol style="list-style-type: none"> When safe, secure ballots and voting equipment Time permitting, evacuate to a safer location If unable to evacuate, take shelter under a stable, heavy object Stay away from power sources, power lines, phone lines, gas lines, and windows Follow directions of emergency response personnel Notify local election authority 	<p>Violent Incident RESPONSE STEPS</p> <ol style="list-style-type: none"> General guidance- when or if it is safe to do so: <ul style="list-style-type: none"> Call 9-1-1 Secure ballots and voting equipment Evacuate the polling place For active shooter, terrorist attack, or workplace violence: RUN, HIDE, FIGHT* <i>Note: very high risk; confront only as a last resort</i> For bomb threat or suspicious object: keep everyone away from the object
<p>Fire/Fire Alarm RESPONSE STEPS</p> <ol style="list-style-type: none"> Dial 9-1-1 Direct voters to evacuation route If safe, secure ballots and voting equipment Proceed to designated assembly location Take a head count. Take note and report any missing people to emergency personnel 	<p>Cybersecurity Incident RESPONSE STEPS</p> <ol style="list-style-type: none"> Take note of any unauthorized or unusual activity Disconnect compromised device from internet and from Wi-Fi Remember information entered into fraudulent website Report incident to local election authority

■ **NOT SURE IF IT'S "SUSPICIOUS"?** Trust your instincts! If something seems strange or unusual, contact your local election official

SECURITY TIPS FOR ELECTION WORKERS

- If a seal or any part of a voting machine looks like it has been tampered with, call your election authority
- Check that there are enough physical ballots before the polling place opens
- If you believe a voter is taking longer than normal, check in with the voter to make sure everything is okay
- If you see something suspicious being brought into the polling place or voting booth (i.e. USB drive, laptops, wire cutters, screwdrivers) contact your election authority or local law enforcement
- If someone shows up claiming to repair or inspect a voting machine or other equipment in the polling place, make sure you clear this with your election authority before letting the individual proceed

ILLINOIS COVID-19 GUIDELINES

✓ PROTECTING ELECTION WORKERS
Election workers will have access to:

- Masks or shields
- Gloves
- Alcohol-based hand sanitizer
- Disinfecting wipes

Equipment will be cleaned according to vendor guidelines provided by the local election official

✓ PROTECTING ILLINOIS VOTERS
Voters will have access to:

- Masks (voters are encouraged to bring their own)
- Alcohol-based hand sanitizer

Social distancing standards should be adhered to in polling places

HELP COMBAT COVID-19



Observe social distancing in polling places



Wash hands before & after voting according to CDC guidance

STATE OF SOUTH DAKOTA ELECTION DAY EMERGENCY RESPONSE GUIDE

IMPORTANT CONTACTS

South Dakota Secretary of State (SOS) Division of Elections
(605) 773-3537

Local Law Enforcement
PH: _____

Fire Department
PH: _____

County IT
PH: _____

Phone Company
PH: _____

Power Company
PH: _____

Internet Service Provider
PH: _____

Local Post Office
PH: _____

HELP COMBAT COVID-19

Recommendations for COVID-19 preparation based on CDC guidelines; for more information visit: www.cdc.gov/coronavirus/2019-ncov/

-  Encourage voters to observe social distancing in polling places
-  Wash hands often
-  Space voting booths 6 ft apart
-  Have an adequate supply of hand sanitizer at every polling place
-  Clean high touch surfaces and voting booths often
-  Clean equipment according to ES&S vendor guidelines: https://www.esac.gov/sites/default/files/electionofficials/coronavirus/ESSS_BestPractices_Cleaning_Disinfecting.pdf

RESPONDING TO INCIDENTS

Recommended incident response guidelines for election offices and polling place workers.

Snow Storm Response Steps

There is no provision in state law to allow for the postponement of a primary or general election due to weather. See your Incident Response Plan for further information.

Violent or Emergency Incident Response Steps

1. Physical Violence/ Active Shooter

- RUN, HIDE, FIGHT**
- Call 9-1-1
- Wait for law enforcement to tell you what to do
- When safe, secure ballots, voting equipment and materials if possible
- Notify SOS

2. Bomb Threat/ Suspicious Object

- Call 9-1-1
- Keep everyone away from the object
- Evacuate the building
- When safe, secure ballots, voting equipment and material if possible
- Notify SOS

**IMPORTANT NOTE: Confronting a violent suspect or active shooter poses a serious risk of injury or death. Fight only as a last resort.

Fire/Fire Alarm Response Steps

- Evacuate the building
- Proceed to designated assembly location
- Call 9-1-1
- Take a head count
- Take note of and report any missing people to emergency response personnel
- If safe, secure ballots and voting equipment
- Notify SOS

Report suspicious activity to local law enforcement

Developed by the South Dakota Secretary of State with support from the Cybersecurity and Infrastructure Security Agency (CISA)



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

Presenter's Name
January 5, 2022



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

SECURITY ASPECT	SAFEGUARD	TRUST FACTOR
Network	Use of federally certified voting systems.	Voting systems undergo testing to ensure that the hardware, software, and firmware meets federally approved guidelines for accuracy, reliability, accessibility and security. All federally certified voting systems have a tool to check to see if the software has been changed.
People	Situate voting booths away from voters and poll workers, place privacy shields on the voting booth, and provide voter secrecy gloves for transporting the ballots.	Ballot secrecy is guaranteed by law in all states. Election officials implement various safeguards to protect voters' choices from being viewable or knowable by others, including the election officials themselves. With few exceptions, these security measures ensure that individual ballots, once cast, cannot be traced back to the voters who cast them.
Processes	Conduct random checks on ballot envelope packages to validate the initial verification conducted by staff.	Senior staff or highly trained party-appointed personnel review the signatures originally inspected by staff to double check their work.
Facilities	Counties partner with local law enforcement to monitor voting locations.	Election officials provide law enforcement the address of voting locations. The two collaborate to map out access routes and procedures to respond to an incident. Law enforcement is trained on the rules of being present inside a voting location—Officers should be close enough to respond to an incident while remaining far enough to not intimidate voters.
Facilities	Each voting location has a physical security assessment conducted.	Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi
People	Professional security guards are onsite while poll workers are present.	Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi
People	Multi-factor authentication required for access.	Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi
Networks	Networks blacklist suspicious IP addresses.	Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi

Election Security Safeguards

The State of Colorado has partnered with the Cybersecurity and Infrastructure Security Agency (CISA) to implement resources for securing all aspects of their election infrastructure.

- Election Security Snapshot
- Physical Security Walkthrough
- EHSAC Membership
- Election Emergency Response Guide
- Risk and Vulnerability Assessment
- Vulnerability Scanning
- Remote Penetration Testing
- Albert Sensor

Securing Networks

- Networks blacklist suspicious IP addresses.
- Intrusion detection and prevention system in place.
- Multi-factor authentication required for access.
- Writing systems are not connected to the internet.
- Datatable backups and recovery/contingency plans are in place.
- Logging capability enables database changes.
- Counties have equipped steps to implement gov-top-level domain.
- Administrators perform out-of-band (OOB) network management.

Securing Facilities

- Each voting location has a physical security assessment conducted.
- Counties partner with local law enforcement to monitor voting locations.
- Emergency management, fire departments, and other first responders are provided with the address and location of staff voting location in the county.
- Incident response are developed and exercised in partnership with law enforcement, first responders, and emergency management.

Securing Processes

- Signature verification of all mail ballots.
- All in-person voters present acceptable identification.
- Counties submit a security plan to the Secretary of State.
- Ballots are securely stored with custody records documented for all voting systems, test ballots.
- Non-electronic audits are observable by the public.
- Ballot reconciliation audits are completed to ensure the number of ballots match the number of voters.

Securing People

- Professional security guards onsite while poll workers are present.
- Each polling location is provided an Election Emergency Response Guide with steps for handling specific incidents and appropriate phone numbers for reporting.
- Staff are checked in and provided sound kits, which must be present at all times.
- All staff required to go through active shooter training.
- Staff is identifiable by the bright safety vests.

State of Colorado Election Security

The State of Colorado has partnered with the Cybersecurity and Infrastructure Security Agency (CISA) to implement resources for securing all aspects of their election infrastructure. This guide provides an overview of the many safeguards and resiliency measures that Colorado has implemented to protect the electoral process and all stakeholders.

Networks

- Networks blacklist suspicious IP addresses.
- Intrusion detection and prevention system in place.
- Multi-factor authentication required for access.
- Writing systems are not connected to the internet.
- Datatable backups and recovery/contingency plans are in place.
- Counties have equipped steps to implement gov-top-level domain.

Facilities

- Each voting location has a physical security assessment conducted.
- In partnership with law enforcement, fire departments, and other first responders are provided with the address and location of each voting location in the county.
- Incident response are developed and exercised in partnership with law enforcement, first responders, and emergency management.
- Geographic emergency supply kits are provided and distributed across the counties for efficient delivery if needed.

Processes

- Signature verification of all mail ballots.
- All in-person voters present acceptable identification.
- Counties submit a security plan to the Secretary of State.
- Ballots are securely stored with custody records documented for all voting systems, test ballots.
- Non-electronic audits are observable by the public.
- Ballot reconciliation audits are completed to ensure the number of ballots match the number of voters.

People

- Professional security guards onsite while poll workers are present.
- Each polling location is provided an Election Emergency Response Guide with steps for handling specific incidents and appropriate phone numbers for reporting.
- Staff are checked in and provided county ID, which must be present at all times.
- All staff required to go through active shooter training.
- Staff is identifiable by the bright safety vests.

State Overview

Registered Voters: 4,114,780
Precincts: 3,124

Voting Types:

- All Mail Ballots
- Election Day Vote Centers
- Hand-Marked Paper Ballots

- Arapahoevotes.com
- 303-795-4511
- elections@arapahoe.gov

- @ArapahoeCounty
- facebook.com/arapahoeCounty

- CISA.gov/rumorcontrol
- 888-282-0870
- central@cisaa.gov

- @CISAgov
- facebook.com/CISA

Three customizable templates



Presenter's Name
January 5, 2022