Managing Inaccurate Election Information

Inaccurate information about election administration and its processes is nothing new. These days, some refer to this as mis-, dis-, and mal-information, but election officials have long worked to ensure voters know their rights and responsibilities–and don't get misled by intentional or unintentional inaccuracies. Each has a increasingly common terms has a specific definition:

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

Both independent threat actors and large nation-states are capable of manufacturing inaccuracies about elections, and some unintentional mistakes will always happen. Threat actors may have hundreds of human threat actors on payroll or choose to conduct operations via automated bots. When users encounter inaccurate information or intentional disinformation they may be unable to differentiate it from genuine information, sharing it and unwittingly influencing an even wider audience.

Increasingly, these threat actors use artificial intellience in their work. Certainly not all uses of artificial intelligence are nefarious, but it is a tool that can be employed to accelerate the pace of harmful activities and create more believable material. This guide also provides guidance on how to manage AI in elections.

Influencing the political environment through social discourse is a tactic observed in well-funded and complex information attacks, but actors may have competitive, financial, or other motivations as well. Disinformation attacks can function by creating continued influence in a system or sector. Attackers may try to popularize perspectives and viewpoints in target demographics that lead to certain policy or political outcomes. Appearing as authentic citizens or a real customer base on social media, individual disinformation accounts can appeal to users and align with their existing beliefs. Organizations and individuals alike then experience the pressure to act on what is perceived as recurring legitimate messaging but, in reality, is deception.

Often, inaccurate statements about elections are unintentional and just the result of misinformed individuals. As election officials, it's not always important to understand the source or intent of the inaccurate information, but to simply address it to maximize the number of potential votes that have accurate messaging. That is the focus of this best practice.

Goals

1. Recognize how inaccurate information can impact election administration (Level 1 maturity)
2. Take action when you encounter inaccurate information (Level 1 maturity)

Actions

For Managing Inaccurate Election Information, the necessary actions vary by maturity as detailed below.

Level 1 Maturity

At Level 1 maturity, simple steps can help you manage misinformation and address it when it occurs.

Preparing for Mis-, Dis-, and Malinformation

1. Set up multi-factor authentication to protect social media accounts from compromise.
2. Establish your office and its communication channels as the authority for information about your jurisdiction.
3. Use public forums to actively counter misinformation.
4. Regularly publish official messaging about the state of your election infrastructure.
5. Work with local media to promote official sources of information.

Remediating Misinformation

1. Establish your office and its communication channels as the authority for information about your jurisdiction by:
   - Communicating with your constituents early and often, and making sure they know the official way to get more information from you.
   - Securing your systems, including websites and social media accounts, to prevent things like deep fakes being posted on an official channel.
   - Signing up for a .gov website domain to signal your status as an official government organization
2. Respond to inaccurate information with accurate information as quickly as possible. This rapid response is even more important as an election nears. These activities are sometimes called debunking or pre-bunking, but what's important is that you are getting an accurate message out in a way that helps your voters, and the public writ large, the most.
3. Track important information by, for instance, following your county name and the names of your election official and other public figures in social media and new reports.
4. Understand the increasing role of generative artificial intelligence in elections and what you can do about it.
5. Election officials can often report identified misinformation to the platforms hosting it, such as email providers or social media platforms. Based on the platforms' terms of service, they may take action on your report.
   - Report anything on social media that's about your jurisdiction, pertains to the administration or security of an election in the United States, and is inaccurate or misleading.
   - Opinions are not misinformation. Only report inaccurate information about election administration itself.
   - Examples include, but aren't limited to, dates of the election, mail ballot rules, ballot information, polling place hours and status, election night reporting procedures, post-election procedures, and voting technology.
   - Here's some information about the approaches of popular platforms. Some of these instructions may no longer be available to users.
     - Meta, including Facebook, Instagram, and WhatsApp
     - X (formerly Twitter)
     - Google
     - Snap
     - TikTok

Level 2 Maturity

Organizations operating at a Level 2 maturity should take additional actions, including:

1. Establish a mechanism for the public to report inaccurate information they encounter to your office, such as an email, phone number, or web form.

Level 3 Maturity

Organizations operating at a Level 3 maturity should take additional actions, including:

1. Consider having a focused workstream to identify and remediate inaccuracies. This can include things like:
   - Tracking hashtags, keywords, and other trends on various social media platforms.
   - Following activity related to your election across a number of platforms, including smaller, niche apps.
   - Contracting with a third party to provide these services for you.
   - If a state, providing services for your locals.

Cost-Effective Tools

- CISA's Rumor vs Reality page: This page is designed to address common disinformation narratives by providing accurate information related to elections.
- CISA, the Federal Bureau of Investigation, and the Office of the Director of National Intelligence's report Securing Election Infrastructure Against the Tactics of Foreign Malign Influence Operations.
- The National Association of Secretaries of State #TrustedInfo2024 site: NASS's public education effort to promote election officials as the trusted sources of election information during the 2024 election cycle and beyond.
- The National Association of State Election Directors FAQs: NASED compiled Frequently Asked Questions to provide high-level information about election administration.
- The Harvard Kennedy School's Belfer Center publication, The Election Influence Operations Playbook: A document to provide advice and guidance for election officials to assist them in better understanding, countering, and responding to influence operations.

Mapping to CIS Controls and Safeguards

- There are no relevant CIS Controls.

Mapping to CIS Handbook Best Practices

- There are no relevant Handbook best practices