This document was created as part of the Election Infrastructure Government Coordinating Council and Subsector Coordinating Council's Joint Mis/Disinformation Working Group. This document is intended to be used by state, local, tribal, and territorial election officials, and industry partners as part of a larger mis-, dis-, and malinformation (MDM) response strategy. SLTT election officials should consult with their legal officer and other necessary officials in their jurisdiction prior to creating an MDM response program.

Mis-, Dis-, and Malinformation

Planning and Incident Response Guide for Election Officials

OVERVIEW

State, local, tribal, and territorial (SLTT) election officials can take proactive steps to prepare for and respond to the threats of misinformation, disinformation, and malinformation (MDM). This guide is intended to help election officials understand, prepare for, and respond to MDM threats that may impact the ability to conduct elections.

WHAT IS MDM?

CISA defines mis-, dis-, and malinformation (MDM) as "information activities." This type of content is referred to as either domestic or foreign influence depending on where it originates.

- **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.

Combined with a lack of public understanding of election processes, the changing landscape of technology and communications creates new risk and evolving vectors for the spread of MDM. This includes inaccurate information about the election process, unsubstantiated rumors, and incomplete or false reporting of results.

WHERE DOES MDM COME FROM?

MDM can originate from a variety of sources across digital, social, and traditional media, and new MDM topics emerge continuously. Foreign actors have used MDM to target American voters for decades.[1] MDM also may originate from domestic sources aiming to sow divisions and reduce national cohesion. Foreign and domestic actors can use MDM campaigns to cause anxiety, fear, and confusion. These actors are ultimately seeking to interfere with and undermine our democratic institutions.

Even MDM that is not directly related to elections can have an impact on the election process, reducing voter confidence and trust. Election infrastructure related MDM occurs year-round — it is **not just a concern in the months prior to Election Day**. False narratives erode trust and pose a threat to democratic transitions, especially, but not limited to, narratives around election processes and the validity of election outcomes.

Definitions adapted from CISA's MDM Resource Library. For an overview of tactics used by disinformation campaigns—such as manipulating audio and videos, conducting forgeries, and developing proxy websites in order to undermine public confidence and sow confusion—see Tools of Disinformation: Inauthentic Content.

[1] Joint Cybersecurity Advisory: AA20-296B Iranian State-Sponsored Advanced Persistent Threat Actors Threaten Election-Related Systems

HOW DOES MDM IMPACT ELECTION SECURITY?

Depending on the narrative, MDM can have various impacts on election security. Categories may include:

Impact	Description	Example (from CISA's Rumor Control page)
Procedural Interference	Narratives or content related to election procedures that cause confusion and interfere with officials' ability to smoothly administer an election.	✔ Reality: Safeguards are in place to prevent home-printed or photocopied mail-in ballots from being counted. ✘ Rumor: A malicious actor can easily defraud an election by printing and sending in extra mail-in ballots.
Participation Interference	Content that might intimidate or deter voters from participating in the election process.	✔ Reality: Voters are protected by state and federal law from threats or intimidation at the polls, including from election observers. ✘ Rumor: Observers in the polling place are permitted to intimidate voters, campaign, and interfere with voting.
Delegitimization of Election Results	Narratives or content that delegitimizes election results or sows distrust in the integrity of the process based on false or misleading claims.	✔ Reality: Election results reporting may occur more slowly than some voters expect. This alone does not indicate a problem with the counting process or results, or that there are issues affecting the integrity of the election. Official results are not certified until all validly cast ballots have been counted, including ballots that are legally counted after election night. ✘ Rumor: If results as reported on election night change over the ensuing days or weeks, the process is hacked or compromised, so I can't trust the results.
Personnel Security	Narratives or content that falsely claims election officials or poll workers are the "bad actor" attempting to interfere in election results or processes.	✔ Reality: Robust safeguards including canvassing and auditing procedures help ensure the accuracy of official election results. ✘ Rumor: A bad actor could change election results without detection.

RESPONDING TO MDM

In today's media and information environment, election officials must play a proactive role in responding to MDM. While each MDM narrative will differ, leveraging the ***TRUST*** model for MDM response can help reduce risk and protect voters.

It is important to acknowledge the opportunities and limitations of government-led MDM intervention—particularly where distrust of government may be fueling the narrative. Focus responses where your team has evidence, expertise, or authority to counter the MDM. Also, recruit trusted community partners to amplify your messaging.

Categories adapted from the Election Integrity Project's (EIP) final report on misinformation and the 2020 election (Revised March 2021).

1. TELL YOUR STORY

Public resilience is increased as your team builds relationships with voters and stakeholders. Educate your communities about election processes and MDM-related threats before they occur.

Educate voters: Educating constituents on how to engage in the electoral process and promoting civic learning is critical to countering MDM. **Communicating clearly in tone, language, and medium, as well as leveraging credible voices your audience trusts** will help reach and engage constituents to convey information about important dates/deadlines, polling locations, processes for voting change, and where to find trusted information about elections and election results.

> Media literacy includes verifying sources, seeking alternative viewpoints, and finding trusted sources of information. The National Association for Media Literacy Education has members in every state that can work with election officials to develop media literacy content. CISA's Resilience Series graphic novels are a great example of a resource aimed at developing media literacy and critical thinking to counter disinformation.

Pre-bunk MDM: Providing constituents with information and resources before MDM activity emerges better equips Americans to identify and question false narratives. In some cases, by leveraging insights from your staff, **you can anticipate where MDM narratives may arise**, such as how election officials secure elections through the use of post-election audits and similar safeguards. Addressing these topics with voters *in advance of* elections and explaining how they are used in MDM narratives can increase resiliency and confidence among voters.

Build media relationships: Reach out to local newspaper, radio, television, podcasts and other media outlets to **build working relationships before election cycles**. Invite them to learn more about how election processes secure election results and key voter education details. Make sure they have a contact in your office. Establishing working relationships with media outlets and journalists helps quickly and pre-emptively debunk or expose MDM activity. It can also help inform accurate reporting around elections, limiting the propagation of misinformation.

2. READY YOUR TEAM

The effectiveness of your response will depend on how much preparation is conducted internally ahead of MDM activity.

Establish your response protocol: Establish a **clear procedure for responding** to MDM and **educate team members** about the process.

- Understand the procedures for reporting or flagging potential online MDM to social media platforms often used by your constituents. Consult with your legal counsel to ensure you respect constitutional rights and privacy protections and abide by any legal restrictions.
- The Center for Internet Security (CIS) was established to support the cybersecurity needs of the election subsector. The CIS can be leveraged to report real-time MDM via email at misinformation@cisecurity.org. Be sure to include links and screenshots, as well as details on the misinformation and your jurisdiction.
- Determine internal roles and responsibilities, including an escalation process within your jurisdiction to ensure the right teams are talking to one another while responding to MDM activity. Be clear that this is not "just" a communications issue; it requires engagement from across departments to ensure responses are accurate and understandable.
- Designate an individual to be responsible for ensuring this process is established, updated, and shared both internally and with relevant stakeholders at the local, state, tribal, territorial, and federal levels — including your CISA Regional Office.
- Hold or participate in tabletop exercises to increase your team's awareness and understanding of MDM threats, evaluate your overall preparedness, identify deficiencies in your incident response plan, and clarify roles and responsibilities during an incident. CISA can assist in development and execution of these exercises, or CISA's Tabletop in a Box resource can help you talk through possible scenarios with your team and stakeholders as well.

Build credible information-sharing channels: MDM can thrive in the absence of easily accessible, credible information. Ensure your agency's website, social media accounts, and other information channels are up to date and active so you can directly respond to MDM. This can help your community have confidence that the messages your organizations disseminate are authoritative and you can further build public confidence in election administration.

- Register your website for a .gov address so the public does not have to guess whether your websites and emails are genuine. CISA makes .gov domains available solely to U.S.-based government organizations and publicly controlled entities **without a fee**.
- Many social platforms (e.g., Facebook, Twitter) will also allow government organizations and users to apply for verification badges. Local election officials should reach out to their state for more information on how to get their accounts verified.
- Consider pre-bunking MDM on your website by responding to common questions relevant to your responsibilities. The Rumor Control Start-Up Guide provides further guidance on establishing this webpage and how to assess which topics to include.

Prepare for incoming questions: Ensure your office has methods for fielding public feedback and questions, including **being able to handle a large influx of calls or messages**. Consider creating a shared voicemail and email inbox so that no one person becomes overwhelmed, with a log to track inquiries and responses. These mailboxes should be regularly checked and there should be an established process for determining who will respond. This will enable your team to both uncover MDM that is circulating and keep systems and phone lines functioning during critical periods of MDM activity. Ensure staff are aware of your office's procedures for reporting threats and harassment, and if possible, rotate responsibilities for responding to calls and emails to avoid burnout.

Team Checklist

- ✓ Understand reporting mechanisms for flagging MDM on social media.
- ✓ Determine roles and responsibilities for MDM response.
- ✓ Designate an individual to oversee the MDM response process.
- ✓ Register your website for a .gov address.
- ✓ Apply for verification badges from social media platforms.
- ✓ Develop a list of common topics and questions vulnerable to MDM.
- ✓ Ensure your communication systems are set up to handle incoming questions.
- ✓ Engage with counsel and, if applicable, your privacy office to ensure protection of constitutional rights and privacy.

3. UNDERSTAND & ASSESS

It is important to understand, to your best ability, the full nature and scope of the MDM activity.

Identify MDM activity: While every election jurisdiction has different resources and capabilities, you should establish a system for identifying and evaluating MDM in your office. Determine if it is appropriate for your office to engage with outside organizations or tools to better understand the risk landscape and monitor for MDM, including your technical systems provider. Monitoring may be proactive, via analytic tools, or reactive, through public feedback channels.

- **Identify and continuously update a list of key elections-related processes and issues vulnerable to MDM**, whether they are short-term trends or long-term narratives. Ensure all members of your office have access to this list and feel comfortable contributing to it. The person responding to inquiries will therefore have a good sense of what topics people are asking about, and who to contact for answers, even if they don't know how to answer the question themselves.
- **Identify the channels that constituents use to receive information.** MDM content can spread through numerous means, including social media, mainstream media, word of mouth, online forums, messaging apps, and emails. Remember that MDM narratives also often move between channels, so content that appears on one platform may also emerge elsewhere.
- For the high priority topics on your list, including those you worked to pre-bunk, **you may want to take a more proactive approach to monitoring for MDM narratives, to the extent permitted by law**. Consider using analytic tools to search for keywords related to MDM content. Evaluate content reach (how many people are seeing it), engagement (how many people are liking, sharing, or reacting to the content), how many channels it is present on, and whether it has reached mainstream media. Consult with your legal counsel to determine what monitoring is permissible under law and platforms terms of service.
- **Leverage publicly available analytical tools**, such as those recommended by the RAND Corporation's Fight Disinformation at Home resource, which can help you gain a greater awareness of the information ecosystem.

Assess the Risk: The team should identify what plausible risks are associated with MDM narratives and how they may impact election infrastructure. Mapping out existing MDM narratives and their impact on elections infrastructure will help the team be prepared for the online and offline consequences and impact to elections infrastructure.

4. STRATEGIZE RESPONSE

Once you have identified MDM, it is important to craft an effective response, taking into account how the information environment and related technology may evolve.

Determine your response: Based on your risk assessment, prioritize which MDM narratives to respond to. In crafting your communications strategy, consider both timing and medium of response.

- **Not all MDM activity warrants an immediate response**. Deciding which rumors make the cut is an exercise of an organization's judgement — and that judgement may change as MDM narratives evolve and community response changes.
- **Understand your audience** for the MDM intervention. Your community isn't homogeneous, and your audience will change depending on the message you are trying to convey and the medium you use. Adapt your messaging to the audiences you are trying to reach, such as new voters, veterans, individuals in specific geographic regions, or those who speak other languages.

Apply communications best practices: In a crisis, specific tactics and language can help build the credibility of your response and reassure voters. Tactics may also look different based on the activity and the audience. A communications strategy might include **social media, radio, local news, or other media platforms** to engage constituents.

Election officials across the country are combatting election-related MDM.

- The Colorado Secretary of State's office conducted social media and digital outreach to voters and set up a website to educate on the threat misinformation and respond to MDM narratives.
- The Kentucky Secretary of State's office launched a Rumor Control page on their website to counter MDM narratives around elections.
- The Wisconsin Elections Commission established a designated FAQ page to answer voter questions about the 2020 election.
- The Maricopa County, Arizona, Elections Department launched a website to address questions and misconceptions about the 2020 election and has engaged in rumor control efforts across social media.

- Identify where your audience receives information and, if possible and advisable, establish a presence on these platforms. It will likely not be realistic for your office to actively use every platform. Focus on using a smaller number of platforms effectively to establish your handle as a trusted source of information.
- Ensure you have the facts before responding.
- State facts first, rather than repeating a falsehood in your headline.
- Be careful not to amplify the source of the MDM by linking to it directly or sharing original images or videos. If referencing an image, use a screenshot with a text overlay that explains the image is inauthentic or misleading. Consider what privacy protections are necessary for all media shared.
- Consider the length of your response. Shorter statements are more easily digestible and can be helpful when the MDM is easily disproven.
- You do not need to respond to each incident of MDM individually. Point back to your office's previous posts, statements or work if MDM recirculates. Inconsistent messaging can create credibility problems.
- Leverage partnerships and trusted community messengers to counter MDM narratives. **Repetition and consistency are key**. Conveying the same message through multiple mediums and platforms will help reach the broadest audience possible.

5. TRACK OUTCOMES

After your response, evaluate the continued prevalence of MDM and evaluate ways to adjust processes moving forward.

Manage and monitor repercussions: While MDM narratives may be effectively addressed or accounts spreading disinformation may be removed, manipulators will often find ways to circumvent these changes. Creating new accounts, adapting coded language, altering audio/visual material, and iterating on narratives already identified as objectionable by platforms are all possible adjustments deployed to increase MDM efficacy. It is important to monitor the MDM environment, as resources allow, to remain aware of changes and adjust response tactics accordingly.

Reassess response strategy: Following an MDM response effort, revisit and reassess your process, including your list of priority topics for media monitoring. In the current information environment, threats are constantly evolving, and the locations, mediums, and narratives of MDM are changing as well.