ELECTION SECURITY: BUILDING TRUST THROUGH SECURE PRACTICES

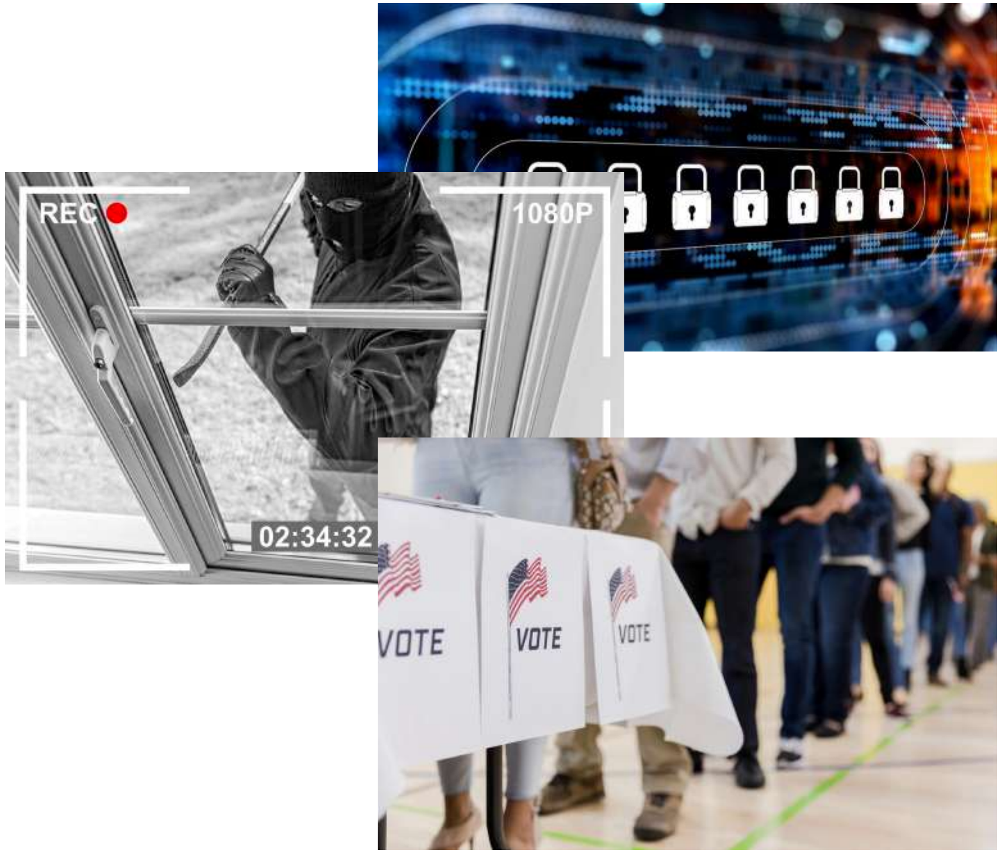
ELECTION SECURITY INITIATIVE
Ryan Macias, SME – Election Security

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.

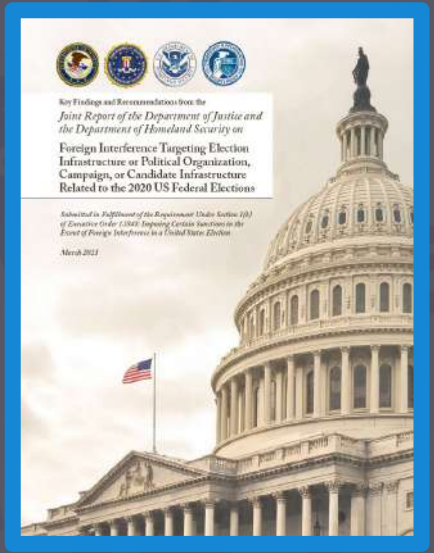
Major Risks Facing Election Officials

- Cyber
- Physical
- Mis-, Dis-, & Malinformation (MDM)
- 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



Key Findings and Recommendations from the

Joint Report of the Department of Justice and the Department of Homeland Security on

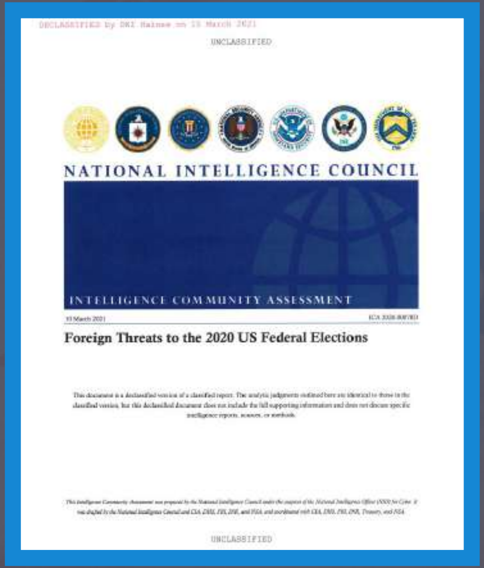
Foreign Interference Targeting Election Infrastructure or Political Organization, Campaign, or Candidate Infrastructure Related to the 2020 US Federal Elections

Submitted in Fulfillment of the Requirement Under Section 1(b) of Executive Order 13848: Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election

March 2021

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."



DECLASSIFIED by DNI Haines on 15 March 2021

UNCLASSIFIED

NATIONAL INTELLIGENCE COUNCIL

INTELLIGENCE COMMUNITY ASSESSMENT

10 March 2021 ICA 2020-00078D

Foreign Threats to the 2020 US Federal Elections

This document is a declassified version of a classified report. The analytic judgments outlined here are identical to those in the classified version, but this declassified document does not include the full supporting information and does not discuss specific intelligence reports, sources, or methods.

This Intelligence Community Assessment was prepared by the National Intelligence Council under the auspices of the National Intelligence Officer (NIO) for Cyber. It was drafted by the National Intelligence Council and CIA, DHS, FBI, INR, and NSA, and coordinated with CIA, DHS, FBI, INR, Treasury, and NSA.

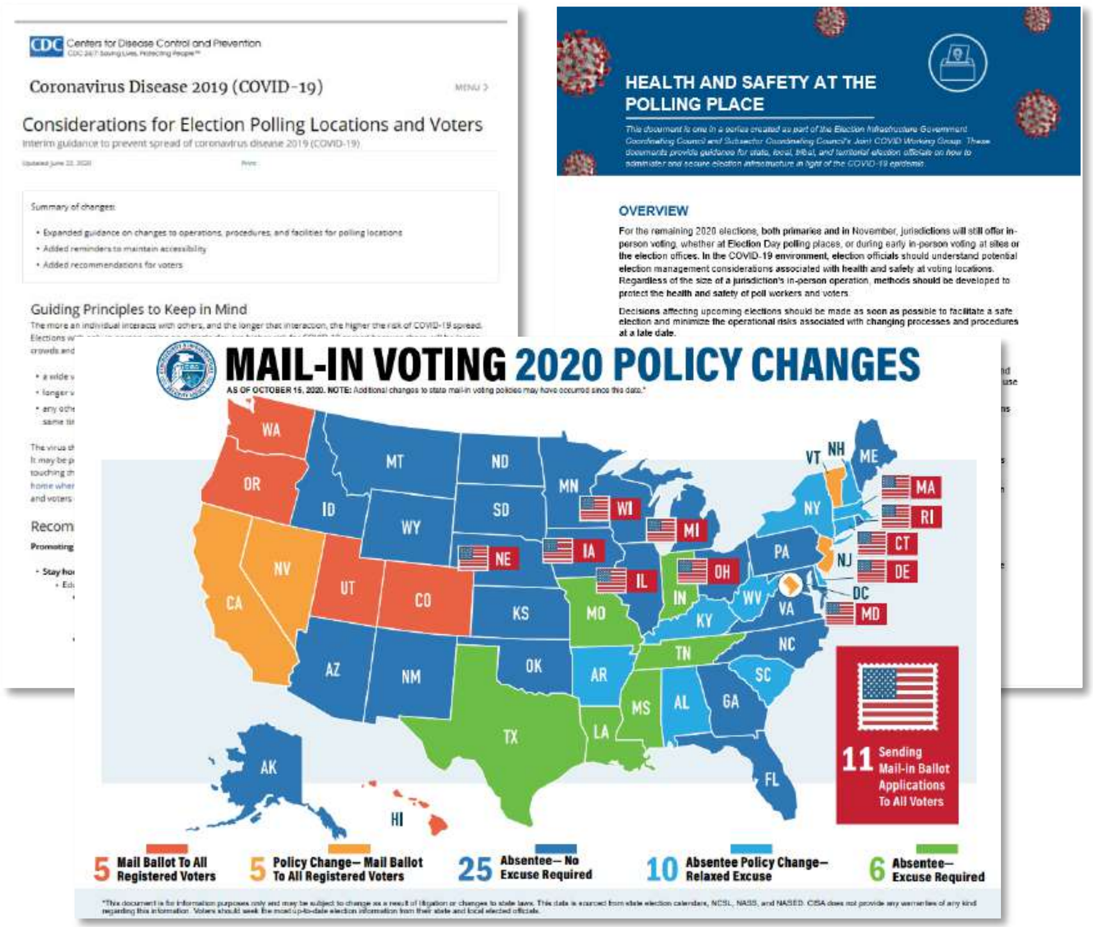
UNCLASSIFIED

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



CDC Centers for Disease Control and Prevention
CDC 24/7 Saving Lives, Protecting People™

Coronavirus Disease 2019 (COVID-19)

Considerations for Election Polling Locations and Voters

Interim guidance to prevent spread of coronavirus disease 2019 (COVID-19)

Updated June 22, 2020

Summary of changes:

- Expanded guidance on changes to operations, procedures, and facilities for polling locations
- Added reminders to maintain accessibility
- Added recommendations for voters

Guiding Principles to Keep in Mind

The more an individual interacts with others, and the longer that interaction, the higher the risk of COVID-19 spread.

HEALTH AND SAFETY AT THE POLLING PLACE

This document is one in a series created as part of the Election Infrastructure Government Coordinating Council and Subsector Coordinating Council's Joint COVID Working Group. These documents provide guidance for state, local, tribal, and territorial election officials on how to administer and secure election infrastructure in light of the COVID-19 epidemic.

OVERVIEW

For the remaining 2020 elections, both primaries and in November, jurisdictions will still offer in-person voting, whether at Election Day polling places, or during early in-person voting at sites or the election offices. In the COVID-19 environment, election officials should understand potential election management considerations associated with health and safety at voting locations. Regardless of the size of a jurisdiction's in-person operation, methods should be developed to protect the health and safety of poll workers and voters.

Decisions affecting upcoming elections should be made as soon as possible to facilitate a safe election and minimize the operational risks associated with changing processes and procedures at a late date.

MAIL-IN VOTING 2020 POLICY CHANGES

AS OF OCTOBER 15, 2020. NOTE: Additional changes to state mail-in voting policies may have occurred since this date.*

11 Sending Mail-in Ballot Applications To All Voters

5 Mail Ballot To All Registered Voters

5 Policy Change— Mail Ballot To All Registered Voters

25 Absentee— No Excuse Required

10 Absentee Policy Change— Relaxed Excuse

6 Absentee— Excuse Required

*This document is for information purposes only and may be subject to change as a result of litigation or changes to state laws. This data is sourced from state election calendars, NCSL, NASS, and NASED. CISA does not provide any warranties of any kind regarding this information. Voters should seek the most up-to-date election information from their state and local elected officials.

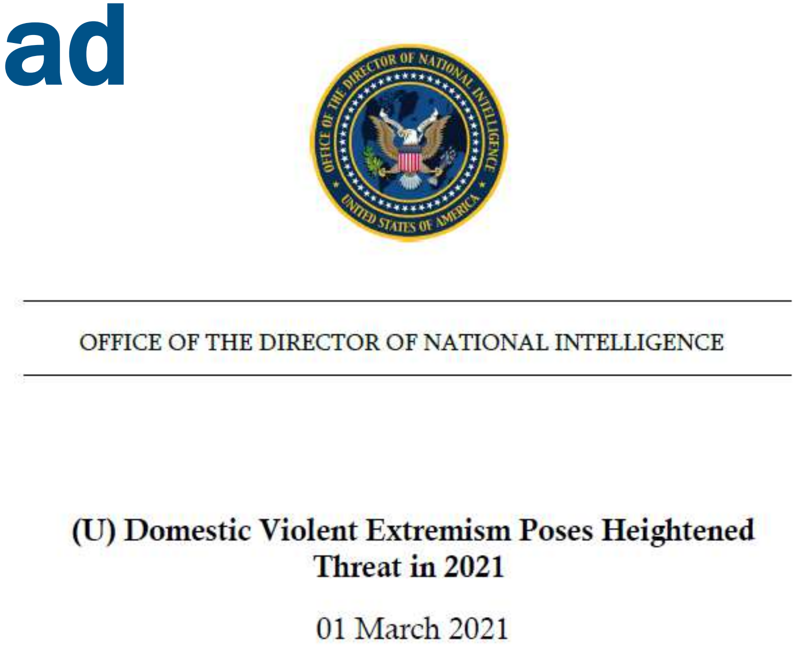
2020 Takeaways: The Bad

Heightened threat from Domestic Violent Extremists:

- Newer sociopolitical developments “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:

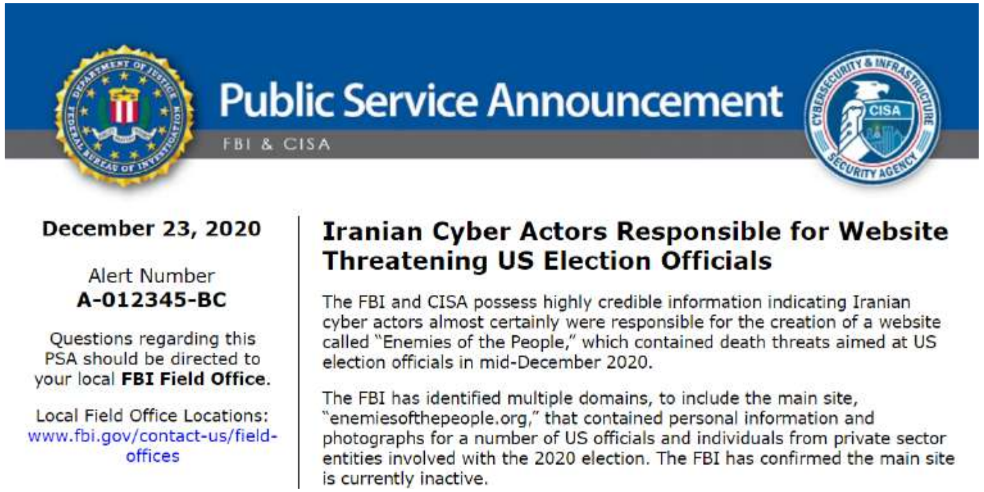
- Including via Iranian influence activity



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.

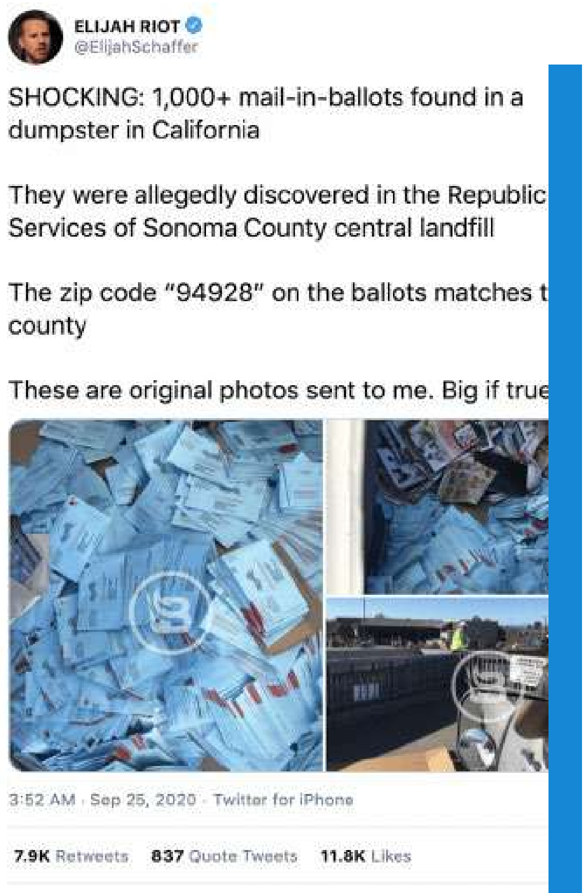
The FBI has identified multiple domains, to include the main site, “enemiesofthepeople.org,” that contained personal information and photographs for a number of US officials and individuals from private sector entities involved with the 2020 election. The FBI has confirmed the main site is currently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

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.



ELIJAH RIOT
@ElijahSchaffer

SHOCKING: 1,000+ mail-in-ballots found in a dumpster in California

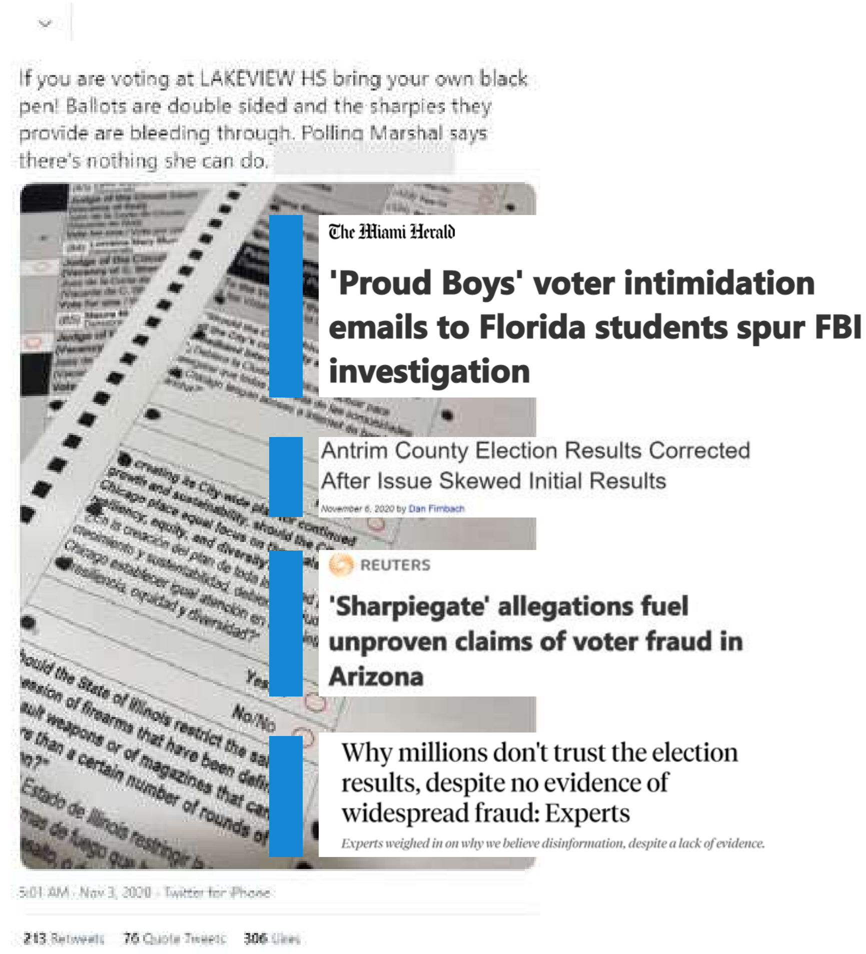
They were allegedly discovered in the Republic Services of Sonoma County central landfill

The zip code "94928" on the ballots matches t county

These are original photos sent to me. Big if true

3:52 AM · Sep 25, 2020 · Twitter for iPhone

7.9K Retweets 837 Quote Tweets 11.8K Likes



If you are voting at LAKEVIEW HS bring your own black pen! Ballots are double sided and the sharpies they provide are bleeding through. Polling Marshal says there's nothing she can do.

The Miami Herald

'Proud Boys' voter intimidation emails to Florida students spur FBI investigation

Antrim County Election Results Corrected After Issue Skewed Initial Results

November 6, 2020 by Dan Fimbach

REUTERS

'Sharpiegate' allegations fuel unproven claims of voter fraud in Arizona

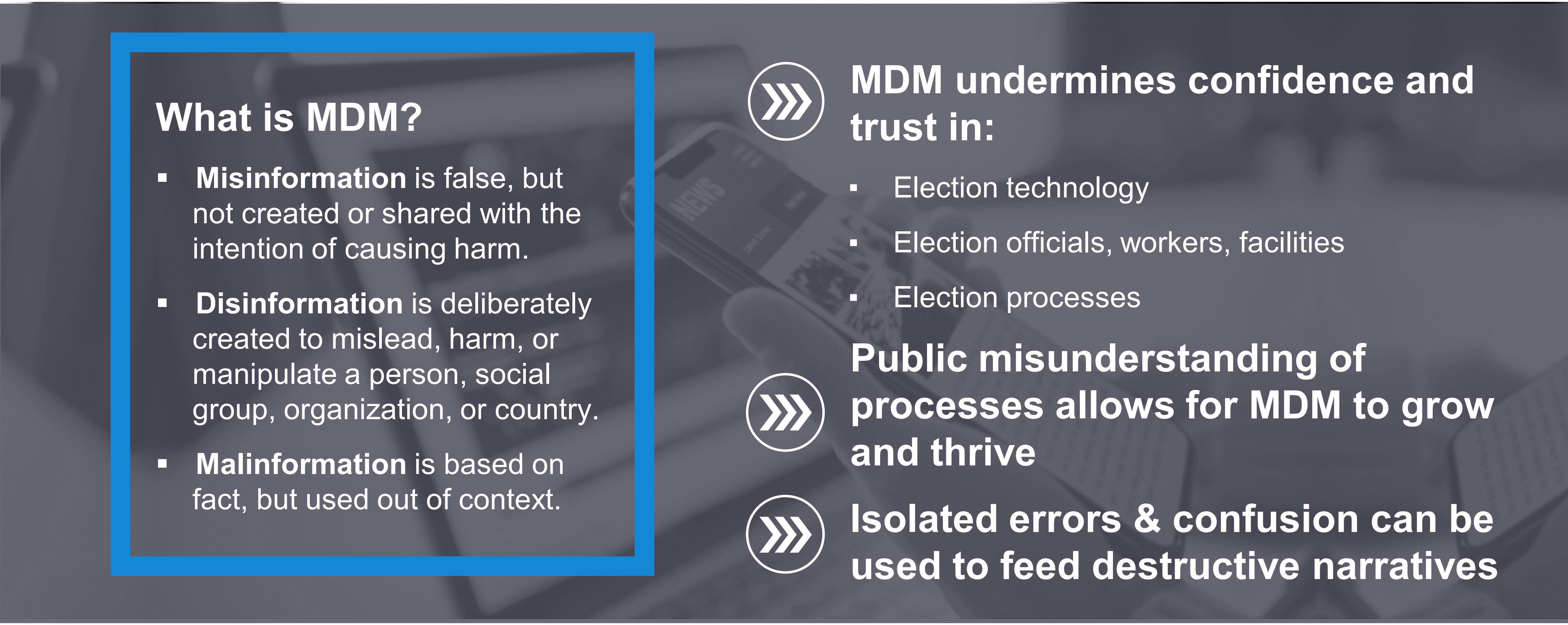
Why millions don't trust the election results, despite no evidence of widespread fraud: Experts

Experts weighed in on why we believe disinformation, despite a lack of evidence.

5:01 AM · Nov 3, 2020 · Twitter for iPhone

213 Retweets 76 Quote Tweets 306 Likes

The Challenge Ahead: Trust



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.

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

Cybersecurity

- Cybersecurity Advisors (CSAs) conduct site visits to discuss protection of networks and systems access control as a defense of networks and devices
- Provide assessment on systems to identify vulnerabilities
- Provide incident response planning support

MDM

- Guidance on how critical infrastructure-related misinformation, disinformation, and malinformation can spread, and what signs to watch for

Risks:

☑ Cyber

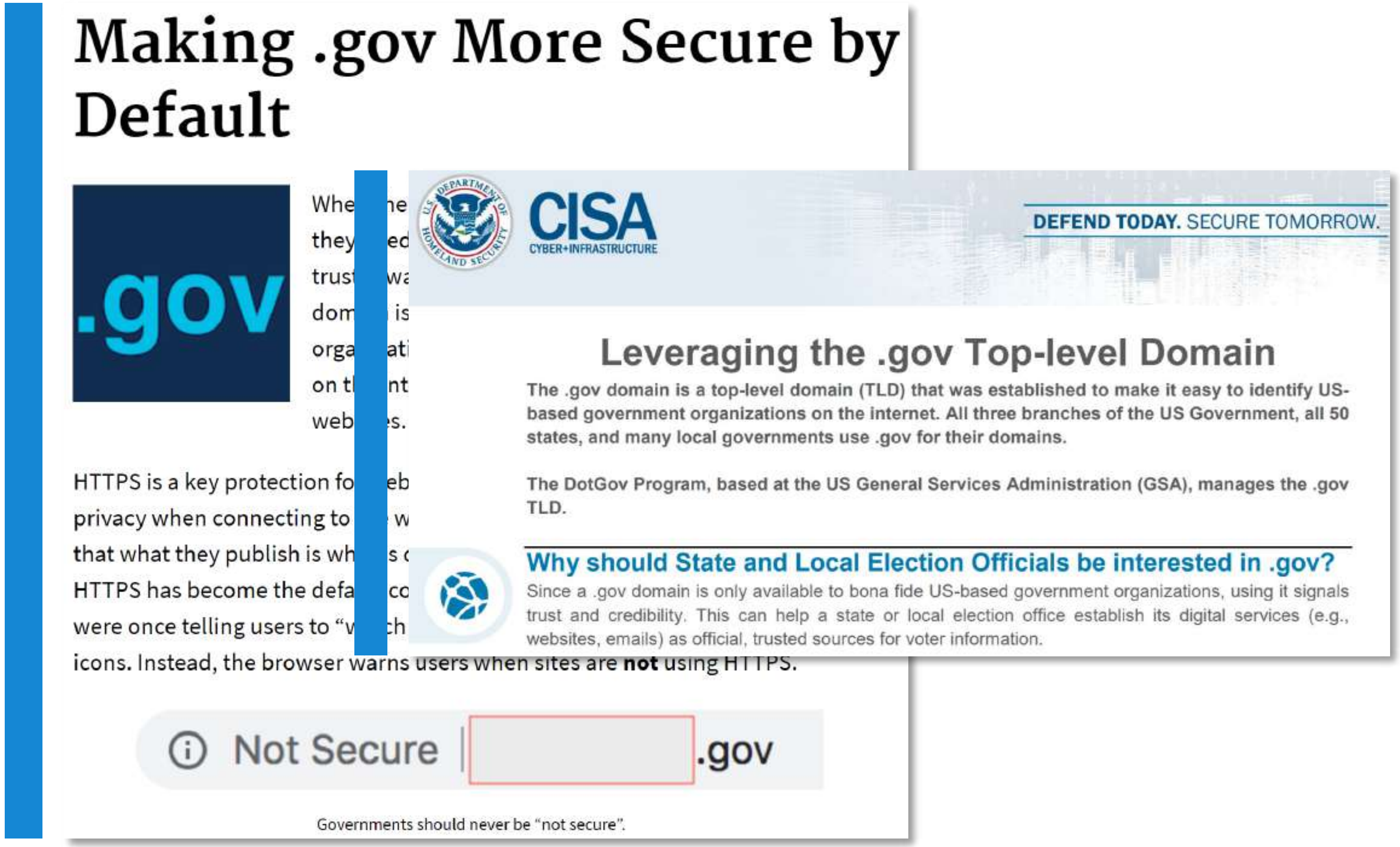
☑ Physical

☑ MDM

.GOV Top-Level Domain

Show you are the trusted source

- Increased use of .gov domains will **improve cybersecurity and trust** in public services across the United States
- **Responsibility** of administering official web domains shifted to CISA from GSA
- Under CISA, .gov domains are available at **no cost** for qualifying organizations



Making .gov More Secure by Default

Whe he
they ed
trust wa
dom is
orga ati
on t nt
web es.

HTTPS is a key protection fo eb
privacy when connecting to w
that what they publish is wh s c
HTTPS has become the defa co
were once telling users to "w ch
icons. Instead, the browser warns users when sites are **not** using HTTPS.

ⓘ Not Secure | .gov

Governments should never be "not secure".

CISA CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

Leveraging the .gov Top-level Domain

The .gov domain is a top-level domain (TLD) that was established to make it easy to identify US-based government organizations on the internet. All three branches of the US Government, all 50 states, and many local governments use .gov for their domains.

The DotGov Program, based at the US General Services Administration (GSA), manages the .gov TLD.

Why should State and Local Election Officials be interested in .gov?

Since a .gov domain is only available to bona fide US-based government organizations, using it signals trust and credibility. This can help a state or local election office establish its digital services (e.g., websites, emails) as official, trusted sources for voter information.

How Can Election Officials Help? The Three T’s

Track

Document your cybersecurity, physical security, and operational security processes and procedures to ensure that safeguards are enacted and implemented.

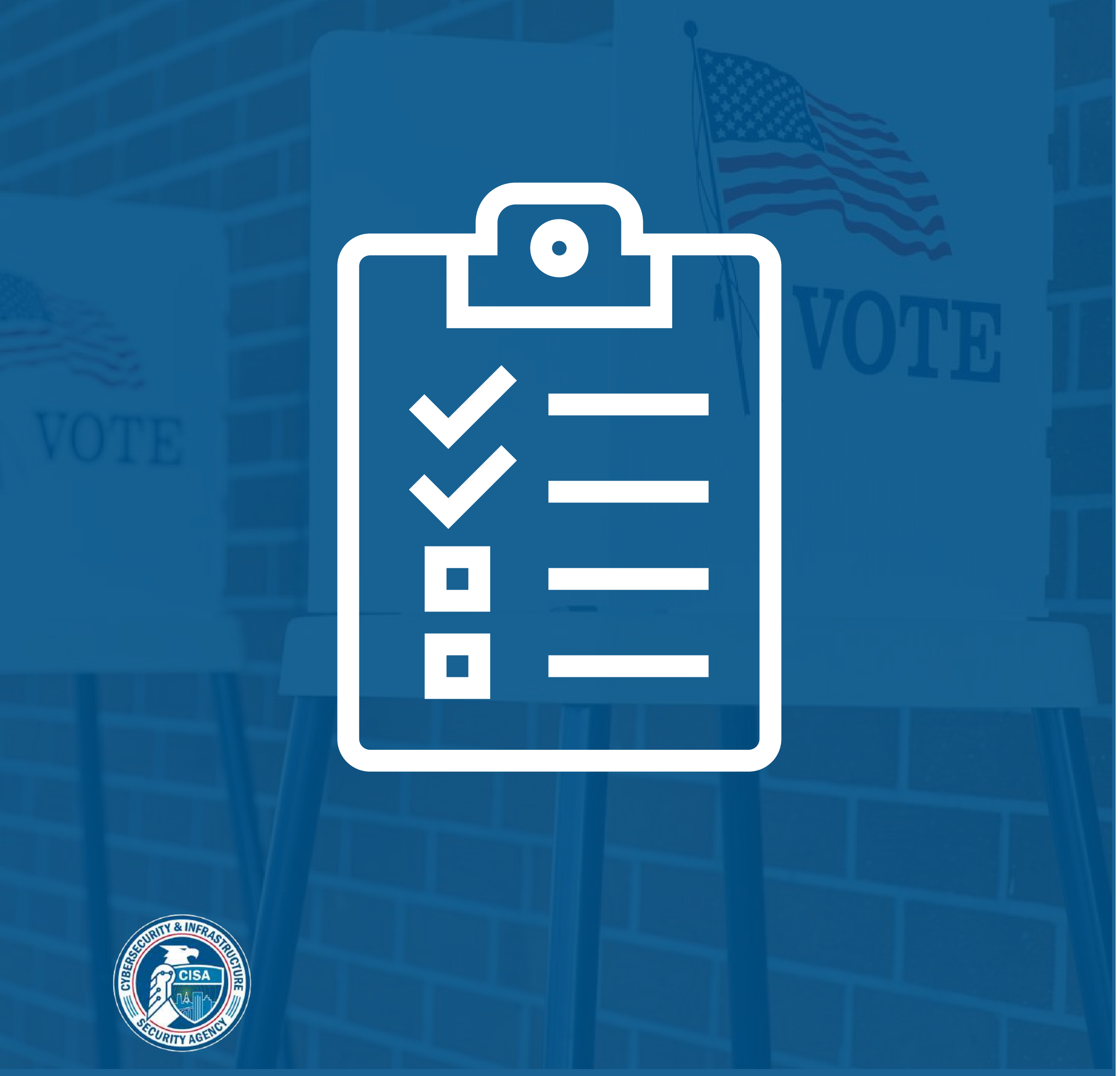
Test

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.

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.

Track: What & How

Standard Operating Procedures (SOPs)

Written SOPs can:

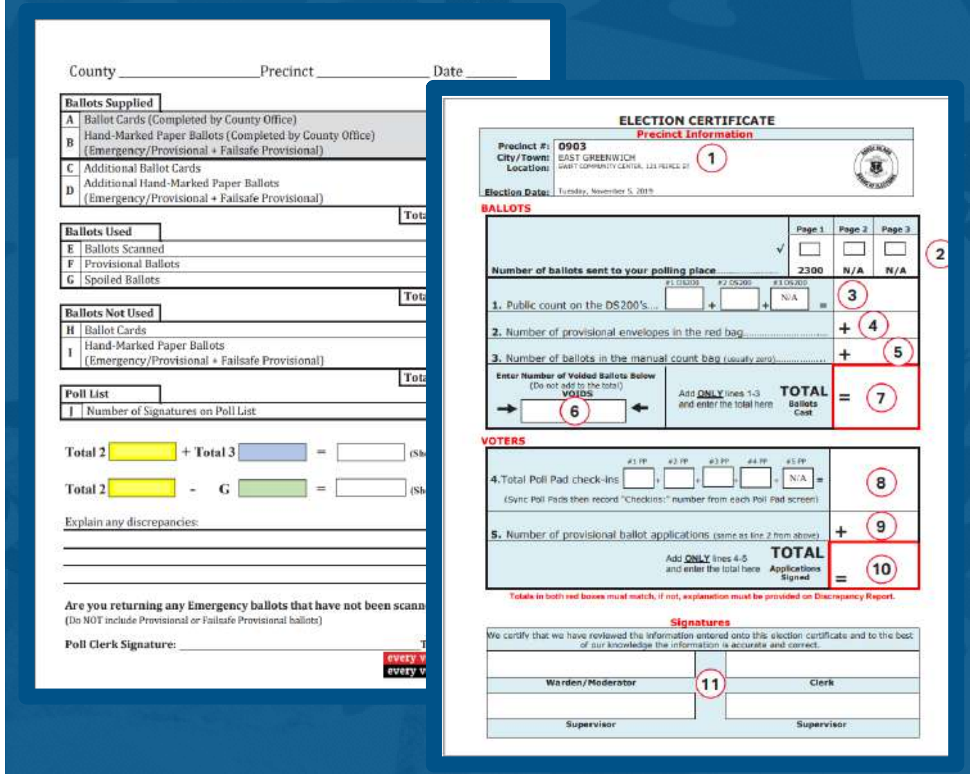
- Limit risks to the operation of election infrastructure
- Limit ad hoc decision making
- Increase quality and consistency of work across staff
- Increase productivity, efficiency and measurement opportunities
- Speed remediation time when following incident response plans

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	
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)
	Tot
Ballots Used	
E	Ballots Scanned
F	Provisional Ballots
G	Spoiled Ballots
	Tot
Ballots Not Used	
H	Ballot Cards
I	Hand-Marked Paper Ballots (Emergency/Provisional + Failsafe Provisional)
	Tot
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 scann

(Do NOT include Provisional or Failsafe Provisional ballots)

Poll Clerk Signature: ______________ T

every v
every v

ELECTION CERTIFICATE

Precinct Information

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

BALLOTS

	Page 1	Page 2	Page 3
✓	□	□	□
Number of ballots sent to your polling place	2300	N/A	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** =

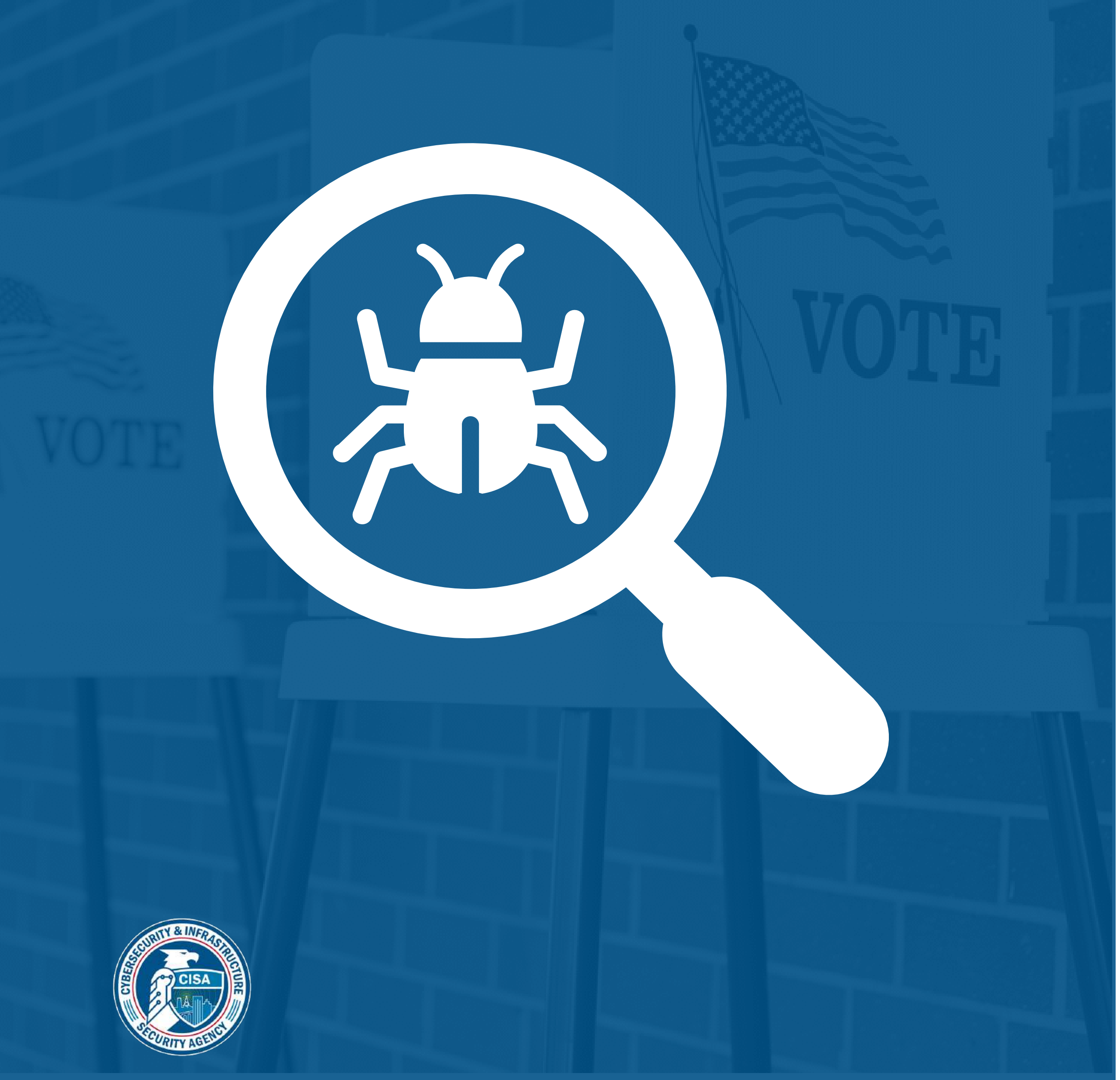
Totals in both red boxes must match, if not, explanation must be provided on Discrepancy Report.

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**

Managing Risk: Test



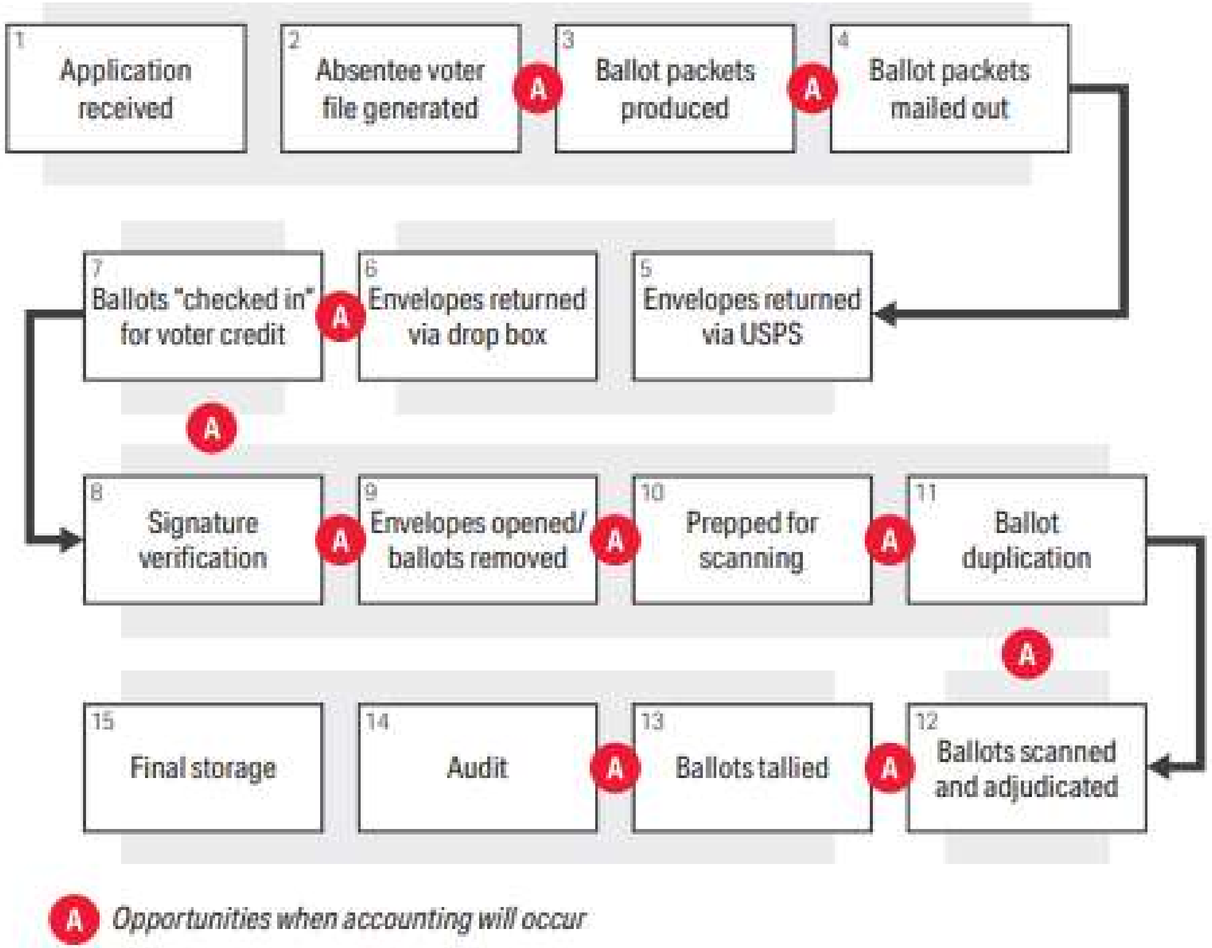
Testing voting equipment and other election assets and processes help election officials manage risk by:

- 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)

Test: Election Audits

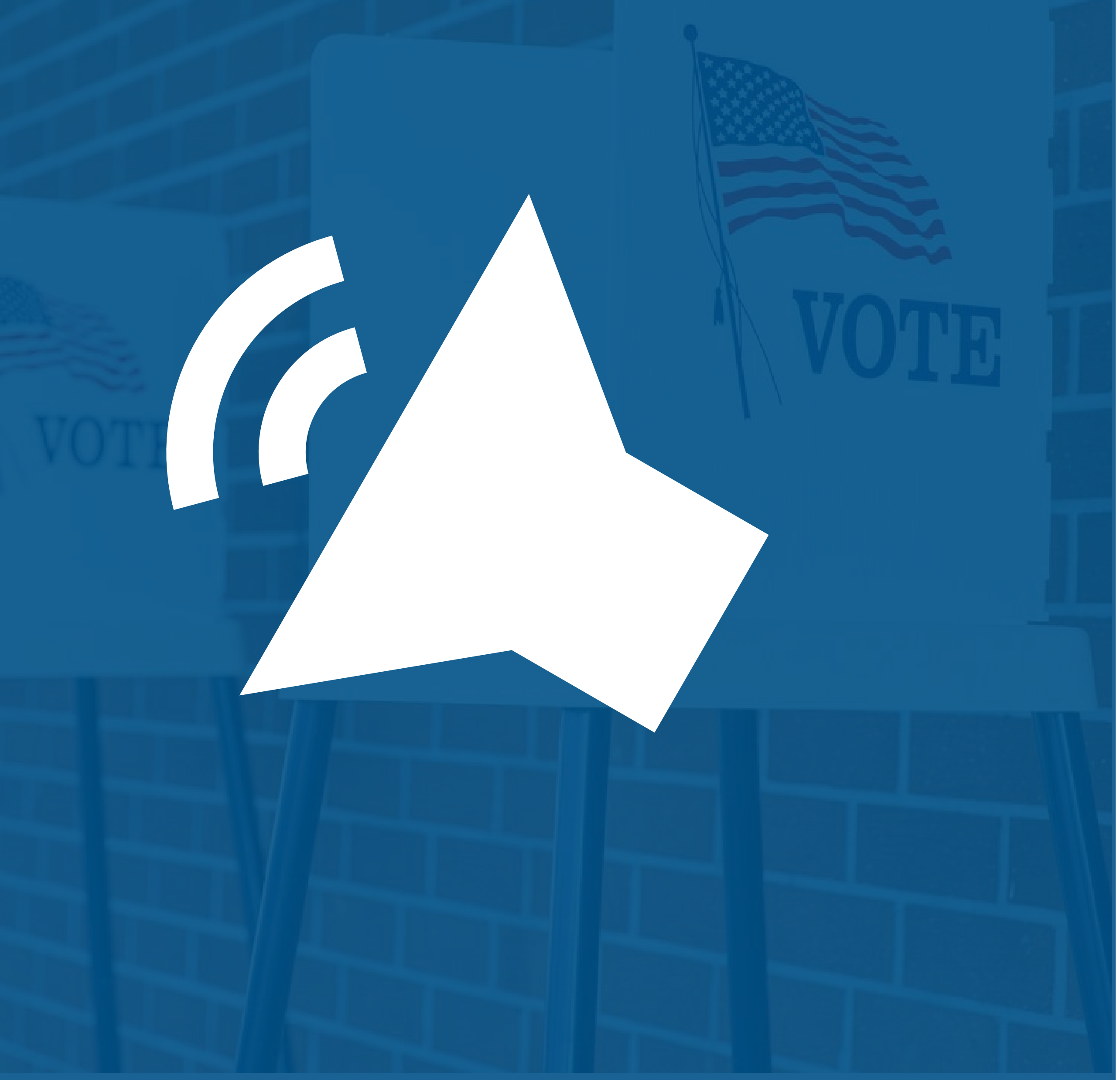
Processes to audit include:

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



1 Application received
2 Absentee voter file generated
A
3 Ballot packets produced
A
4 Ballot packets mailed out
5 Envelopes returned via USPS
6 Envelopes returned via drop box
A
7 Ballots "checked in" for voter credit
A
8 Signature verification
A
9 Envelopes opened/ ballots removed
A
10 Prepped for scanning
A
11 Ballot duplication
A
12 Ballots scanned and adjudicated
A
13 Ballots tallied
A
14 Audit
15 Final storage
A Opportunities when accounting will occur

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

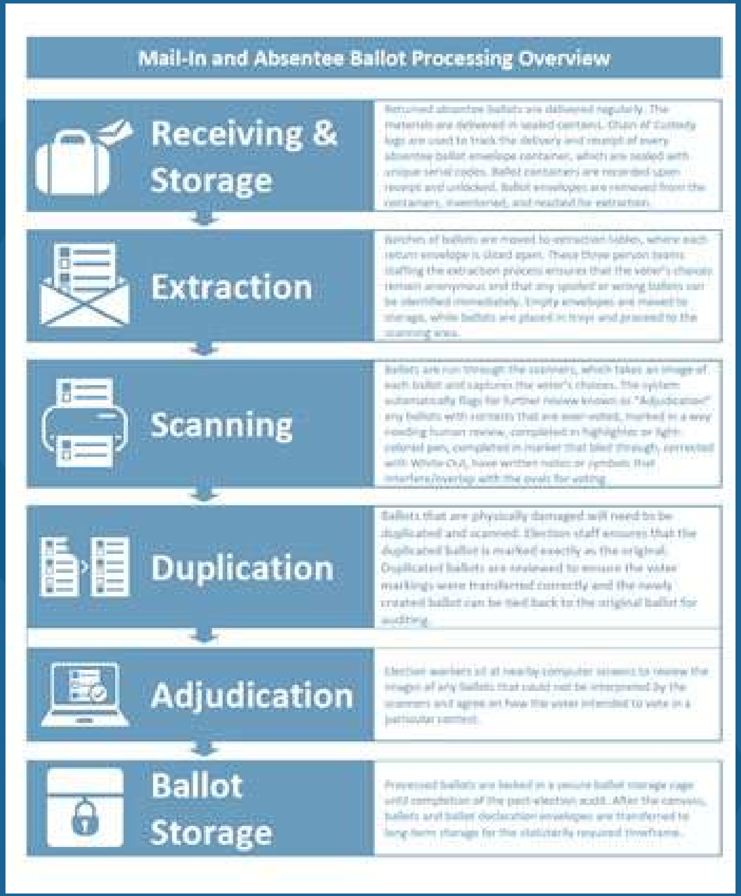
Tell: What You Can Tell Your Voters

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 procedures
- Voter registration list maintenance procedures
- Voting equipment testing and security procedures



Mail-In and Absentee Ballot Processing Overview

Receiving & Storage	Returned absentee ballots are delivered regularly. The materials are delivered in sealed containers. Chain of Custody logs are used to track the delivery and receipt of every absentee ballot envelope container, which are sealed with unique serial codes. Ballot containers are recorded upon receipt and unlocked. Ballot envelopes are removed from the containers, inventoried, and readied for extraction.
Extraction	Batches of ballots are moved to extraction tables, where each return envelope is sliced open. These three person teams staffing the extraction process ensures that the voter's choices remain anonymous and that any spoiled or wrong ballots can be identified immediately. Empty envelopes are moved to storage, while ballots are placed in trays and proceed to the scanning area.
Scanning	Ballots are run through the scanners, which takes an image of each ballot and captures the voter's choices. The system automatically flags for further review known as "Adjudication" any ballots with contests that are over-voted, marked in a way needing human review, completed in highlighter or light-colored pen, completed in marker that bled through, corrected with White-Out, have written notes or symbols that interfere/overlap with the ovals for voting
Duplication	Ballots that are physically damaged will need to be duplicated and scanned. Election staff ensures that the duplicated ballot is marked exactly as the original. Duplicated ballots are reviewed to ensure the voter markings were transferred correctly and the newly created ballot can be tied back to the original ballot for auditing.
Adjudication	Election workers sit at nearby computer screens to review the images of any ballots that could not be interpreted by the scanners and agree on how the voter intended to vote in a particular contest.
Ballot Storage	Processed ballots are locked in a secure ballot storage cage until completion of the post-election audit. After the canvass, ballots and ballot declaration envelopes are transferred to long term storage for the statutorily required timeframe.

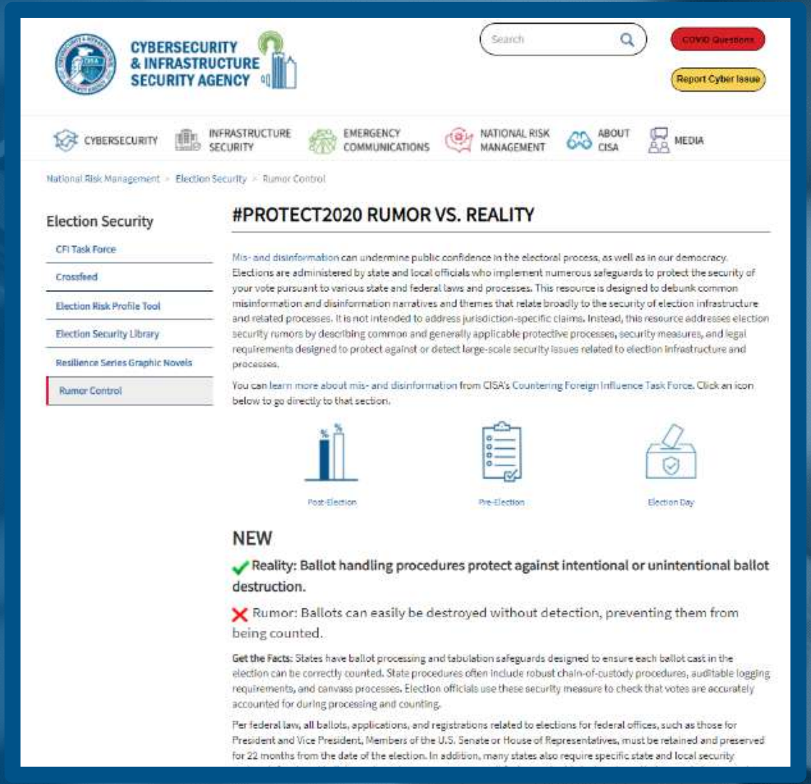
Tell: Tools for Telling Your Story

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)

Tell: 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



#PROTECT2020 RUMOR VS. REALITY

Mis- and disinformation can undermine public confidence in the electoral process, as well as in our democracy. Elections are administered by state and local officials who implement numerous safeguards to protect the security of your vote pursuant to various state and federal laws and processes. This resource is designed to debunk common misinformation and disinformation narratives and themes that relate broadly to the security of election infrastructure and related processes. It is not intended to address jurisdiction-specific claims. Instead, this resource addresses election security rumors by describing common and generally applicable protective processes, security measures, and legal requirements designed to protect against or detect large-scale security issues related to election infrastructure and processes.

You can learn more about mis- and disinformation from CISA's Countering Foreign Influence Task Force. Click an icon below to go directly to that section.

NEW

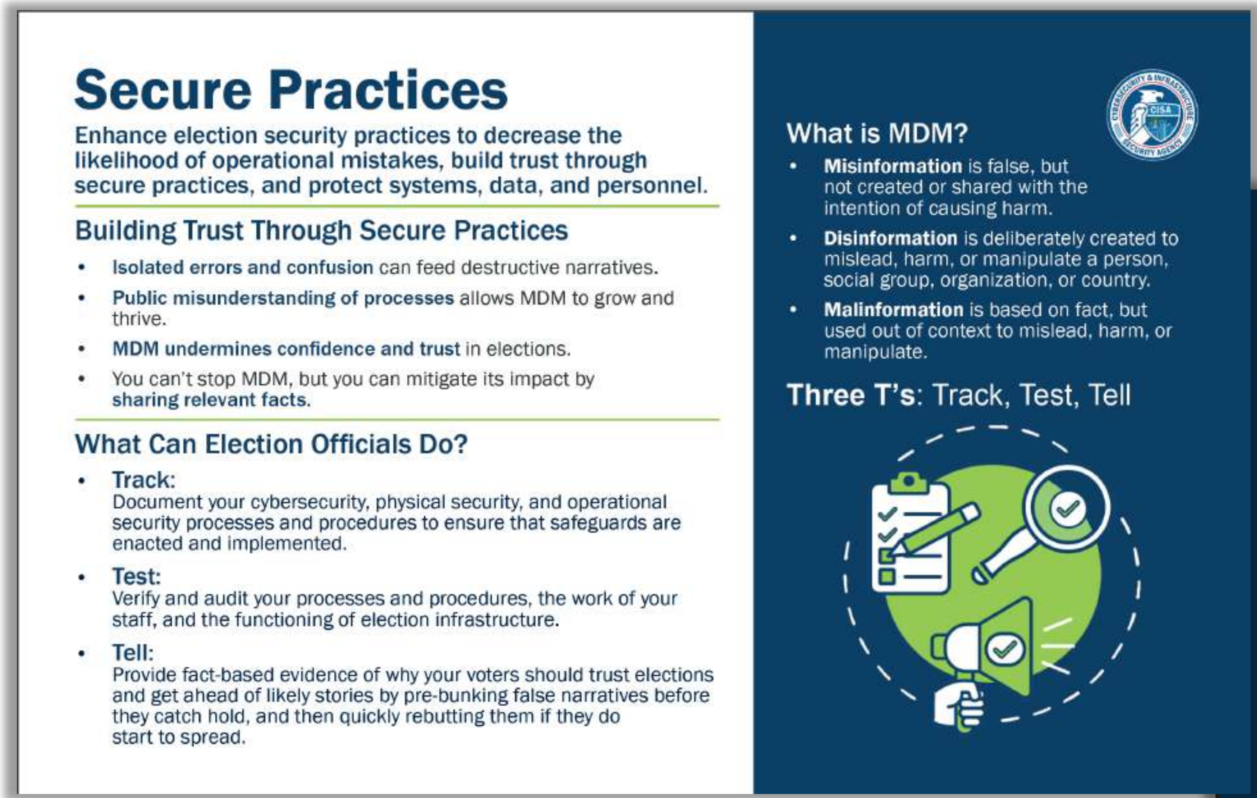
✓ **Reality: Ballot handling procedures protect against intentional or unintentional ballot destruction.**

✗ Rumor: Ballots can easily be destroyed without detection, preventing them from being counted.

Get the Facts: States have ballot processing and tabulation safeguards designed to ensure each ballot cast in the election can be correctly counted. State procedures often include robust chain-of-custody procedures, auditable logging requirements, and canvass processes. Election officials use these security measure to check that votes are accurately accounted for during processing and counting.

Per federal law, all ballots, applications, and registrations related to elections for federal offices, such as those for President and Vice President, Members of the U.S. Senate or House of Representatives, must be retained and preserved for 22 months from the date of the election. In addition, many states also require specific state and local security

Secure Practices 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.**

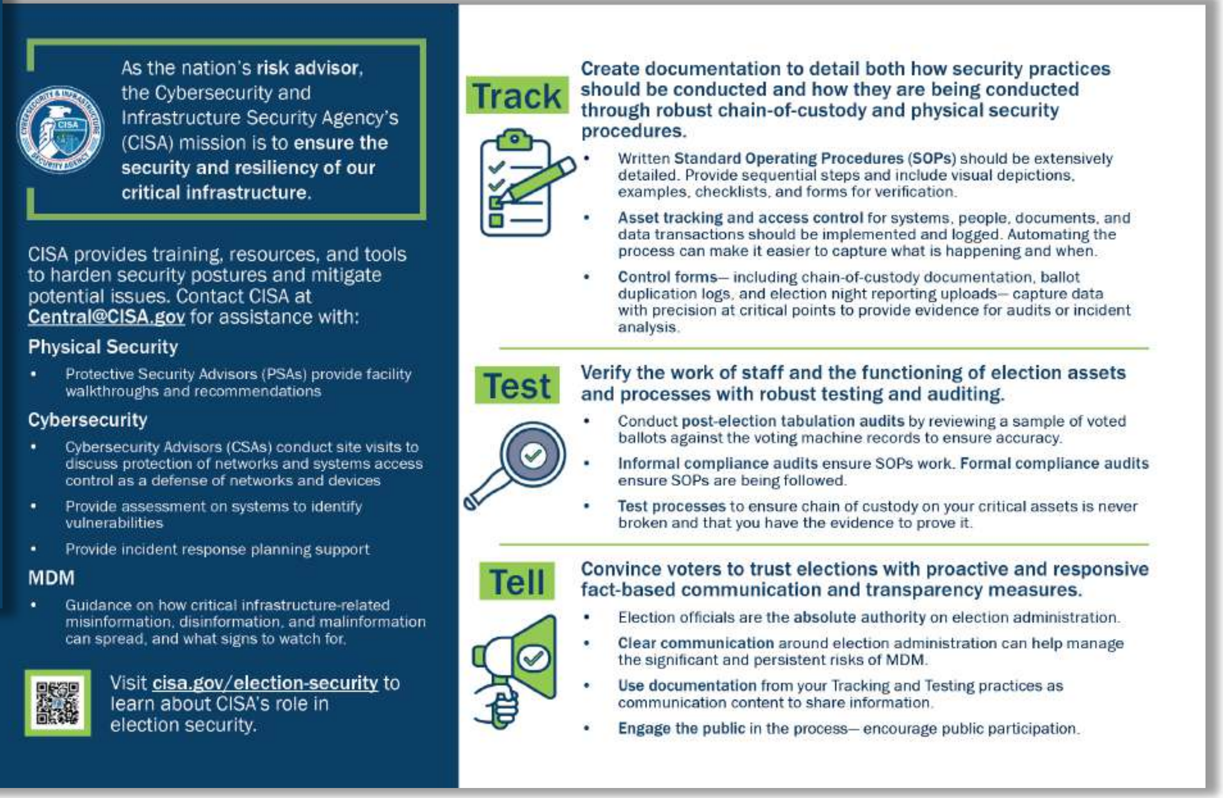
What Can Election Officials Do?

- 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



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.**

CISA provides training, resources, and tools to harden security postures and mitigate potential issues. Contact CISA at Central@CISA.gov for assistance with:

Physical Security

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

Cybersecurity

- Cybersecurity Advisors (CSAs) conduct site visits to discuss protection of networks and systems access control as a defense of networks and devices
- Provide assessment on systems to identify vulnerabilities
- Provide incident response planning support

MDM

- Guidance on how critical infrastructure-related misinformation, disinformation, and malinformation can spread, and what signs to watch 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.

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

Contact CISA:
Central@cisa.dhs.gov

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA