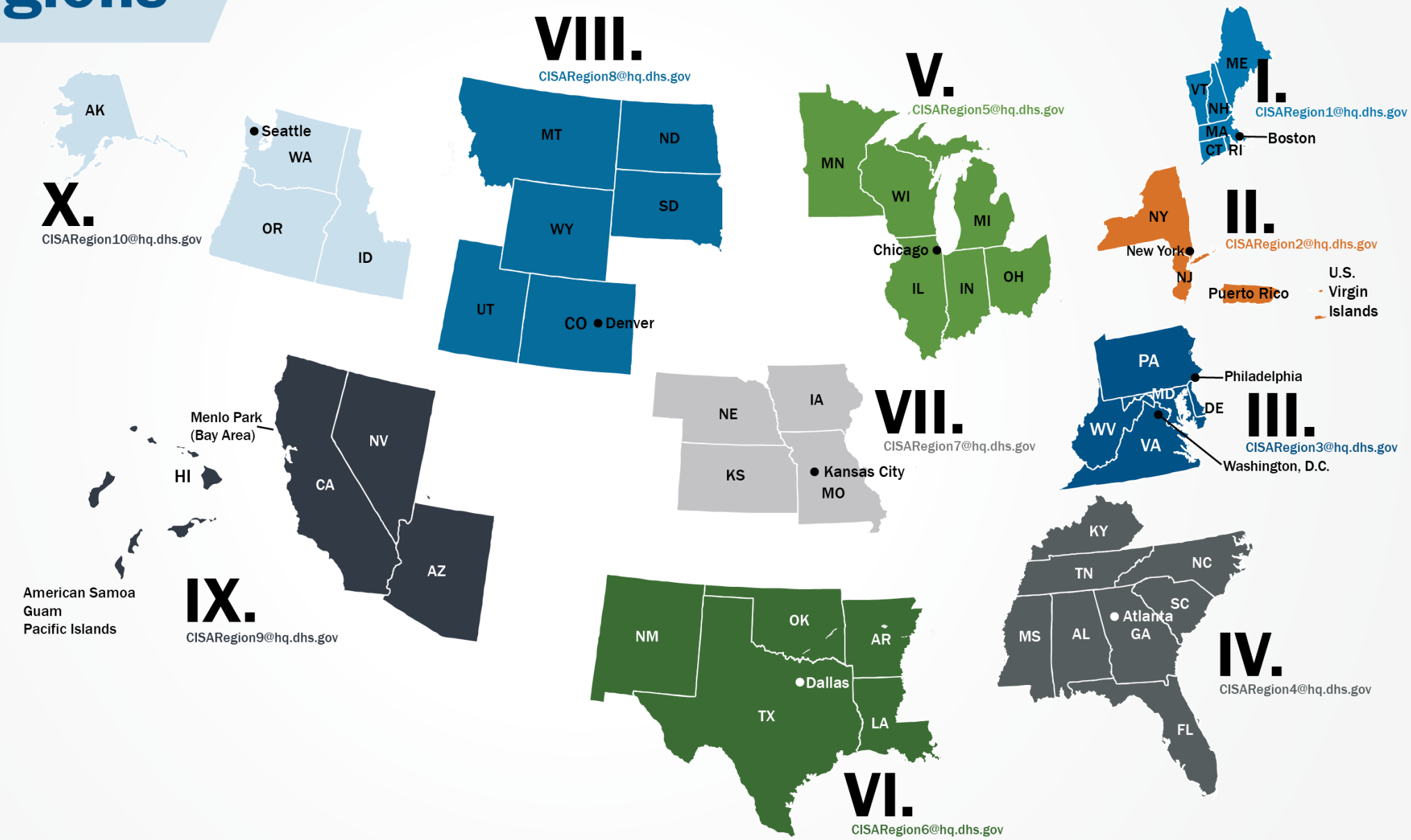
ELECTION SECURITY: BUILDING TRUST THROUGH SECURE PRACTICES

ROB MOONEY, SUPERVISORY PROTECTIVE SECURITY ADVISOR

NOAH PRAETZ, ELECTION SECURITY SUBJECT MATTER EXPERT

CISA Regions



I	Boston, MA
II	New York, NY
III	Philadelphia, PA
IV	Atlanta, GA
V	Chicago, IL
VI	Irving, TX
VII	Kansas City, MO
VIII	Lakewood, CO
IX	Oakland, CA
X	Seattle, WA
CS	Pensacola, FL

CISA Offers No-Cost Cybersecurity Services

- **Preparedness Activities**
  - Cybersecurity Assessments
  - Cybersecurity Training and Awareness
  - Cyber Exercises and “Playbooks”
  - Information / Threat Indicator Sharing
  - National Cyber Awareness System
  - Vulnerability Notes Database
  - Information Products and Recommended Practices

- **24/7 Response Assistance**
  - Incident Coordination and Response assistance
  - Threat intelligence and information sharing
  - Malware Analysis

- **Cybersecurity Advisors**
  - Incident response coordination
  - Cybersecurity assessments
  - Cybersecurity Workshops
  - Working group collaboration
  - Advisory assistance
  - Public Private Partnership Development

Contact CISA to report a cyber incident

Call 1-888-282-0870 | email CISAservicedesk@cisa.dhs.gov | visit https://www.cisa.gov

Range of Cybersecurity Assessments

- Cyber Resilience Review (Strategic)
- External Dependencies Management (Strategic)
- Cyber Infrastructure Survey (Strategic)
- Cyber Security Evaluations Tool (standards based)
- Phishing Campaign Assessment (EVERYONE)
- Validated Architecture Design Review (Tactical)
- Cyber Hygiene (Technical)
  - Vulnerability Scanning
  - Web Application Scanning
  - Remote Penetration Test
- Risk and Vulnerability Assessment (Technical)

Protective Security Advisors

- Protective Security Advisors (PSA) are field-deployed personnel who serve as critical infrastructure security specialists
- Protective Security Advisors (PSA) have five mission areas that directly support the protection of critical infrastructure:
  - Plan, coordinate, and conduct security surveys and assessments
  - Plan and conduct outreach activities
  - Coordinate and support improvised explosive device awareness and risk mitigation training

Available Tools and Resources

- Infrastructure Survey Tool (IST)
- Site Assessment at First Entry (SAFE)
- Infrastructure Visualization Platform (IVP)
- Homeland Security Information Network (HSIN)
- OBP Counter-IED Training
- Active Shooter Preparedness Briefings
- Exercise Coordination and TTX in a Box

Risks to Election Infrastructure

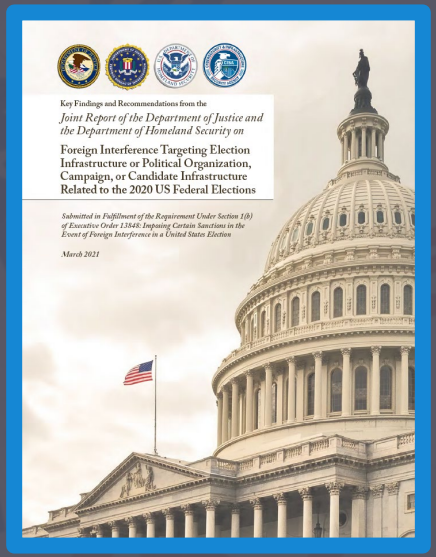
As the nation's **risk advisor**, the Cybersecurity and Infrastructure Security Agency's (CISA) mission is to ensure the security and resiliency of our critical infrastructure.

Major Risks Facing Election Officials

- Cyber
- Physical
- Mis & Disinformation
- Operational

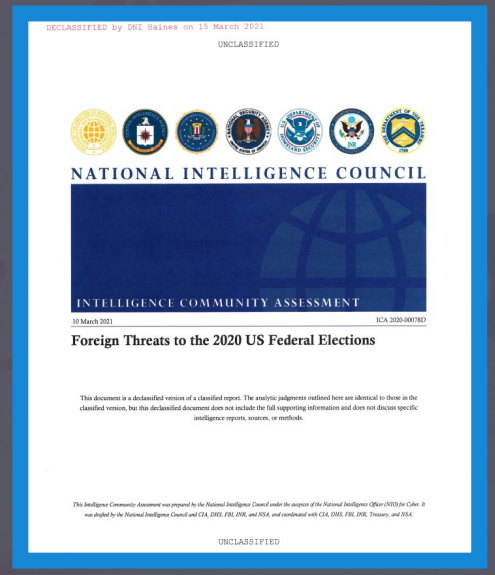
2020 Takeaways: The Good

- **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."

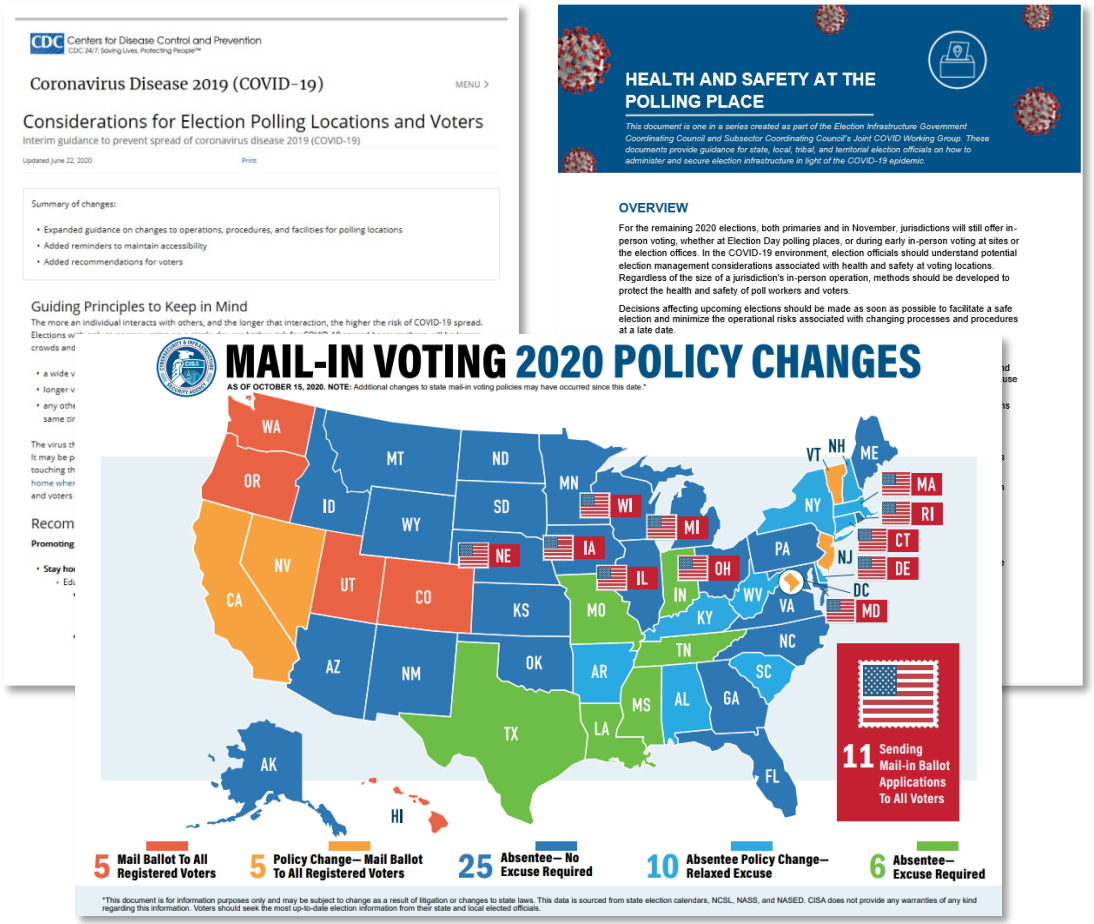


US Intelligence Assessment of Foreign Threats to the 2020 US Federal Election:

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

2020: Impact of COVID-19 Pandemic

- The pandemic shifted the risk landscape & informed updated CISA risk assessment
- Increased private sector outreach w/ greater emphasis on mail-in voting support vendors
- Briefings from USPS, CDC, FVAP, and EAC
- Showed value of the GCC & SCC structure
  - Worked with EAC on joint GCC-SCC Working Group on COVID-19 produced 15 guidance documents
  - SCC deepened engagement w/ mail vendors
  - Platform for coord. w/ CDC & other fed agencies
- The scale & speed of changes created ripe environment for mis/disinformation

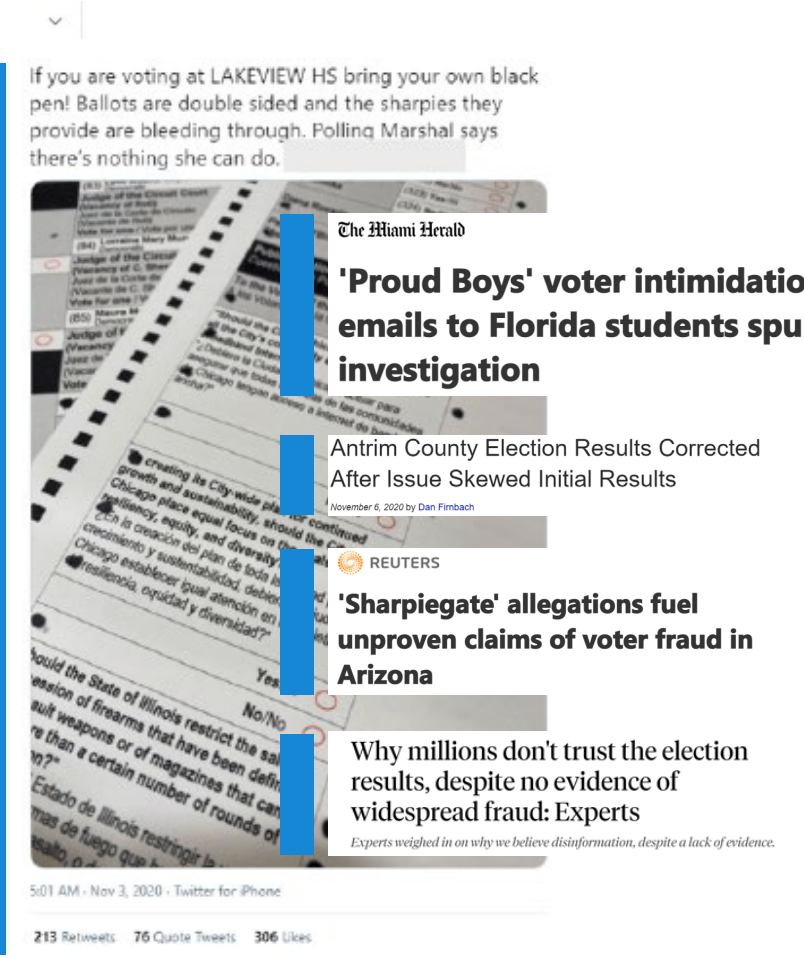


2020 Takeaways: The Bad

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.

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

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.

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:

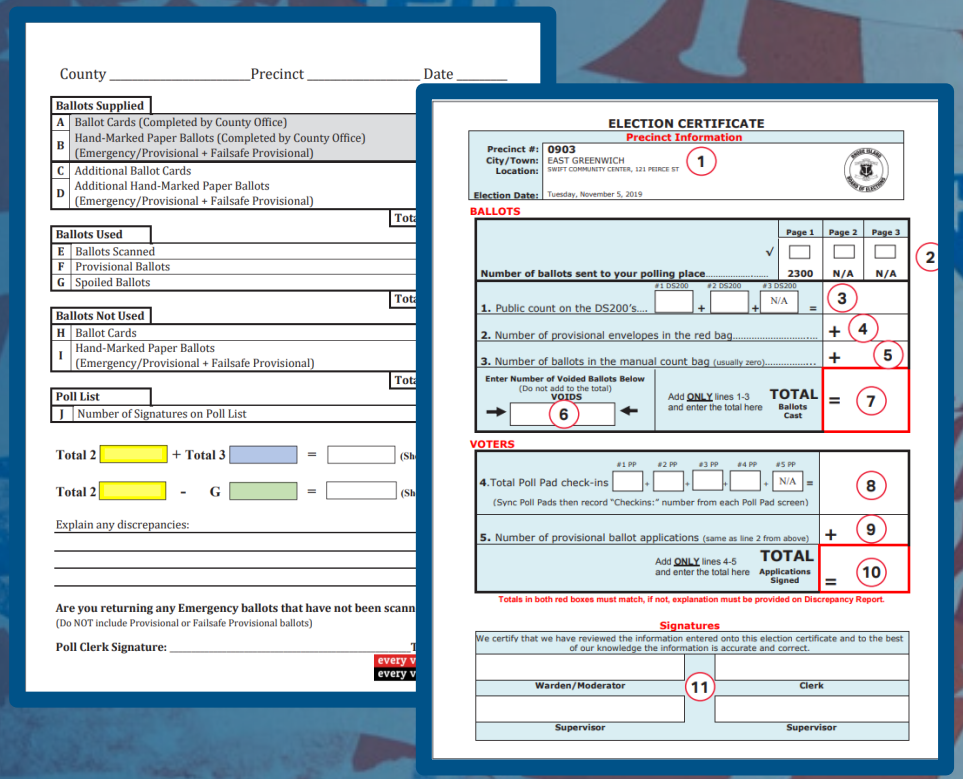
- Limit risks to the operation of election infrastructure
- Limit ad hoc decision making
- Increase quality and consistency of work across staff
- Increase productivity, efficiency and measurement opportunities
- Speed remediation time when following incident response plans

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 at critical points in time to help manage workflow and can provide evidence for audits or incident analysis


County _____ Precinct _____ Date _____

Ballots Supplied
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)

Ballots Used
E Ballots Scanned
F Provisional Ballots
G Spoiled Ballots

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

Poll List
J Number of Signatures on Poll List

Total 2 + Total 3 =

Total 2 - G =

Explain any discrepancies:

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

Poll Clerk Signature:

ELECTION CERTIFICATE
Precinct Information
Precinct #: 0903
City/Town: EAST GREENWICH
Location: SWIFT COMMUNITY CENTER, 121 PEIRCE ST
Election Date: Tuesday, November 5, 2019

BALLOTS
Number of ballots sent to your polling place — Page 1: 2300; Page 2: N/A; Page 3: N/A
1. Public count on the DS200's — #1 DS200 + #2 DS200 + #3 DS200 (N/A) =
2. Number of provisional envelopes in the red bag +
3. Number of ballots in the manual count bag (usually zero) +
Enter Number of Voided Ballots Below (Do not add to the total) VOIDS
Add ONLY lines 1-3 and enter the total here TOTAL Ballots Cast =

VOTERS
4. Total Poll Pad check-ins — #1 PP + #2 PP + #3 PP + #4 PP + #5 PP (N/A) =
(Sync Poll Pads then record "Checkins:" number from each Poll Pad screen)
5. Number of provisional ballot applications (same as line 2 from above) +
Add ONLY lines 4-5 and enter the total here TOTAL Applications Signed =
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 | Clerk
Supervisor | Supervisor

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

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
- 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.

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

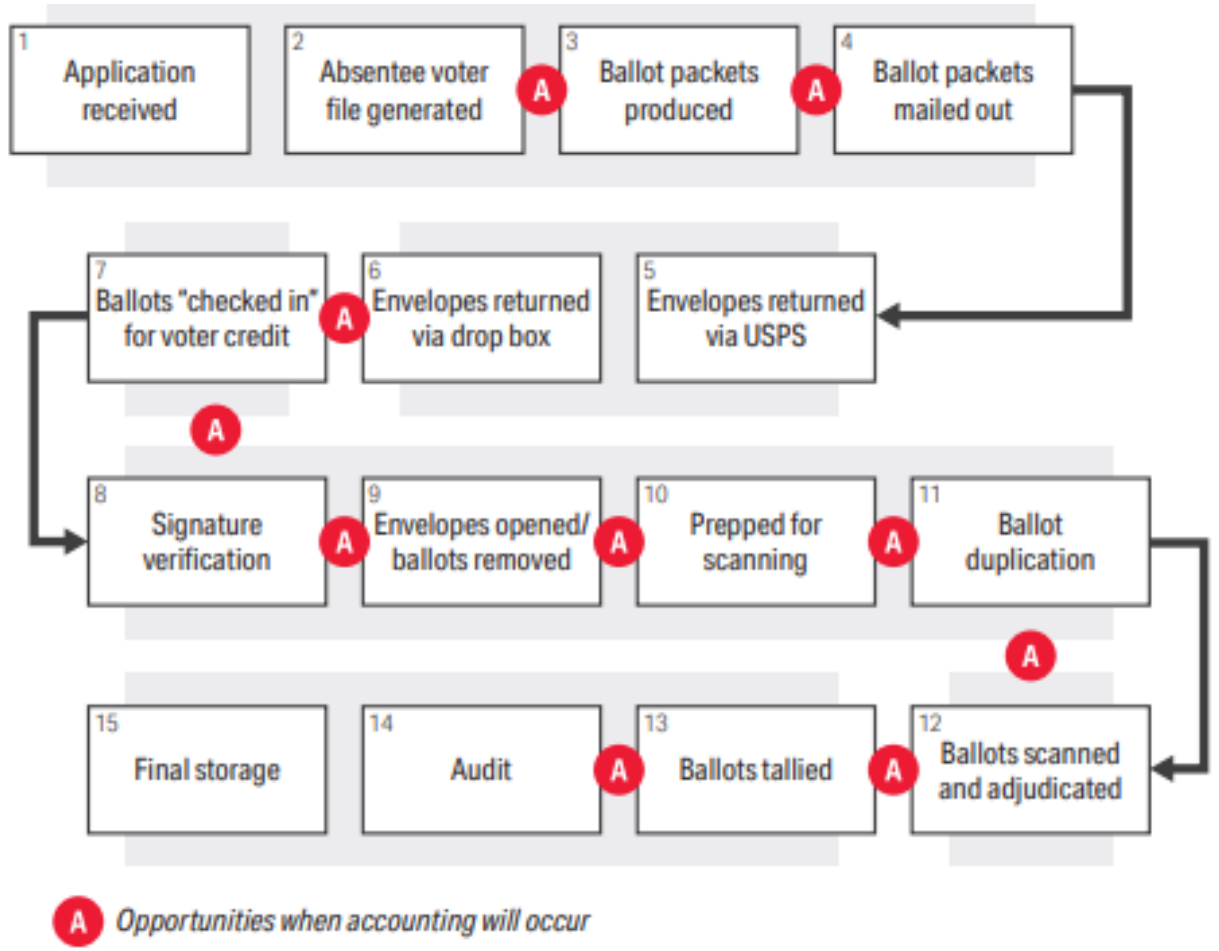
Formal compliance audits ensure SOPs are being followed. These might be conducted by:

- Election authority or supervisor
- External office

Testing: Other Audits

Processes to audit include:

- 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

Why should election officials focus on telling their story?

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

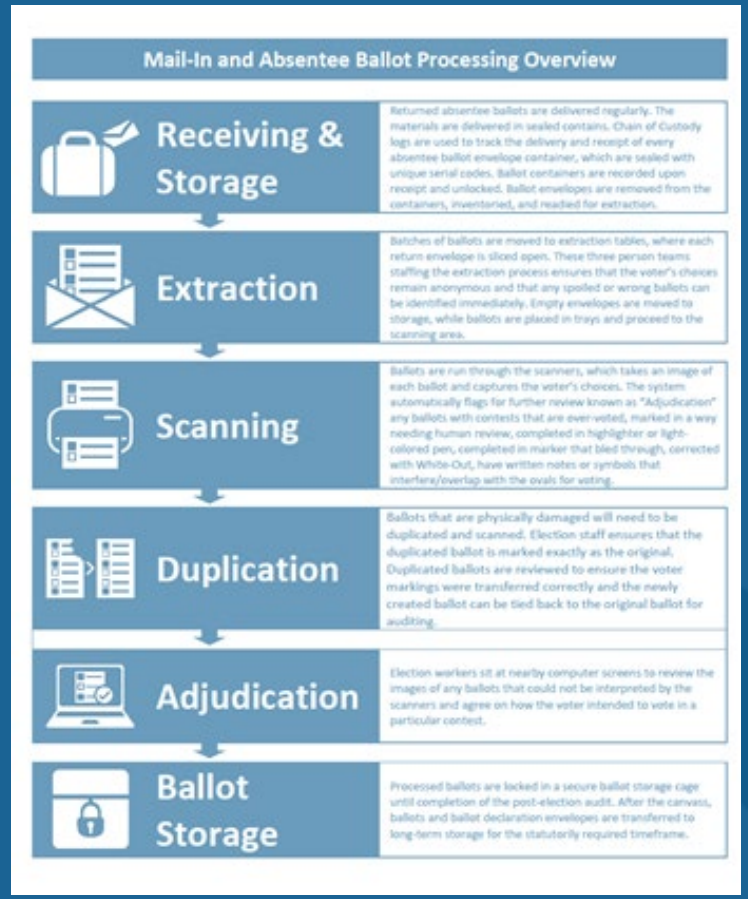
Telling: What You Can Tell Your Voters

Processes and Procedures

- The how and why of election administration
- Highlight processes that voters may have diminished trust in

Examples of processes to track

- Mail ballot processing procedures
- Voter verification and signature verification procedures
- Voter registration list maintenance procedures
- Voting equipment testing and security procedures



Telling: Tools for Telling Your Story

Tactics to support your communications efforts

- In-person observation (building team of validators)
- Stakeholders help spread accurate information
- Civic and government partnerships
- Community town halls
- Earned media (local news, radio, newspapers, etc.)
- Videos of your processes
- Facility tours to explain election security
- Process graphics and maps
- Livestream activities
- 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

Operational Security Postcard

Secure Practices

Enhance election security practices to decrease the likelihood of operational mistakes, build trust through secure practices, and protect systems, data, and personnel.

Building Trust Through Secure Practices

- **Isolated errors and confusion** can feed destructive narratives.
- **Public misunderstanding of processes** allows MDM to grow and thrive.
- **MDM undermines confidence and trust** in elections.
- You can't stop MDM, but you can mitigate its impact by **sharing relevant facts**.

What Can Election Officials Do?

- **Track**:
  Document your cybersecurity, physical security, and operational security processes and procedures to ensure that safeguards are enacted and implemented.
- **Test:**
  Verify and audit your processes and procedures, the work of your staff, and the functioning of election infrastructure.
- **Tell:**
  Provide fact-based 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.

What is MDM?

- **Misinformation** is false, but not created or shared with the intention of causing harm.
- **Disinformation** is deliberately created to mislead, harm, or manipulate a person, social group, organization, or country.
- **Malinformation** is based on fact, but used out of context to mislead, harm, or manipulate.

Three T's: Track, Test, Tell

visor,

Agency's
sure the
of our

, and tools
nitigate

with:

rovide facility

ct site visits to
systems access
d devices

dentify

support

re-related
malinformation
for.

Visit **cisa.gov/election-security** to learn about CISA's role in election security.

Track

Create documentation to detail both how security practices should be conducted and how they are being conducted through robust chain-of-custody and physical security procedures.

- Written Standard Operating Procedures (SOPs) should be extensively detailed. Provide sequential steps and include visual depictions, examples, checklists, and forms for verification.
- Asset tracking and access control for systems, people, documents, and data transactions should be implemented and logged. Automating the process can make it easier to capture what is happening and when.
- Control forms— including chain-of-custody documentation, ballot duplication logs, and election night reporting uploads— capture data with precision at critical points to provide evidence for audits or incident analysis.

Test

Verify the work of staff and the functioning of election assets and processes with robust testing and auditing.

- Conduct post-election tabulation audits by reviewing a sample of voted ballots against the voting machine records to ensure accuracy.
- Informal compliance audits ensure SOPs work. Formal compliance audits ensure SOPs are being followed.
- Test processes to ensure chain of custody on your critical assets is never broken and that you have the evidence to prove it.

Tell

Convince voters to trust elections with proactive and responsive fact-based communication and transparency measures.

- Election officials are the absolute authority on election administration.
- Clear communication around election administration can help manage the significant and persistent risks of MDM.
- Use documentation from your Tracking and Testing practices as communication content to share information.
- Engage the public in the process— encourage public participation.

DotGov Program

Bona fide government services should be easy to identify on the internet. CISA operates the .gov top-level domain (TLD) and makes it available to U.S.-based government organizations, from federal agencies to local municipalities. Using a .gov domain shows you're official.

Benefits:

- **April 27th, 2021 Update:** Easily register and keep a .gov domain at ***no cost*** for qualifying U.S.-based government organizations at https://home.dotgov.gov
- Quickly identify your government organization on the Internet
- Ensure that the name resolves in the global domain name system (DNS)
- Maintain a trusted & secure .gov space (i.e., published policies & security best practices and .gov domain data publicly available)

CISA
CYBER+INFRASTRUCTURE

Noah Praetz
CISA Election Security Expert
Consultant
electionsecurity@hq.dhs.gov

Rob Mooney
Supervisory Protective Security Advisor
robert.mooney@hq.dhs.gov

Contact CISA:

Central@cisa.dhs.gov