# ELECTION SECURITY: BUILDING TRUST THROUGH SECURE PRACTICES

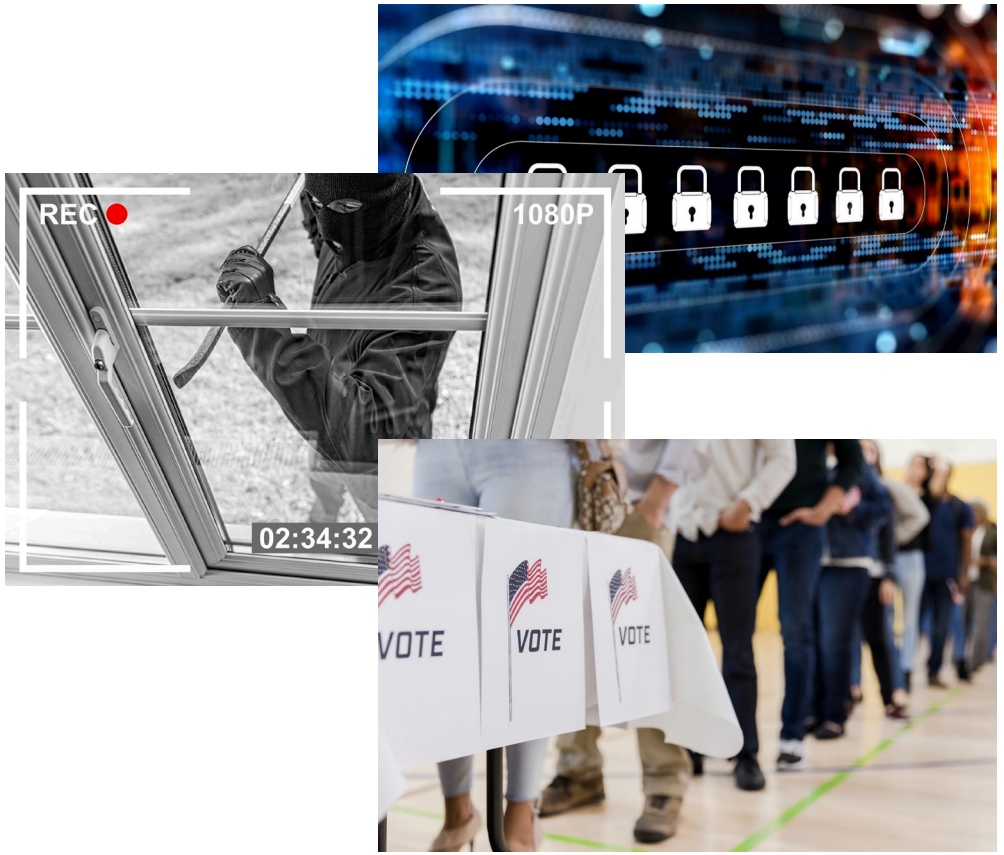
**ELECTION SECURITY INITIATIVE**
**NOAH PRAETZ, ELECTION SECURITY EXPERT**
**CISA**

# 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.

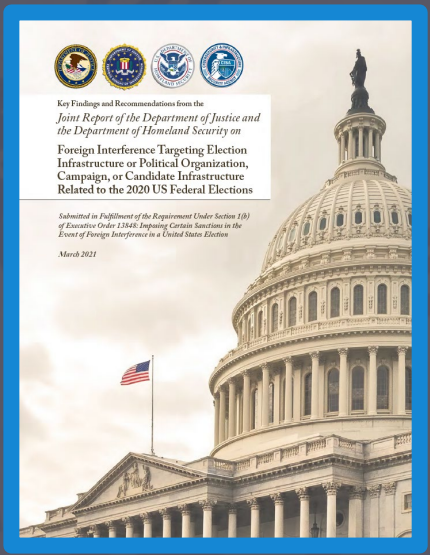
**Major Risks Facing Election Officials**

- Cyber
- Physical
- Mis & Disinformation
- Operational



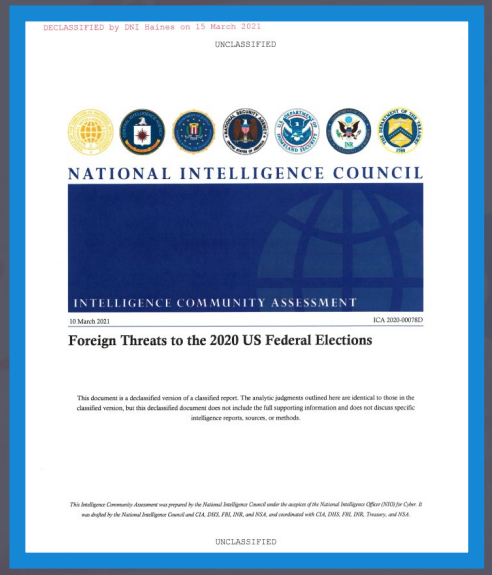
# 2020 Takeaways: The Good

- **Election officials conducted a successful and secure election under unprecedented circumstances**
- **State and local election officials remained the trusted source of information for many. #TrustedInfo2020**




## DHS-CISA-DOJ-FBI Joint Report on 2020:

"We […] have **no evidence** that any foreign government-affiliated actor prevented voting, changed votes, or disrupted the ability to tally votes or to transmit election results in a timely manner; altered any technical aspect of the voting process; or otherwise compromised the integrity of voter registration information of any ballots cast during 2020 federal elections."




## US Intelligence Assessment of Foreign Threats to the 2020 US Federal Election:

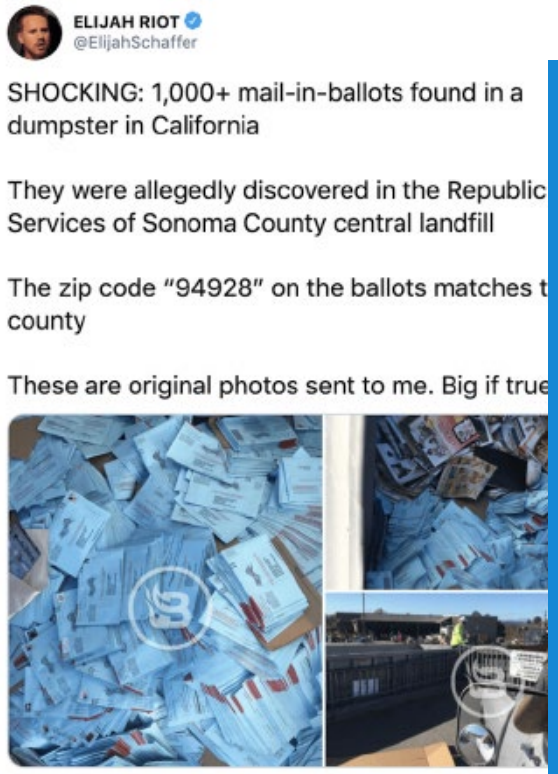
"We have **no evidence** [...] that a **foreign government or other actors** compromised election infrastructure to manipulate election results.

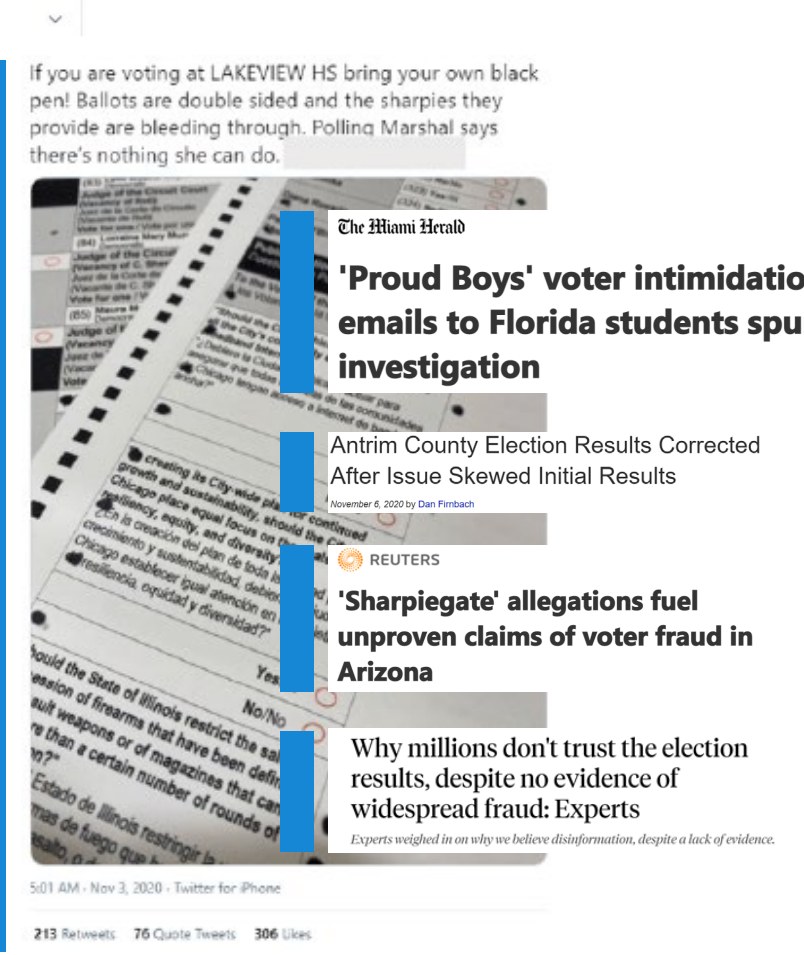
# 2020 Takeaways: The Bad

## Unprecedented levels of MDM:

- Some MDM created or amplified by foreign threat actors
- Russia and Iran engaged in influence operations aimed, in part, at undermining confidence in U.S. elections
- Isolated errors and poorly understood processes fed some MDM narratives

## Decreasing trust in elections among some populations.



# 2020 Takeaways: The Bad

## Heightened threat from Domestic Violent Extremists:

- DVEs "will almost certainly spur some DVEs to try to engage in violence this year," including violence targeting government facilitates and personnel
- DVEs are motivated in part by "newer sociopolitical developments, such as **narratives of fraud in the recent general election**, the emboldening impact of the violent breach of the U.S. Capitol, conditions related to the COVID-19 pandemic, and conspiracy theories promoting violence"

## Election officials facing threats of violence:

- Including via Iranian influence activity

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

**(U) Domestic Violent Extremism Poses Heightened Threat in 2021**

01 March 2021

**Public Service Announcement**

FBI & CISA

**December 23, 2020**

Alert Number
**A-012345-BC**

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field-offices

**Iranian Cyber Actors Responsible for Website Threatening US Election Officials**

The FBI and CISA possess highly credible information indicating Iranian cyber actors almost certainly were responsible for the creation of a website called "Enemies of the People," which contained death threats aimed at US election officials in mid-December 2020.

The FBI has identified multiple domains, to include the main site, "enemiesofthepeople.org," that contained personal information and photographs for a number of US officials and individuals from private sector entities involved with the 2020 election. The FBI has confirmed the main site is currently inactive.

# The Challenge Ahead: Trust

## What is MDM?

- **Misinformation:** information that is false but not created with the purpose of causing harm
- **Disinformation:** information that is false and created to harm on a person, social group, organization, or country
- **Malinformation**: information based on reality used to create harm on a person, social group, organization, or country

**Rampant MDM undermines confidence and trust in:**

- Election technology
- Election officials, workers, facilities
- Election processes

**Public misunderstanding of processes allows for MDM to grow and thrive**

**Isolated errors & confusion can be used to feed destructive narratives**

# The Challenge Ahead: Trust

## You can't stop MDM, but you can mitigate its impact by telling your story:

- Transparently and proactively communicating election processes to build trust in advance of expected MDM
- Know when to engage MDM
- When refuting MDM, be careful not to promote the source of MDM

## Enhance election security practices to:

- Protect programs, systems, and personnel from bad actors
- Decrease likelihood of operational mistakes
- Build evidence that elections are trustworthy

# How Can CISA Help?

## CISA provides training, resources and tools to harden security postures and mitigate potential issues:

### Physical Security

- Protective Security Advisors (PSA) provide facility walkthroughs and recommendations

### Cyber Security

- Cybersecurity Advisor (CSA) visit to discuss protection of networks and systems access control as a defense of networks and devices
- Provide assessment on systems to identify vulnerabilities
- Incident Response Planning Support

### MDM

- Information on how misinformation, disinformation, and malinformation can spread and what signs to watch for
- Collection point for US Intel Community about information spreading online – potential reconnaissance

## Risks:

- ☑ Cyber
- ☑ Physical
- ☑ MDM

# How Can Election Officials Help? The Three T's

## Tracking

Create documentation to detail how things should be done and how they are being done

## Testing

Verify and audit the work of staff and functioning of election equipment and software

## Telling (Your Story)

- Convince your voters they should trust elections by getting ahead of likely stories, by pre-bunking false narratives before they catch hold, and quickly rebutting them if they do catch.
- 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.

# Scenario: A Challenging Election

| Weeks Out | Scenario Detail | Risks | Mitigations |
|---|---|---|---|
| -16 | Video of an election facility with apparent security weaknesses and claims that equipment stolen. | | |
| -12 | Phishing exploit alert. | | |
| -6 | New vulnerability in website software. | | |
| -3 | “New” videos of same facility surface. | | |

## Risks:

- ☑ Cyber
- ☑ Physical
- ☑ MDM

# Scenario: A Challenging Election

| Weeks Out | Sceanrio Detail | Risks | Mitigations |
|---|---|---|---|
| -3 | Legal Group sends letters demanding an accounting of applications. | | |
| 0 | Results show fewer ballots cast than expected. | | |
| 1 | Ballot counting facility under microscope. | | |
| 2 | Protests at central count facility and online threats against leadership. | | |

## Risks:

- ☑ Cyber
- ☑ Physical
- ☑ MDM

# 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;
- Provides evidence that demonstrates election security, accuracy, and integrity has been maintained.

# Tracking: Standard Operating Procedures

## Written Standard Operating Procedures (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

## SOPs for each procedure or operation should:

- Provide sequential steps for each process and be extensively detailed
- Include visual depictions along with examples for completing forms
- Include checklists and logs used for verification

# Tracking: Control Forms

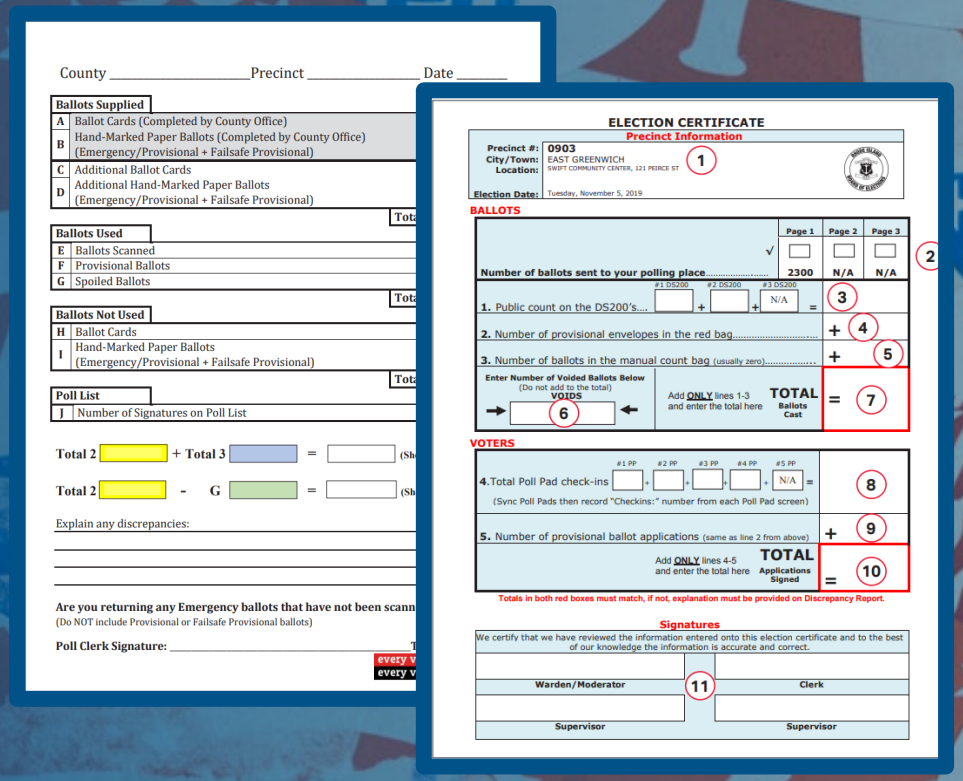
**Control forms capture data with precision at critical points in time and provide evidence for audits or incident analysis**

**Control forms include things like:**

- Chain of custody documentation
- Secure location entry and exit logs
- Ballot duplication logs
- ENR uploads

**Forms not filled out completely or neatly can lead to problems:**

- Ensure good form design
- Use multi-person verification to ensure accuracy and completeness
- Pre-fill as much information as possible or use automation software



# Tracking: Assets

**Movements of assets, people, materials, and data should be tracked to manage access controls risks.**

**Automating the tracking process can make it easier to capture what is happening and when.**

**What aren't you currently tracking that you can/should?**

**For Example:**

- Election equipment (voting equipment, mail ballot sorters, signature verification, asset management, etc.) as it moves from resting storage state to testing, to production, to post-election testing, and back to storage
- Mail ballots being moved from receipt to verification to opening to scanning, to auditing, and to permanent storage

# Managing Risk: Test

**Robust testing and auditing of 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
- Ensuring that election workers are operating in the secure manner proscribed in your standard operating procedures (SOPs)

# Testing: Election Audits

## Post-Election Tabulation Audits

- A post-election tabulation audit is the act of reviewing a sample of voted ballots against the results produced by the voting system to ensure accuracy.
- A risk-limiting audit (RLA) is a type of post-election tabulation audit that examines a random sample from all voted ballots to provide a statistical level of confidence that the outcome of the election is correct.

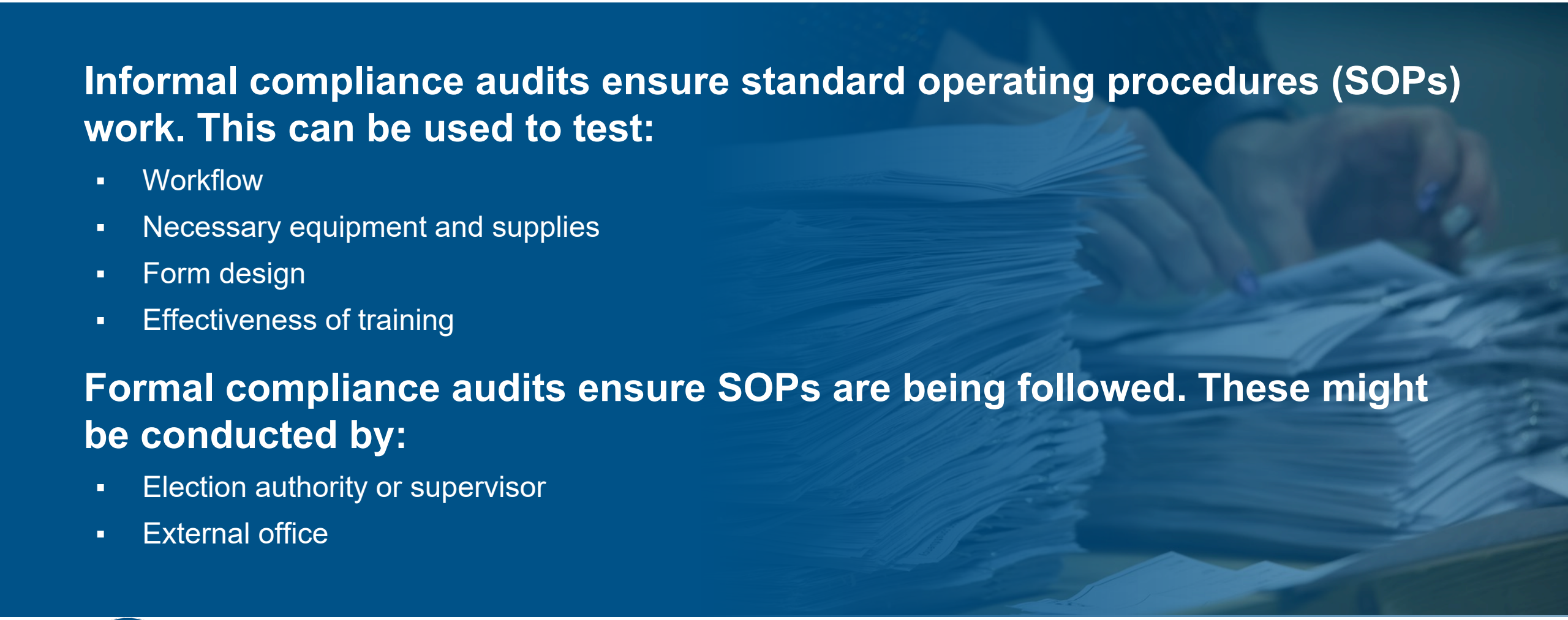
## Any audit, not just tabulation audits, should provide election officials with a way to:

- Detect voting system errors; human error, misconfiguration or manipulation
- Provide accountability to voters
- Deter fraudulent activity
- Assure ballots issued, counted, and reported accurately
- Provide feedback for process improvement

## Systems you should audit include:

- Voting Systems
- Voter Registration Systems
- Signature Verification Systems (ASR & manual)
- Mail Ballot Sorters (including ASR/ASV function)
- ePollbooks
- Website tools (voter lookup, polling location finders, ENR page)

# Testing: Compliance Audits



**Informal compliance audits ensure standard operating procedures (SOPs) work. This can be used to test:**

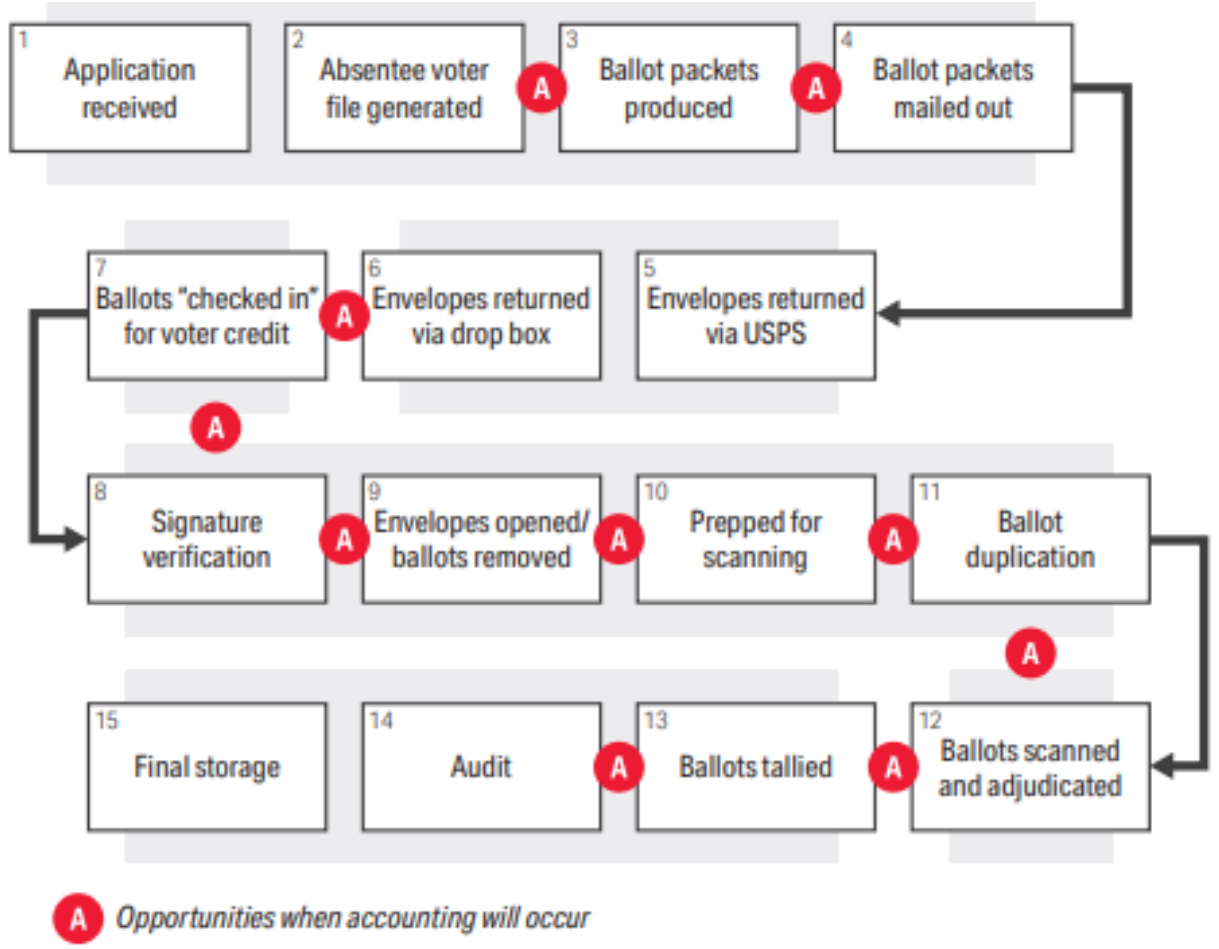
- Workflow
- Necessary equipment and supplies
- Form design
- Effectiveness of training

**Formal compliance audits ensure SOPs are being followed. These might be conducted by:**

- Election authority or supervisor
- External office

# Testing: Other Audits

- Systematic audits of the voter registration database
- GIS audits for correct voter and district assignments
- Security audits
- Ballot reconciliation/chain of custody audits
- Ballot layout and design audits
- Resource allocation audits to ensuring enough equipment, supplies, and people have been allocated to meet demand



# 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 on election administration - They are the **trusted source**
- Local election officials are closest to the voter and most likely to have effective subject matter authority that can be used to retain trust in elections
- Election officials can bring in external validators from the community to add their credibility; political party leadership, local elected officials and community leaders can spread the good word

## Why should election officials focus on telling their story?

- Clear communications around election administration can help manage the significant and persistent risks of MDM

# Telling: What You Can Tell Your Voters

## Processes and Procedures (Track)

- Clear communications around election administration can help manage significant and persistent risks of MDM
- What process and procedure documents are worth sharing?
- Consider augmenting communication around processes that voters may have diminished trust in

## Examples of processes to track

- Secure mail ballot processing procedures
- Rigorous voter verification and signature verification procedures
- Voter registration list maintenance procedures
- Voting equipment testing and security procedures

## Test & Audit Results (Test)

- Providing information that your best practices are followed can minimize the risks of MDM catching hold
- Being transparent by involving the public allows them to verify the testing and results on their own

## Examples of results to provide

- Compliance audits (SOPs, security, chain of custody)
- L&A test results (Pre- & Post-election L&A)
- Ballot reconciliation logs and forms
- Ballot manifests
- Post-election tabulation audit results

# Telling: How to Set Public Expectations

## Clear communication around public expectations

- Important dates both pre- and post Election Day
- Historical turnout data for like elections
- Voter registration trends since last like election
- Schedule of when results will be released (stress that counting is never completed on Election Day)
  - Stay on schedule, do not post updated results off-schedule
  - Depending on frequency, you may see large updates (spikes) to results well after closing of polls on election night.
  - Stress that until all ballots are counted, results will change, and outcomes may change until final certification
- Any variation to the above should be communicated broadly and immediately
- Provide as much transparency as possible on voter numbers and update them regularly (e.g., number of registered voters; number of mail-ballots requested, transmitted to voters, returned; number of early in-person voters; etc.)

## Engage the public in the process – encourage public participation

- When feasible, testing and auditing should be open to the public
- Encourage bi-partisan 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

# Telling: Tools for Telling Your Story

- Encourage in-person observation (building team of validators)
- Use election stakeholders to help spread accurate information
- Build civic and government partnerships
- Conduct community town halls (in-person or virtual)
- Strengthen relationships with earned media (local news, radio, newspapers, etc.)
- Post educational videos of your processes
- Perform facility tours to explain election security measures and processes (in-person or virtual)
- Visually present process maps
- Livestream your activities
- Distribute important information via social Media (pay for targeted messaging)

# Telling: When MDM Impacts Your Operation

- Engage trusted voices
- Communicate without amplifying the MDM narrative
- Lead with the truth, not the rumor
- Restate the fact again
- Keep it simple
- Be consistent in your choice of MDM narratives to debunk

# Scenario: A Challenging Election

| Weeks Out | Scenario Detail | Risks | Mitigations |
|---|---|---|---|
| -16 | Video of an election facility with apparent security weaknesses and claims that equipment stolen. | • Physical<br>• MDM<br>• Operational<br>• Cyber | • CISA PSA Visit & Services |
| -12 | Phishing exploit alert. | • Cyber<br>• Operational | • CISA Phishing Assessment<br>• ISAC<br>• CISA RPT<br>• Tracking - SOPs |
| -6 | New vulnerability in website software. | • Cyber<br>• Operational | • ISAC<br>• CISA RPT<br>• CISA Vuln Scanning<br>• Local Relationships |
| -3 | "New" videos of same facility surface. | • Physical<br>• Operational<br>• MDM | • Tracking<br>• Testing<br>• Telling |

## Risks:

- ☑ Cyber
- ☑ Physical
- ☑ MDM

# Scenario: A Challenging Election

| Weeks Out | Scenario Detail | Risks | Mitigations |
|---|---|---|---|
| -3 | Legal Group sends letters demanding an accounting of applications. | • Operational<br>• Cyber<br>• MDM | • Tracking<br>• Testing<br>• Telling |
| 0 | Results show fewer ballots cast than expected. | • cyber<br>• Operational<br>• MDM | • Tracking<br>• Testing<br>• Telling |
| 1 | Ballot counting facility under microscope. | • Physical<br>• Operational<br>• MDM | • Tracking<br>• Testing<br>• Telling |
| 2 | Protests at central count facility and online threats against leadership. | * Physical<br>• Cyber<br>• Operational<br>• MDM | • Local Law Enforcement Coordination<br>• PSA Visit & Services |

## Risks:

- ☑ Cyber
- ☑ Physical
- ☑ MDM


CISA
CYBER+INFRASTRUCTURE

**Noah Praetz**
CISA Election Security Expert
Consultant
noah@electionsgroup.com

Eric Puype, CPP, PCI
Protective Security Advisor, Region X
eric.puype@cisa.dhs.gov

**Contact CISA:**
Central@cisa.dhs.gov


# CISA

CYBER+INFRASTRUCTURE