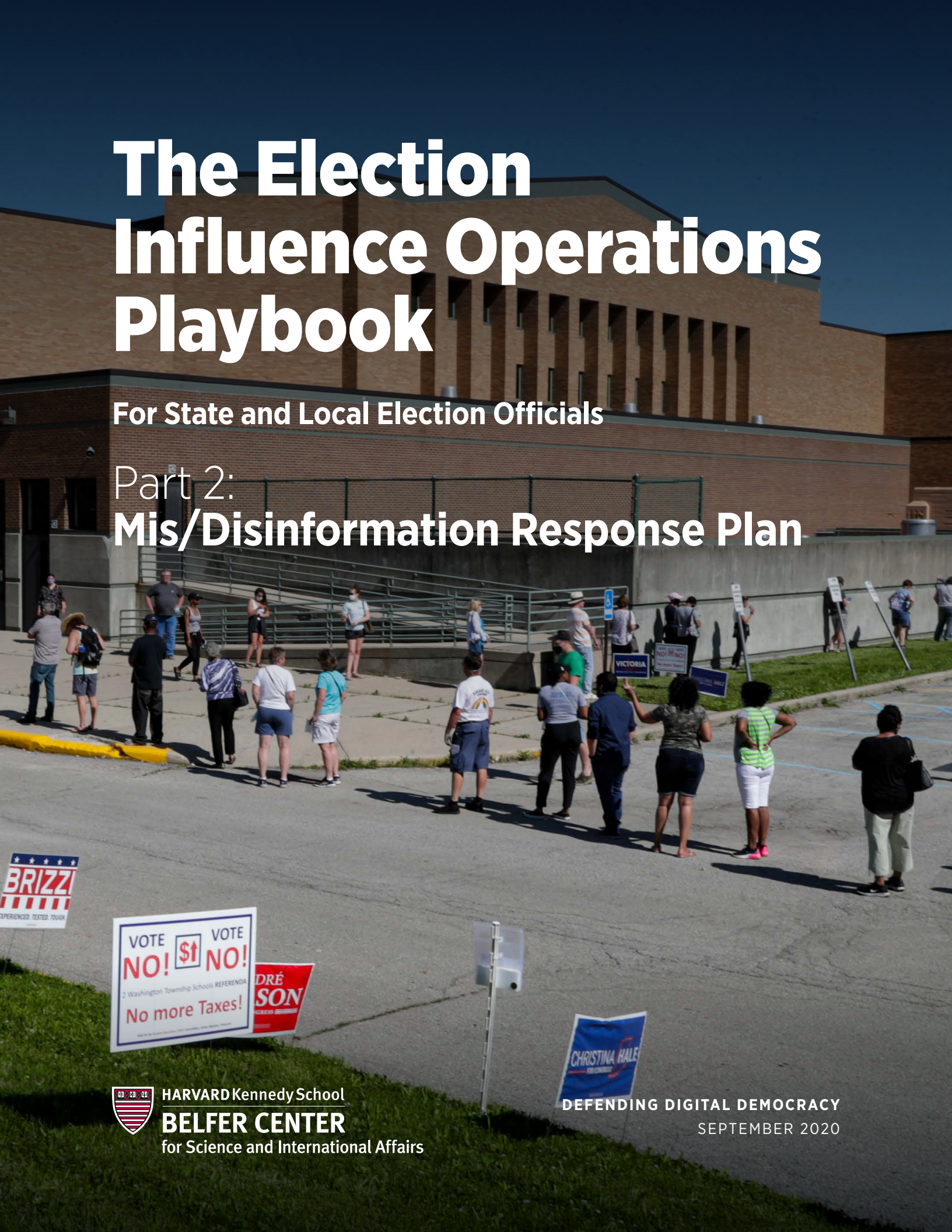
The Election Influence Operations Playbook

For State and Local Election Officials

Part 2: Mis/Disinformation Response Plan



HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

DEFENDING DIGITAL DEMOCRACY
SEPTEMBER 2020

Defending Digital Democracy Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/D3P

Design & Layout by Andrew Facini

Cover photo: Voters wait in a line outside Broad Ripple High School to vote in the Indiana primary in Indianapolis, Tuesday, June 2, 2020 after coronavirus concerns prompted officials to delay the primary from its original May 5 date. (AP Photo/Michael Conroy)

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

DEFENDING DIGITAL DEMOCRACY
AUGUST 2020

The Election Influence Operations Playbook
Part 2: Mis/Disinformation Response Plan

Contents

Introduction:
The Four Stages of Countering Election Influence Operations

Modern influence operations typically attack the democratic process online and can spread quickly. The most effective responses are swift, simple, and clear. A unified team effort, including those responsible for operations reporting and incident communications segments of your team, should be engaged in countering these efforts.

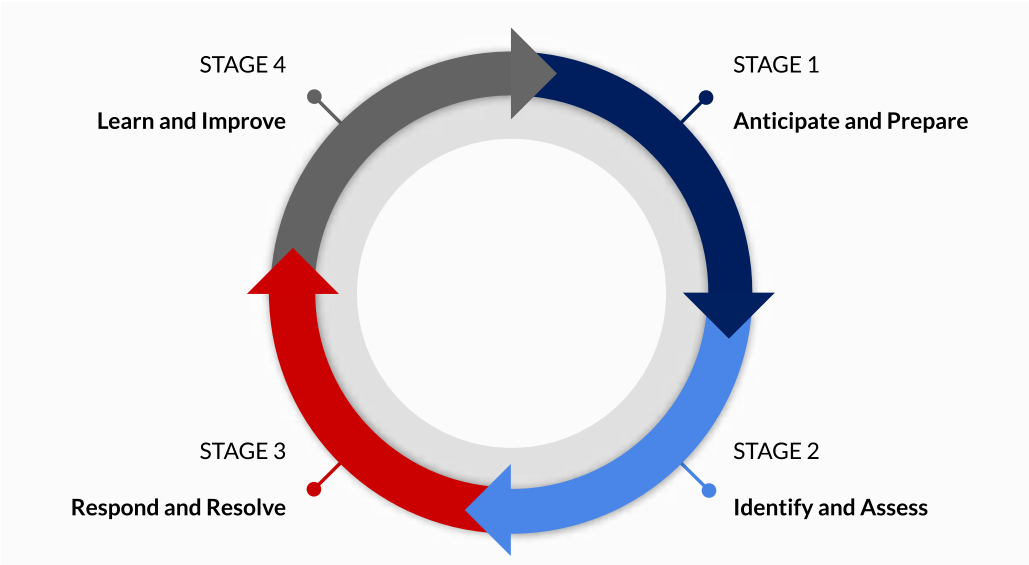
This Part 2 guide of the Playbook includes guidelines and template materials focused on the response process to help election officials respond to election-related mis and disinformation incidents quickly and in a coordinated fashion.

In this playbook, we refer to mis/disinformation throughout as one concept. Instances of both misinformation and disinformation in the elections process provide incorrect information to voters. Incorrect information can be conveyed intentionally or unintentionally. For election officials, any incorrect information, regardless of source or intention, presented to voters can pose a threat to elections, because it can undermine voters' understanding of and trust in the election.

Plans, especially crisis response plans, often evolve as an incident unfolds. You should update it to fit your needs as often as necessary but no less than once a year. One central organization should own this plan and lead stakeholders and organizations through a process of familiarizing themselves with the updated plan. The plan owner may also consider guiding a process to collect input from related users for updating the plan.

There is no conclusive solution to counter mis/disinformation incidents. The recommendations in this playbook will need to change as these tactics evolve. The most effective means to counter mis/disinformation incidents is to ensure that your office is a well-known, trusted source of information on election processes and requirements, in advance of election day.

In this guide, we advocate for a four-stage approach to counter IO which can help you make a response plan:



1. **Anticipate & Prepare**
    - Steps officials can take ahead of elections to make mis/disinformation incidents less likely to occur or to lay a foundation for an efficient response to such incidents.
2. **Identify & Assess**
    - How officials can identify mis/disinformation incidents and assess their relative severity.
3. **Respond and Report**
    - What officials can do to address mis/disinformation incidents when they occur.
4. **Learn and Improve**
    - How officials can learn from past mis/disinformation incidents to improve responses and defenses in later election cycles.

This guide's **Toolkit** includes templates and important information to use in drafting a respose plan and in reporting.

A Master Checklist can be found in this guide's Toolkit, **pg. 33.**

Stage 1: Anticipate & Prepare

Mis/disinformation incidents targeting the election system can exploit gaps in voters' knowledge about the election process, undermine trust in the process, and damage faith in our democratic system.

The most effective way to prevent mis/disinformation incidents is to reduce the number of areas where gaps in knowledge exist. Educating the public well in advance on the basics of the process and what to expect on voting day is the best way to fill these gaps. Ensuring that the information you provide about the 'who, what, when, where, how' (the "5 Questions") of the election process is completely up to date and well publicized.

Planning and conducting regular public outreach across various mediums, online, in-person and establishing relationships, and sharing information with media, election colleagues, voters, community organizations, and other stakeholders will help lay the groundwork for an efficient response.

To lead confidently, election officials need to prepare, train for, and test responses ahead of time. This effort includes establishing election officials as a trusted and authoritative source of information prior to Election Day. Building a community of trusted voices that can join you in countering false information will validate and help quickly move your message. Coordinated and timely responses are important.

Build Your Team and Plan Your Communications Response

It's critical to establish in advance who on your team will respond to a mis/disinformation incident. Elections officials should create a communications plan that provides escalation thresholds for reporting an incident internally and publicly. The guidelines should address who is responsible for communicating to key external stakeholders, such as the media, the social media platforms, voters and law enforcement. It should also spell out the timeframe for these communications and key individuals involved in the communications response. Your team will support your communications response process to incidents. Creating a communications response plan, taking note of the coordinating recommendations, will prepare you to respond quickly.

Jurisdictions will need to tailor response guidelines to their local circumstances, particularly smaller counties with smaller teams. In these instances, coordination with other bodies is particularly important.

Establishing an Incident Response Team

Mis/Disinformation incident response should use, to the degree possible, the processes a jurisdiction already has to respond to other election-related crises. It should be able to quickly adjust to respond to specific issues and adapt to address mis/disinformation incidents.

Key roles and responsibilities can include:

- **Chief Election Official** The key decision maker responsible for consulting and activating a jurisdiction's incident response plan.
- **Director of Elections** Responsible for coordinating communications information with local elected officials and administrators in a jurisdiction.
- **Communications Team** Key roles for these team members include: message development in cooperation and coordination with key internal and external stakeholders; communicating with the public via the media and your own channels e.g. website and social media; liaising with social media companies and tech platforms to report content; and monitoring social media for new information.
- **Jurisdiction [Local IT Director/CIO, Information Officer]** Responsible for coordinating with the Communications, IT, and other staff and leading any technical reponses.
- **Government and Community Relations Director** Responsible for coordinating governmental briefings for members of state legislatures, county commissioners, and other elected officials.
- **Chief Legal Officer** Responsible for advising the office on legal matters.
- **Law Enforcement Liaison** Responsible for coordinating communications information with law enforcement and affiliated communicators.
- **Affected Local Elections Administrators** Local officials from affected local jurisdictions representing a "field" perspective and providing relevant incident-related information to the coordination process. These officials may also help identify mis/disinformation incidents given their proximity to voters.

Communications Coordination

The following steps will serve as a guide as you build a response team and develop a response plan.

Step 1:	**Decide on your team.** • Select the individuals who will fill the roles previously listed. • Outline their roles and identify the decisions around messaging and communication that they can make in real time. • Determine which people in your team are responsible for monitoring and reporting mis/disinformation. • Monitoring can include details or tools from other parts of your planning (see 'Identify and Assess' section). • Reporting can include election bodies, federal authorities and the social media platforms (see 'Respond and Resolve' section).
Step 2:	**Internal communications.** • Establish how you will communicate across your team in an incident. • Make sure there is a backup communications plan/channel in place. » Options you may like to consider include chat tools like a slack channel, encrypted texting tools like Signal or back up Gmail accounts with two factor authentication turned on. » Messaging tool settings should confirm backup logs and chat histories can be recorded. » Ideas for planning communication channels can be found in D3P's Elections Battle Staff Bootcamp Playbook, pg. 16-21.[1]
Step 3:	**Self assessment and scenario planning.** • Building on the scenario planning from Step 3, 'Know the Threats' and the Part 3 Mis/Disinformation Scenario Plans Template, the team should discuss new tools, or processes that may help identify instances of mis/disinformation.
Step 4:	**Stakeholder analysis.** • Assess and prioritize your key stakeholders, based on their influence on voters, because public opinion can turn very quickly as mis/disinformation spreads. • Establish ongoing relationships with these stakeholders before a crisis and decide who would be willing to be a validator to amplify your response to a disinformation incident. • Your stakeholders may include: » Voters » Federal, state, and local elections communications counterparts » County registrars, clerks or auditors » Election workers and voting locations » Law enforcement » State and federal lawmakers » Media » Political parties and campaigns » Third-Party advocacy groups » Nonprofits and civil society groups » Local community leaders and elected officials

1 Belfer Center, December 2019, "The Elections Battle Staff Playbook": https://www.belfercenter.org/sites/default/files/2019-12/Battle%20Staff.pdf

Step 5:	**Response support and alignment.** • Determine and document how you will coordinate with stakeholders and establish relationships in advance. • It may be helpful, as appropriate, especially for high severity incidents, to have intra-state, cross-state, or national communication and collaboration partners in your stakeholder map. • Key organizations to establish a contact with or designate for regular communications include: » **Local:** Develop good working relationships between state and county registrars, clerks, and/or auditors. The relationships and credibility of each team member and group is vital to a successful response. » **National:** The Cybersecurity and Infrastructure Security Agency (CISA)[2], Department of Homeland Security (DHS)[3], the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)[4], the Federal Bureau of Investigation (FBI)[5], the National Association of State Election Directors (NASED)[6], the National Association of Secretaries of State (NASS), and the U.S. Election Assistance Commission (EAC)[7].
Step 6:	**Decide what baseline information you can communicate ahead of the election.** • Establish a baseline understanding among potential core members of your team and key stakeholders to implement best practices for mis/ disinformation response ahead of the next election. • Share elements of how you may reach out as incidents occur. You may choose to share elements of your baseline planning in 'Knowing Your Threats,' incident review, information about current incidents, or public briefings on disinformation trends by CISA or others.
Step 7:	**Select one or more spokespersons.** • Establish ahead of time who will speak for your jurisdiction in a mis/disinformation incident, and make sure that they have received media training. • You may choose different spokespeople for different audiences: the Chief Election Official, Communications Director or other leadership. Consider factors such as who has the best communication skills, prior experience with the media, authority in the agency, and relationships with stakeholders.
Step 8:	**Establish a drafting and approval process for your team. Include approval steps of this process in your communications response plan.** • This process will be specific to your jurisdiction's incident response team structure, and you can build from the general process outlined in the following box.

Templates for your planning are available in this guide's toolkit, **pg. 40.**

2 https://www.cisa.gov/election-security

3 https://www.dhs.gov/topic/election-security

4 https://www.cisecurity.org/ei-isac/

5 https://www.fbi.gov/investigate/counterintelligence/foreign-influence/protected-voices

6 https://www.nased.org/

7 https://www.nass.org/

Pro Tip: However you choose to coordinate the process of approval, make sure that it is streamlined so that there is one person who is responsible for approving everything that goes out externally. Any communications process should work in tandem with operations. The ultimate message approver should also be signing off on the operations response. This ensures that the message leaving your office is consistent, which is imperative in avoiding a misstep and maintaining trust.

Example: ***Message Drafting and Approval Process***

Identify Incident Communication Need	• Your team communications lead identifies the need for a communications responIse. This research helps assess how the incident is affecting your audience/stakeholders and can be done as needed by monitoring social media, press inquiries, and stakeholder communications. • Your team lead will outline the needs a message should address, audiences it needs to get to, materials that should be generated and the timeline.
Consult with final decision-maker and other internal players	• Your communications team lead will consult with the final decision-maker, likely the jurisdiction's chief election official, on overall communications strategy, plan and messaging. • Consultation may depend on the incident severity (may not be needed). • Consult, as needed, with social media lead and other subject-area experts related to the disinformation involved.
Develop Materials	• Your communications team lead will guide the drafting process of materials. [Add steps from the Stage 3 "Communicate" section]. » *First:* Incident key messages. Identify the audience and develop the message and materials. » *Second:* Any questions/issues raised for further discussion. » *Third:* Develop other needed materials. • The communications team consults any stakeholders or experts as needed for input or to provide approval. • Share drafted materials with legal.
Legal Review	• Legal reviews language and shares feedback with communications lead. • Communications lead updates and finalizes materials.
Final Review	• Ultimate decision-maker reviews the materials and approves the messaging to be shared.

Accompanying templates for customizing your jurisdiction's response plan is included in this playbook's toolkit, **pg. 40.**

Update and Secure Your Communication Channels

Your website and social media presence is a critical source of information for voters. It is how many voters will interact with your office and how they will seek authoritative information from you. Depending on your local circumstances, more traditional communications channels such as radio, TV, and print media may remain an important way to reach voters.

The following suggestions focus on your digital information tools, but in preparing these tools and in mapping your stakeholders in Step 3, you will also create relationships for information sharing that extend beyond the digital realm.

Website

Your website should be secured, and it is therefore recommended that you use a .gov domain. One of the most common disinformation tactics is to create fake election jurisdiction website to confuse voters. Malicious actors are unable to purchase or re-create .gov domains, making them a more authoritative source of information. You can find more information about registering for a .gov domain at the DotGov website.[8]

Ensure that your website is fully up to date with relevant information and, where necessary, provide links to other authoritative sources. The Center for Tech and Civic Life (CTCL) offers an election website template and course, Building an Election Website[9], as well as a course on "Improving Your Election Website".[10]

The courses offer guidance for transitioning your current url to a .gov url.[11] The free materials associated with the course discuss paperwork, costs and other considerations to implement this important change. The U.S. General Services Administration can also serve as a resource.[12] A .gov domain can take some time to be approved. Timelines can vary 2-4 weeks

8 DotGov, "Recent Updates": https://home.dotgov.gov/

9 Center for Tech and Civic Life, "Building an Election Website: https://www.techandciviclife.org/course/building-an-election-website/

10 Center for Tech and Civic Life, May 2020, "Improving your Election Website": https://www.techandciviclife.org/wp-content/uploads/2020/03/CTEI-Improving-Your-Election-Website-Participant-Guide.pdf. Video presentation: https://vimeo.com/416151915

11 ibid. page 27, video 42:40 minute mark.

12 U.S. General Services Administration, "DotGov Domain Services": https://www.gsa.gov/policy-regulations/policy/information-integrity-and-access/dotgov-domain-services

or longer depending on the jurisdiction. It may not be possible to get a new .gov website established before the 2020 election. Nevertheless, we recommend you start the process, as it will be valuable in the long-term. Plan on leaving sufficient time to transition your domain. We recommend transitioning your domain all at once.

Your website should include information about:

- How a voter finds their polling place.
- How to vote.
- What requirements there are to vote on election day.
- When voters can vote.
- How voters should ask questions or report concerning information or other problems (e.g. a phone number to call if a voter is turned away from their polling place for any reason).
- The measures you have taken to ensure that elections will run smoothly.
- When results are likely to be announced.
- Other jurisdiction-specific high importance information identified in scenario planning.

Internet Platforms and Social Media Channels

There are a range of internet platforms which election officials should be aware of (see Part 1, Appendix 1 of this Playbook). The most widely used of these, and therefore the most important to ensure that your jurisdiction is represented are: Facebook, Twitter, Google and YouTube. The below guidelines should be applied to any other social media channel/internet platform that your jurisdiction uses.

Your presence on each of these platforms/channels should be kept up to date with the latest, clearly stated information about the upcoming deadlines and elections. Even if you do not plan to run any social media content, creating accounts and verifying them across social media platforms will allow you to easily report incidents of mis/disinformation if needed.

Each social media company has its own process to verify your office or your personal account are valid. Even if you do not communicate via social media, having verified accounts on different platforms makes it more difficult for malicious actors to pretend to be you.

Facebook	Facebook offers two security tools that election officials should take advantage of: Blue Badge Accounts[13] and Facebook Protect[14]. These prove your identity on the platform and strengthen the authenticity of the messages you push out. • **Blue Badge Accounts:** When Facebook has confirmed that an account is the authentic presence of the public figure, celebrity, or global brand it represents, it awards it a Blue Badge as a sign of verification. As an official, you can request a Blue Badge Account by reaching out to your regional Facebook representative (see Toolkit, pg. 45). • **Facebook Protect:** Once you enroll as a Blue Badge account, you should also enroll in Facebook Protect. By enrolling in Facebook protect, you will gain stronger account security protections like two-factor authentication and inclusion in Page Publishing Authorization[15], which helps public sector pages establish their legitimacy as trusted accounts. It also monitors your account for potential hacking threats. In August 2020, Facebook launched a Voting Information Center.[16] Among the new tools the center provides, officials are able to send out "voting alerts" to share important updates on voting. • **Become Voting Alert Eligible:** To be eligible to use voting alerts, there are specific guidelines[17] a jurisdiction's page should meet, such as being an "office" page, not associated with an individual official. Your page does not need to be Blue Badge verified to have voting alert access. As of August 2020, state officials have access to the voting alert feature. A form to request eligibility will be available through Facebook's Help Center pages associated with voting alerts. Voting alerts[18] can help you share correct information ahead of and throughout the election. Additionally, Facebook has created a page with tools and information[19] for public officials. Bookmark it in your web browser so that you can reference it throughout the election cycle.
Twitter	Twitter provides a blue checkmark by some account names to show that the account is a credible/vetted voice on Twitter. You can email gov@twitter.com to seek verification as an election official on an account designated for official and non-personal use. Getting verified may take some time.[20] At minimum, knowing which accounts may be verified in your state can help support your response on this platform by sharing your messages acting as a validator to voters.

13 Facebook, "How do I request a Verified Badge on Facebook?": https://www.facebook.com/help/1288173394636262

14 Facebook, "Facebook Protect": https://www.facebook.com/gpa/facebook-protect

15 Facebook, "Get Authorized to Manage Pages with Large Audiences": https://www.facebook.com/business/m/one-sheeters/page-publishing-authorization

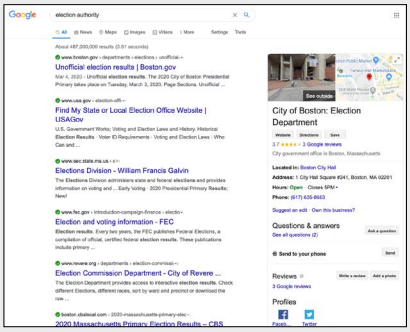
16 Facebook, "Launching Our US 2020 Voting Information Center": https://about.fb.com/news/2020/08/launching-voting-information-center/

17 Facebook, "Voting Alert Guidelines": https://www.facebook.com/business/help/626587208260920?id=1549080658590154

18 Facebook, " Use Local and Voting Alerts": https://www.facebook.com/business/help/572490746512593?id=1549080658590154

19 Facebook, "Facebook for government, politics and advocacy": https://www.facebook.com/gpa

20 Twitter, "About verified accounts": https://help.twitter.com/en/managing-your-account/about-twitter-verified-accounts

Google	Google provides many companies and official agencies with its email and Google Suite services, in addition to its popular search service. Ahead of the elections, Google suggests that officials take three steps to secure their accounts and Google search presence: • Add **two factor authentication** on your Google accounts, and monitor the security of your account via Google's Security Checkup.[21] Doing this will protect google products related to the account after signing in (Gmail, calendar, Google drive etc.) Even if you use a Google email account through Microsoft Outlook or another email provider, you can and should turn on two factor authentication. • State and Local Chief Election Officials, and others facing heightened security risks can enroll in the Google Advanced Protection Program.[22] This will provide additional screening to your account, and physical verification using a key fob or similar. • Verify your local election authority's business profile[23] with Google. This is to ensure that any information displayed in Knowledge Panels (short summaries on the right hand side of search results) is correct. (Example on right) **Plan ahead:** enrolling in these measures can take some time, with timelines currently extended due to the COVID-19. 
Youtube	If your jurisdiction runs a YouTube account,YouTube has published blog posts on securing[24] and verifying[25] your account. YouTube's securing features can be applied to all accounts.

Traditional Media and Community Outreach

You will also want to make sure you have established relationships with traditional media, including radio, TV, print media, local media, community message boards, information sent by mail, or community gatherings. These entities or individuals may also become part of your list of trusted validators you want to engage in responding to a mis/disinformation incident depending on its severity.

Some examples of outreach include:

- Allowing community groups or schools to use voting equipment for local contests.

21 Google, "Security Checkup": https://g.co/securitycheckup

22 Google, "Advanced Protection Program": https://landing.google.com/advancedprotection/

23 Google, "My Business": https://www.google.com/business/

24 YouTube, "Three steps to keep your YouTube account secure": https://youtube-creators.googleblog.com/2020/05/three-steps-youtube-account-secure.html

25 Google, "Verification badges on channels": https://support.google.com/youtube/answer/3046484?hl=en

- Pairing public education with civil society or political parties' voter registration efforts.
- Sharing the Cyber and Infrastructure Security Agency's (CISA) public briefings on mis/disinformation trends with community groups and press.
- Creating an engagement role or team within your office to help further public education efforts and public briefing information by direct community engagement.
- Proactively sharing your election preparation processes with the press ahead of the election.

It can be important to engage key media directly. The more reporters understand what your jurisdiction has in place, the more they can help inform voters. Media may also report incidents to you.

Publicize Your Online Channels

You should publicize your website URL, social media handles and any other locally important communications channels regularly so they are well known to your voters. Reach out in the months and weeks ahead of Election Day to voters via community groups, key journalists, local news media, election jurisdictions, local authorities, and influential social media figures or local public figures to ensure they know your channels and can publicize them if necessary. Ensure that other election authorities, e.g. your state election office, are aware of your channels and you theirs. Follow each other and help broaden your reach by liking and sharing each others' content. Make sure that all websites and accounts that you are liking or sharing are legitimate.

Even if you are not usually posting information on your jurisdiction's social media channels, in the event you need to share correct information widely, these other trusted voices can act as validators and help share correct information. At a minimum, create a list and try to reach out via social media or other channels (phone, email, in person) to your own list of community voices.

Know Your Threats

To effectively prepare for and defend against mis/disinformation incidents, officials need to be aware of the specific risks that face their jurisdiction. This will enable you to tailor your preparations to ensure that your key vulnerabilities are protected.

To establish what your major risks may be, officials can:

- **Conduct an incident review** by studying past examples of mis/disinformation affecting your jurisdiction or surrounding jurisdictions. Look at lessons learned, solutions implemented and what worked well and less well. Analyze and discuss real examples, trends or communications gaps in your jurisdiction that might be exploited in a disinformation attack.
- **Conduct stakeholder mapping and a reputational risk analysis** to understand your priority stakeholders, and how to reach them to address key concerns.
- **Conduct crisis simulation and table-top exercises,** coordinated with legal, technical, and outside advisors, including key senior leaders across jurisdictions. This exercise can be as simple as a conference call or walk through.
- **Map your potential vulnerabilities** using the "Top Targets of Election Interference"[26] framework:

You can map these potential vulnerabilities by answering the "5 Questions of the Election Process " for your jurisdiction.

Who? *The people who make elections run.*

What? *The machines, systems and ways that we vote.*

When? *The day(s), time, places and deadlines that help us come together to vote.*

Where? *Where we show up to exercise democracy.*

How? *How voting happens.*

26 For more, see The Elections Influence Operations Playbook, Part 1.

Mis/disinformation incidents tend to affect voters' understanding of the answers on one or more of these 5 questions. Consider which answers to these questions may be least well understood by voters in your jurisdiction, or where there are avenues for mis/disinformation to create confusion. Your work here will significantly inform the indicators you develop to assist you in monitoring in real time (see 'Identify and Assess' section).

A template for generating keywords and identifying potential top targets can be found in the toolkit. See: *Top Targets of Election IO: "5 Questions of the Election Process" Keywords*, **pg. 41.**

Stage 2: Identify & Assess

This section recommends ways that you can proactively identify ongoing mis/disinformation incidents, enabling officials to respond to them before they gain traction. The following are suggestions for identifying and assessing potential mis/disinformation.

Develop Indicators and Warning Signs

Keywords

In the lead up to key election events, use your incident review from 'Know the Threats' (p...) to determine your main mis/disinformation vulnerabilities. For each of these, write down:

- Individuals and institutions that may publicly comment on issues relevant to these vulnerabilities. Find their social media handles and pages, websites and any other major communications channels (e.g. radio shows).
- Keywords that are likely to be used when people talk about issues relevant to your vulnerabilities. On many social media platforms these keywords can be preceded by a # ('hashtag'), which functions as a label that groups content. You can search your answers to the "5 Questions" of the election process, used in your mapping to search hashtag keywords to see who and how these are being discussed online.

This information will become your indicators and warning signs. There is no wrong list, even a small list of a few key words will help you check in on conversations unfolding online for these top potential targets of mis/disinformation during elections.

Look for posts that:

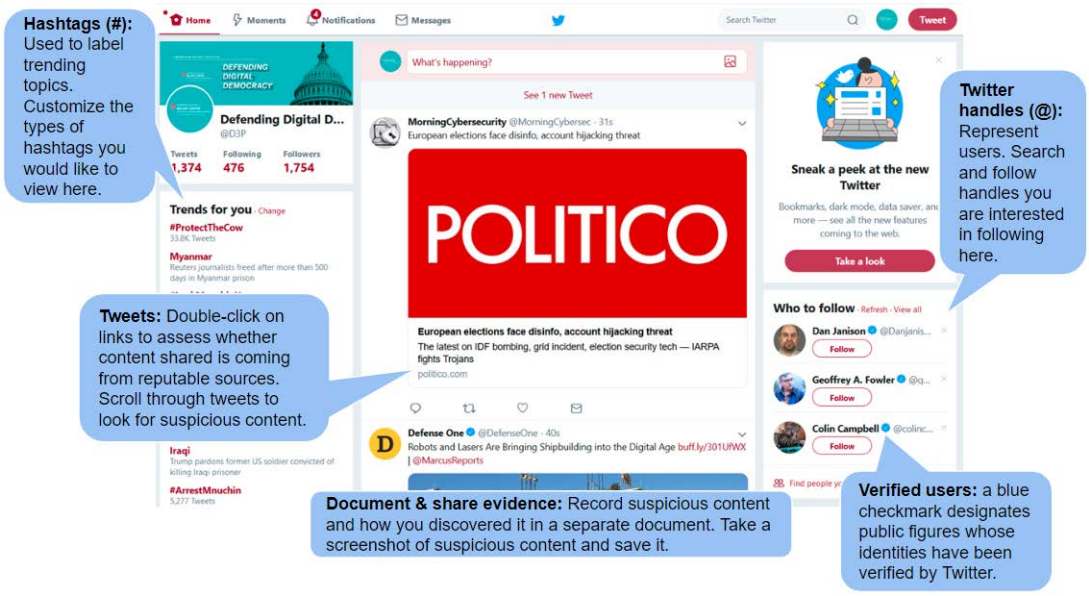
Who? *Impersonate or disparage the people that run elections.*

What? *Spread allegations of disrupted election hardware or software.*

When? *Misrepresent when voting, registration, or other events occur.*

Where? *Report false locations for voting, registration, or other events.*

How? *Misrepresent how voting or registration occurs (e.g. by Twitter, Mail-in Ballots)*

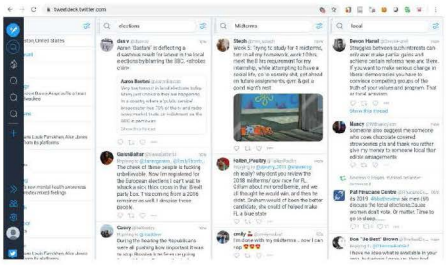
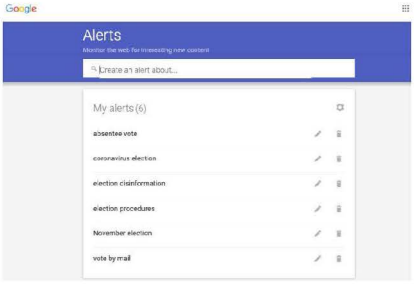
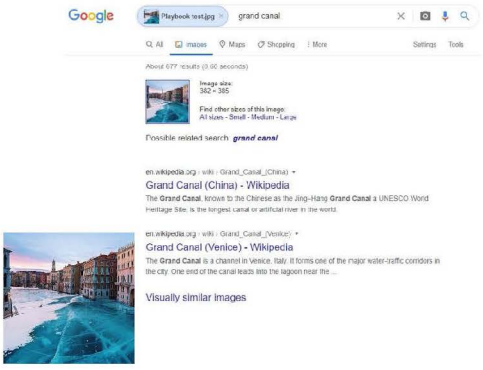


Twitter Example: As an example, by searching hashtags (#) in Twitter, even simple keywords based on answers to the "5 Questions" for your jurisdiction, you can see what type of discussion is unfolding online.

A *Top Targets of Election IO: "5 Questions of the Election Process" Keywords* template to help your keyword and indicator planning can be found in the Toolkit, **pg. 41.**

Monitor in Real Time

By performing regular searches using your keyword indicators, you can develop a running list of hashtags and accounts that generate suspicious content. Review these hashtags, accounts, and trends in real time. Look for misleading posts on topics you can verify about the "5 Questions." The following are potential free tools that can help you monitor.

TweetDeck: You can use a social media aggregator platforms like TweetDeck, a free Twitter tool, which enables users to monitor a large number of hashtags and Twitter accounts of interest on one screen.	 *Example Screenshot of TweetDeck with keyword search terms.*
Google Alerts: For monitoring traditional media, a useful free tool is Google Alerts. Use your indicators and warning signs to create tailored news digests that are sent directly to your email inbox at a frequency that you select.	 *A screenshot of example election related keywords you can receive news alerts regarding.*
Image Source Search: Mis/Disinformation can include images or videos that pretend to illustrate a particular event. Sometimes visuals from unrelated events can be shared, or even altered to make it appear that something happened that did not. If you identify potential mis/disinformation includes visual content like a picture, it is often worth trying to investigate whether an image is real. A useful tool is Google's Image Search. This allows you to upload an image to Google and obtain search results of where that image and similar ones appear online. If the image in question appears online in an unrelated context, it is highly possible that it is not real. Since June 2020 Google has been adding 'fact check' labels directly to some images in search results. These labels can be clicked for immediate fact check information.	 *A fake image of frozen canals in Venice, Italy. It is an image of Venice superimposed on one from Russia.*

TweetDeck[27], Google Alerts[28], Google's Image Search.[29]

27 Twitter, "TweetDeck": https://tweetdeck.twitter.com/

28 Google, "Alerts": https://www.google.com/alerts

29 Google, "Google Images": https://images.google.com/

Document Evidence

It is important that organizations have ways to capture and log suspected mis/disinformation, especially if you're monitoring proactively. You may be able to stop these incidents from gaining momentum and spreading. The same "5 Questions of the Election Process," can also be a helpful shorthand for what details to document in tracking evidence for potential reporting.

"5 Questions of Reporting"

- **Who:** Document the account names, pages, and hashtags that are spreading mis/disinformation.
- **What:** Take screenshots of false posts and document their URLs links to them if possible.
- **When:** Record the dates and times that false posts appeared.
- **Where:** Many mis/disinformation events occur on multiple platforms at once. Document which platforms have been affected.
- **How:** Document how the mis/disinformation event is impacting elections, or risks impacting them. Here you could also add ***Why*** you believe the incident may violate the platform's policies. In the toolkit we include insights on each platform's removal policies (pg. 44).

Documenting evidence will enable you to report the mis/disinformation in a clear, concise way. This makes it easier for social media companies and other bodies to take action to deal with cases of mis/disinformation.

More in the Toolkit:

pg. 40: 'Sample Incident Reporting Email [Template]' includes a sample reporting format for reporting a mis/disinformation incident based on the evidence you've documented.

pg. 44: Reporting 'Mis/Disinformation to the Social Media Platforms- Detailed Reporting Steps' shares insights on each mainstream platform's removal policies.

Assess Incident Severity

You may become aware of a mis/disinformation incident through your monitoring in real time or through reports of the incident to your office. Once mis/disinformation has been identified, you should conduct an initial analysis of the severity of the incident. This analysis will help you determine how to move forward with a communications response and a reporting response. Three key considerations will assist in this assessment:

- **Established voice:** who is it who is sharing the mis/disinformation? If it is a well known figure or institution, the information is likely to be perceived as more credible by the public and to gain more traction.
- **Credibility:** Are voters likely to believe the information that is being shared? Things that may not be believable to experienced election officials may be perceived as credible by the public.
- **Volume:** how prominent is the mis/disinformation? Are a lot of people engaging with it? Assess the momentum of the incident and how the message is gaining traction. Either online or through contacts to your office.

Answers to these questions will help determine the initial level of response. Note that an incident can increase or decrease in severity as an incident continues to gain traction.

It is imperative that you use your local understanding based on situational factors, like realities about your community, and the sources involved in spreading the mis/disinformation. This will assist you in making decisions about what the appropriate scale and next steps for escalation are in a given incident. Bear in mind that it is easier to scale back an initial over reaction than it is to catch up after you have initially under-responded.

When to Activate the Incident Response Team (IRT)

High	**Urgent activation of the Incident Response Team is necessary.** • Mis/disinformation is circulating in the public, on social media, or in local media **that threatens to significantly undermine elections and/or voter confidence in the integrity, process, and outcome of elections**. • The misleading information is prompting voter questions to your office, is changing voting behavior, and has or will undoubtedly result in inquiries from local/state leaders, political parties, and voter advocacy groups.
Medium	**Activation of the Incident Response Team is necessary.** • Mis/disinformation is circulating in the public, on social media, or in local media **that has the potential to negatively affect voter confidence in elections or hinder voter turnout**. • The misleading information will likely spur voter questions to your office, could change voter behavior, and may prompt inquiries both from local/state leaders, political parties, and voter advocacy groups. » If a medium severity incident gains a lot of traction, but is not necessarily severe in nature, it may escalate to a high severity incident because of a growing audience.
Low	**Activation of the Incident Response Team is not necessary, unless the situation graduates to a medium severity incident. Reporting the incident may alone be sufficient.** • A misleading piece of information **that does not receive significant coverage, is widely seen as implausible, and poses a limited threat to voter confidence**. At this stage, intervention is unnecessary because drawing attention to the information risks giving it more oxygen than it otherwise might receive. • Continue to monitor the situation: If additional actors start to share the misleading coverage, the severity of the incident may rise.

Stage 3: Respond & Resolve

Responding to and resolving a mis/disinformation incident requires two simultaneous and coordinated actions:

Report	Communicate
Reporting content is important to report for potential removal and for authorities tracking IO beyond the incident you are encountering. Reporting may or may not slow the spread of mis/disinformation incidents.	Responding quickly, authoritatively and accurately to mis/disinformation is vital to counter it.

Reporting to the platforms, trying to minimize an incident's viral traction, can become important. But, it can not be your only response. You must also be prepared to respond and correct the record. Regardless of a reporting result, what you can control is your communication response to reach voters. **Reporting to others in your state and to authorities** helps identify larger scale mis/disinformation incidents and may give you more voices and coordinating capacity with which to counter an incident. However, the effect of these incidents may spread more quickly than authorities or platforms are able to act. Your action and your voice, are the frontline of countering mis/disinformation.

Report

Once you have identified inaccurate content, in conjunction with your communications response, report mis/disinformation. Following these steps, in conjunction with existing response plans, can help election officials initiate a process to request removal and/or investigate false content.

Reporting Mis/Disinformation

Reporting mis/disinformation can be a challenge, but it is a critically important part of ensuring the safety, security, and integrity of our elections.

What to Report:

As discussed in the 'Document Evidence' section, when reporting mis/disinformation, it is critical to include key details and content. The "5 Questions of Reporting" can help as a reminder of what to detail. That means including links, screenshots, and account names in your reports, and being as specific as possible about the issue you are reporting.

'Sample Incident Reporting Email [Template]' in the toolkit, **pg. 40.**

Who to Report to:

For reporting to be effective, you must report to three groups:

1. **State election official's office**
   In some cases, your chief election official may have access to tech platform reporting tools local jurisdictions do not yet have access to. They may also have more access to identify trends and can be partners in your response and reporting efforts.

2. **Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)**
   The EI-ISAC, a part of the Center for Internet Security (CIS), is able to route reports through a network of collaborators including CISA, the FBI, and other federal authorities. Through these collaborators your report is also routed to the social media platforms. This facilitated routing of information can distribute your report to decision-makers that can help assess your incident. Importantly, EI-ISAC is able to take reports from members and non-members. Traditionally, EI-ISAC has received many reports through its Security Operations Center (SOC) during Election Day. However, they are able to receive and distribute reports year-round, 24/7. Through EI-ISAC's routing to collaborators nationally, the analysis of an incident may determine a broader pattern than what you may encounter. Collaborators that can also flag your incident beyond your direct reporting to platforms can be helpful.

3. **Social Media Platforms**
   Our Toolkit includes a special section that details what you need to know to report to each major platform (Facebook, Google, Twitter and YouTube) and shares specific reporting guidance. You can also share your platform record reporting number in your report exchange with EI-ISAC.

Looking Ahead: As more progress continues to address the difficulty in reporting mis/disinformation incidents, seek updates from your professional election membership association or the EI-ISAC. Ahead of November 2020, efforts underway continue to help make reporting easier for officials and engage advocates on their behalf in the reporting process. Working in coordination, EI-ISAC, CIS, CISA, the Election Integrity Partnership (EIP) and others aim to help streamline reporting and get reports to the best sources for addressing them.

Our recommendation, especially if you are short on time or don't have access to some of the social media platform tools, is to send the same content in an email or portal reporting form to the following collaborators:

PRIORITY	WHO TO REPORT TO		CONTACT
1	**Chief Election Officials** and **State Election Organizations**		**Varies by state** *Include Contacts in your Stakeholder Map.*
2	**Authorities:** • EI-ISAC *Optional:* • DHS/CISA • FBI		SOC@cisecurity.org NCCICCustomerService@hq.dhs.gov cywatch@fbi.gov or your local field office.
3	**Platforms***	Facebook	reports@content.facebook.com *See Toolkit to cc your regional contact as well.*
		Twitter	If you've been enrolled in the Partner Support Portal, report at PSPOnboarding@twitter.com. If you're not enrolled, report by Twitter's form: help.twitter.com/forms and coordinate with your state or national contacts to flag your report.
		Google & YouTube	Report by Google product: https://support.google.com/legal/troubleshooter/1114905 civics-outreach@google.com For questions on reporting tools: civics-outreach@google.com
Please see detailed reporting steps in the Toolkit. For some reporting avenues, local officials may have to coordinate with state officials for reporting access.			
MONITOR THE SITUATION.			
4	**IF YOU NEED ADDITIONAL SUPPORT:** State Officials can seek support from National Membership Associations. In addition to these organizations, federal partners like CISA are in touch with representatives at the major platforms and may be able to provide further advocacy in resolving an incident. Coordinate with the stakeholders you've established relationships with to seek further support in the reporting process.		

For more information around reporting to specific social media platforms see **pg. 44.**
A template stakeholder map is available at **pg. 40.**

Communicate

If a mis/disinformation incident begins to take hold and you have assessed its severity is sufficient to activate the Incident Response Team, the top priority is to maintain the public trust that you have built over time through your regular public outreach. The most effective way to achieve that goal is to respond accurately, confidently and quickly. Be mindful, though, that in some cases a response from you may make an otherwise low profile incident become something bigger, by providing it with additional oxygen.

Communications Process for a Mis/Disinformation Incident

The steps below will help you take basic actions while you develop a more detailed communications plan. Each situation must be fully assessed on its own merits before a particular strategy is executed. The following are general guidelines:

Step 1:	• Once you are aware of an incident and assess its severity, decide what to do, communicate or leave it alone and monitor it. • If you decide you need to communicate about it, activate the Incident Response Team and obtain a briefing from the Communications Team on the status of the incident on media and social media. • Establish ground truth facts as much as possible. Assess who the key stakeholders are in this incident.
Step 2:	• Decide if you should respond and if so, what to say. » Which bucket of mis/disinformation does this fall into? » Build on the scenario pre-work. » Adapt the starting point for the facts on the ground. • Draft message and have the designated reviewers review. • Finalize message.

Step 3:	• Notify key people, internal and external. • Decide on the most trusted information channels and validators to convey the message you want to put out to counter the mis/disinformation incident. • Each incident may require the involvement of different stakeholders. • Provide messaging to them and guidance on what to do. • Stakeholders you engage could be national or federal collaborators, local advocate groups, campaigns, political parties or community leaders. • Your stakeholder mapping can help inform who you involve depending on the situation.
Step 4:	• Consider how you need to inform the media/public about the incident. • Make sure you inform the media only of confirmed facts that you are confident will not change (very few facts will fall into this category). • Consider distributing your counter-message to all interested stakeholders and encouraging them to share the correct information on their social media, websites, or other distribution channels.
Step 5:	• Continue monitoring media coverage, social media and establish a feedback loop for how your statements are being picked up and responded to.
Step 6:	• Develop a medium-term message, if necessary, and recalibrate your message in response to information picked up via your feedback loop.
Step 7:	• Prepare for continued press outreach/briefing and media schedule.

Additional communications response materials are available to elections officials on request in ***Part 3: Mis/Disinformation Scenario Plans*** from the D3P Team at the Belfer Center: email connect@d3p.org.

Incident Severity Escalation Table

Building on your assessment of the severity level of a mis/disinformation incident, once you have activated the incident response team, this table aims to suggest key actions you can take and materials you can consider creating in response to high, medium and low severity incidents.

HIGH SEVERITY: Incident threatens to significantly undermine voter confidence in the integrity, process, and outcome of elections.

Urgent activation of the Incident Response Team is necessary.

- *Mis/disinformation is circulating in the public, on social media, or in local media* ***that threatens to significantly undermine elections and/or voter confidence in the integrity, process, and outcome of elections.***
- *The misleading information is prompting voter questions to your office, is changing voting behavior, and has or will undoubtedly result in inquiries from local/state leaders, political parties, and voter advocacy groups.*

Key Considerations / Actions	Potential Key Materials Checklist
• Activate Response Team. Identify mis/disinformation narrative and establish ground-truth. • Prioritize stakeholders for outreach. • Develop a fact-based statement. If further investigation is required, deploy a holding statement. • Determine if broader public communication is appropriate. • Alert authorities and social media companies [See pages 40, 44]. • Brief senior state officials. • Develop clear, straightforward graphics, images, videos or charts to provide correct information in a way that is visually appealing and easily digestible for your voters. • Contact legislators, policy makers, or stakeholders as needed. • Reach out to third-party validators to vouch for election processes with the media. • Issue follow-up statement once you have established the facts (*if necessary*). • Continue media and digital media monitoring and feedback loop. • If applicable, consult law enforcement.	• (*Preferred*) Fact-based statement deployed multichannel (state/local election website, social media, traditional media, shared with stakeholder groups). • *(If necessary)* Holding statement to allow for more investigation. • Key talking points taken from the statement. • Peer communication/email. • Email to social media contacts (*if applicable*). • Voter communications. • Poll worker communications (*if applicable*). • Website / social media materials. • Visual infographics, charts, images, and videos as applicable. • Media materials. • Legislator / policy maker materials. • Political party / community leader / third-party validator materials or talking points (*derived from key messages*). • State election [broader] employee communications / email. • State Elections official talking points (*derived from key messages*). • Local County Elections official talking points (*derived from key messages*). • Briefing materials for law enforcement. • Follow up materials for media briefings.

MEDIUM SEVERITY: Incident has the potential to negatively affect voter confidence in elections.

Activation of the Incident Response Team is necessary.

- *Mis/disinformation is circulating in the public, on social media, or in local media* ***that has the potential to negatively affect voter confidence in elections or hinder voter turnout.***
- *The misleading information will likely spur voter questions to your office, could change voter behavior, and may prompt inquiries both from local/state leaders, political parties, and voter advocacy groups.*
  - » *If a medium severity incident gains a lot of traction, but is not necessarily severe in nature, it may escalate to a high severity incident because of a growing audience.*

Key Considerations / Actions	Potential Key Materials Checklist
• Activate Response Team. Identify mis/disinformation narrative and establish ground-truth. • Prioritize stakeholders for outreach. • Develop a fact-based statement. If further investigation is required, deploy a holding statement. • Determine if broader public communication is appropriate. • Alert authorities and social media companies [See pages 40, 44]. • If necessary, develop clear, straightforward graphics, images, videos, or charts to communicate correct information in a way that is visually appealing and easily digestible. • Issue follow-up statement once facts established (if necessary). • Continue media and digital media monitoring and feedback loop.	• *(Preferred)* Fact-based statement, deployed multichannel (state/local election website, social media, traditional media, shared with stakeholder groups). • *(If necessary)* Holding statement to allow for more investigation. • Peer communication / email. • Email to social media contacts (if applicable). • Poll worker communications (if applicable). • State election [broader] employee communications / email. • Website / social media materials. • Visual infographics, charts, images, and videos as applicable. • Legislator / policy maker materials. • Political party / community leader / third-party validator materials or talking points (derived from key messages).

LOW SEVERITY: Incident is not receiving significant coverage, is widely seen as implausible, and poses a limited threat to voter confidence.

At this stage, intervention is unnecessary because drawing attention to the information risks giving it more oxygen than it otherwise might receive.

Activation of the Incident Response Team is not necessary. It becomes necessary if the situation graduates to a medium severity incident. Reporting the incident may alone be sufficient.

- *A misleading piece of information* ***that does not receive significant coverage, is widely seen as implausible, and poses a limited threat to voter confidence.*** *At this stage, intervention is unnecessary because drawing attention to the information risks giving it more oxygen than it otherwise might receive.*
- *Continue to monitor the situation: If additional actors start to share the misleading coverage, the severity of the incident may rise.*

Key Considerations / Actions	Potential Key Materials Checklist
• Increase your dissemination of correct information in the places your voters consume news, like Twitter, Facebook or other local channels. • Prioritize traditional and digital media monitoring to continue to assess if the incident remains low severity. • Communications to peer organizations warning of the misleading information, especially if the issue is multi-jurisdictional. • Alert authorities and social media companies.	• Peer communication / email, if needed. • Email to authorities and social media contacts (if applicable). • Prepare contingency communications to be used if mis/disinformation escalates to medium severity.

Stage 4: Learn & Improve

Improving Through Experience

It is vital to conduct some type of lessons learned exercise post-incident. Key considerations include:

- **Stage 1 (Anticipate & Prepare):** Update your incident review and scenario planning to include the situations you faced in the current election cycle. Where did unexpected issues emerge, and how can you prepare for them next time?
- **Stage 2 (Identify & Assess):** Refresh you key indicators used for monitoring for mis/disinformation incidents. If your monitoring strategies did not allow you to see emerging mis/disinformation incidents, consider adjusting your tactics and tools.
- **Stage 3 (Respond & Resolve):** Identify where your response process was effective and where it faced difficulties. Put in place steps to ensure that strong points can be repeated and difficulties overcome.

Conclusion

As you head into another election cycle, especially one that is posing unique and evolving challenges, we hope that this Playbook Response Plan and Template provides a running start for officials who are seeking to counter mis/disinformation incidents. We hope the guidance and format of this template helps officials prepare for, and manage, the emerging and evolving mis/disinformation risks to our elections process. As with all communications plans, we recommend that you regularly update your plan to account for changes in agency structures and personnel and customize for your state and jurisdiction.

Your voice matters, your public service makes you a trusted community leader and your trusted voice combined with other trusted voices in your community will be the most effective counter to the divisive and confusing nature of these incidents which can undermine our elections.

Please visit our website to learn more and to access resources like these Playbooks online.

Playbook Part 3 | Mis/Disinformation Scenario Plans: A further supplementary guide is available on request from D3P at the Belfer Center by contacting connect@d3p.org This guide is exclusively for officials and includes resources you can use in preparing your own response plan.

We hope these resources support you as you serve voters across the country.

The Election Influence Operations Playbook
Toolkit

To add further details to each of these phases and provide additional resources for your planning this guide includes a toolkit with important information and templates for each phase of countering IO.

- The Four Stages of Countering Election Influence Operations **Master Checklist**
- **Stage 1: Anticpate & Perepare**
  - » Incident Response Team [Template]
- **Stage 2: Identify & Assess**
  - » "5 Questions of the Election Process" Election IO Identification Keywords [Template]
- **Stage 3: Respond & Resolve**
  - » Reporting Mis/Disinformation to the Social Media Platforms-***Detailed Reporting Steps***
  - » Sample Incident Reporting Email [Template]
  - » Best Practices for Responding to Mis/Disinformation

The Four Stages of Countering Election Influence Operations

Master Checklist

This checklist provides a summary of this Part 2 Mis/Disinformation Response Plan to help officials develop their own plan.

Stage 1: Anticpate & Prepare

Build Your Team and Plan Your Communication Response

Establish your Incident Response Team (pg. 5):

- ☐ Set out key contact information, roles and responsibilities for the Incident Response Team. This includes:
  - ☐ Name
  - ☐ Contact information (phone, email)
  - ☐ Backup contact information
  - ☐ Contact information of the backup individual responsible in the event that the primary person is unavailable
  - ☐ Set responsibilities of the person (e.g. media spokesperson or social media director)
  - ☐ Establish communications bridge line for IRT to connect in an incident.

Incident Response Team [Template]: pg. 40.

Communications Coordination (pg. 6):

- ☐ Decide on your team.
- ☐ Notify the Incident Response Team members of their responsibilities in writing.
- ☐ Coordinate an internal communication plan with elections staff.
- ☐ Set backup communications method if primary means fails.
- ☐ Complete self assessment, building on preparatory work in the 'Know the Threats' section.
- ☐ Conduct scenario planning with Part 3 Mis/Disinformation Scenario Plans.

- ☐ Conduct stakeholder analysis, building on work in the 'Know the Threats' section.
  - ☐ Ensure you have a relationship with each stakeholder ahead of election day.
- ☐ Establish process for response support and alignment with local and national-level bodies.
- ☐ Appoint team members responsible for social media monitoring and reporting mis/disinformation.
- ☐ Select spokesperson/s.
- ☐ Establish an approval process for developing and disseminating external messages.
- ☐ Decide what baseline information you can communicate ahead of the election with members of your team.
- ☐ Update this plan regularly.

Update and Secure Your Communication Channels

Website

- ☐ Claim a .gov url for your website
- ☐ Update website content pages:
  - ☐ How a voter knows where to vote.
  - ☐ How to vote.
  - ☐ What requirements voters must meet to be eligible to vote on Election Day.
  - ☐ When voters can vote.
  - ☐ What happens when things go wrong (e.g. a phone number to call if a voter is turned away from their polling place for any reason).
  - ☐ The measures you have taken to ensure that elections will run smoothly.
  - ☐ How voters can ask questions or report concerning information.
- ☐ Determine who has access to edit your website, and ensure that all users only have the permissions required for their specific roles.
- ☐ Implement two-factor authentication on your website for all webmasters and IT administrators.
- ☐ Work with your IT team to stress-test web server load and ensure that your website can handle traffic exceeding "worst-case" peak scenarios.
- ☐ Consider utilizing a DDoS protection service for your most critical websites.

Social Media Channels

- ☐ Facebook (pg. 11)
  - ☐ Register for Blue Badge Account
  - ☐ Enroll in Facebook Protect
  - ☐ Prepare your Facebook page to be voting alert eligible
  - ☐ Bookmark https://www.facebook.com/gpa
- ☐ Twitter (pg. 11)
  - ☐ Get recognized as a Verified Account
  - ☐ Bookmark https://blog.twitter.com/en_us/tags.blog--elections.html
- ☐ Google (pg. 12)
  - ☐ Add two factor authentication to google accounts
  - ☐ Senior officials can qualify for the Google Advanced Protection Program. See if you qualify and register.
  - ☐ Verify your local election authority's business profile.
- ☐ YouTube (pg. 12)
  - ☐ Secure your existing YouTube account https://youtube-creators.googleblog.com/2020/05/three-steps-youtube-account-secure.html

Traditional Media and Community Outreach

- ☐ Establish relationships and share election information with key local voices and groups. These include:
  - ☐ Radio stations
  - ☐ TV stations
  - ☐ Print media outlets
  - ☐ Community groups
  - ☐ Other

Publicize Your Online Channels

- ☐ Create a list of community voices and try to reach out to them via social media or other channels (phone, email, in person).
- ☐ Check that your channels are well known by key local voices and groups (see previous bullet).
- ☐ Share your social media channels with other election jurisdictions and organizations.
  - ☐ Establish a norm of supporting each other to publicize important content.
  - ☐ Follow your stakeholders and state chief election officials' social media channels.

Know Your Threats

- ☐ Conduct incident review (pg. 14)
- ☐ Conduct stakeholder mapping and reputational risk analysis
- ☐ Conduct crisis simulations and tabletop exercises
- ☐ Map your potential election day vulnerabilities, using the "5 Questions" of the election process. (pg. 14)

Stage 2: Identify & Assess

Develop Indicators and Warning Signs (pg. 16)

- ☐ Use questions from the 'Know the Threats' section to create key indicators and warning signs.
  - ☐ The "5 Questions of the Election Process" can help you identify top targets of IO and generate key-words you can use as indicators (pg. 41).

Monitor in Real Time (pg. 18)

- ☐ Set up tools for monitoring key identified voices, themes, and hashtags.
- ☐ Use tools to monitor and identify mis/disinformation incidents.
- ☐ Fact check and verify your information.

Document Evidence (pg. 19)

- ☐ Establish the format you will use for documenting evidence of mis/disinformation, answering the **"5 Questions of Reporting."** Documenting evidence as incidents evolve will help you lay the groundwork for reporting.

Assess Incident Severity (pg. 20)

- ☐ Determine whether the incident is high, medium or low severity. Consider:
  - ☐ What voices are sharing the mis/disinformation? Are they established voices?
  - ☐ What is the credibility of the information being shared?

- ☐ Is the information being shared at high volume or gaining momentum?
- ☐ Can it be contained relatively quickly/easily?

Incident Severity Escalation Table pg. 20.

When to Activate the Incident Response Team (pg. 20)

- ☐ Is the incident severe enough to activate the Incident Response Team?
  - ☐ High: Urgent Activation of the Incident Response Team is necessary.
    - ☐ Does the incident threaten to significantly undermine voter confidence in the integrity, process, and outcome of the election?
  - ☐ Medium: Activation of the Incident Response Team is necessary.
    - ☐ Does the incident have the potential to negatively affect voter confidence in elections?
    - ☐ Report incident.
  - ☐ Low: Activation of the Incident Response Team is not necessary, unless the situation graduates to a medium severity incident. Reporting the incident may alone be sufficient.
    - ☐ Is the incident recieving low coverage or could it be seen as implausable? Does it pose a limited threat to voter confidence?
    - ☐ Monitor the incident in case its severity graduates to medium.

Stage 3: Respond & Resolve

Report Mis/Disinformation (pg. 22)

- ☐ Ensure you have answers to all "5 Questions of Reporting" (who, what, when, where, how) prepared for your report.
  - ☐ Use evidence gathered in the 'Document Evidence' section.
  - ☐ Include:
    - ☐ Account names
    - ☐ Pages
    - ☐ Hashtags
    - ☐ Dates and times posts appeared
    - ☐ Platform
    - ☐ Hyperlinks, screenshots, or images
    - ☐ Document how the incident is impacting, or risks, impacting the election.

Report mis/disinformation incident to:

- ☐ Chief Election Official(s), State Election Bodies
- ☐ Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
- ☐ Social media platforms

Reporting Priority Table and Contacts (pg. 24)

Reporting to the Tech Platforms- Detailed Reporting Steps and Additional Contacts (pg. 44).

Sample Incident Reporting Email [Template] (pg. 52.)

Communicate (pg. 25)

Communications Process for a Mis/Disinformation Incident

- ☐ Assess incident severity, decide what to do, communicate, leave it alone or monitor it
- ☐ Activate the Incident Response Team
  - ☐ Who are the stakeholders in this specific incident?
  - ☐ How will you reach out to each of these stakeholders, using what channels?
  - ☐ Establish ground truths as much as possible.
- ☐ Notify key internal and external stakeholders
  - ☐ State and local elections bodies
- ☐ Notify key external stakeholders
  - ☐ Federal bodies
  - ☐ Social media platforms
- ☐ Inform any additional incident-specific stakeholders
  - ☐ Political campaigns
  - ☐ Local community leaders
  - ☐ Advocacy groups
- ☐ Plan and execute external outreach
  - ☐ Adapt communications plan to specific details of this incident
  - ☐ Draft communications materials using what your assessment, or verified audiences are saying to guide response
    - ☐ Ensure that any materials include the latest verified facts
  - ☐ Coordinate for approval by key decision-maker

- ☐ Send out for dissemination through your official communications channels such as the official website and social media accounts (Facebook, Twitter, etc.), validators and media

☐ Establish a feedback loop.

- ☐ Establish feedback intake process via media and social media monitoring, and track media inquiries and stakeholder comments.
- ☐ Review and revise messaging as needed, based on feedback.

Incident Severity Escalation Table, pg 20.

Best Practices for Responding to Mis/Disinformation, pg. 54.

Part 3: Mis/Disinformation Scenario Plans, email connect@d3p.org

Stage 4: Learn & Improve

Improving Through Experience (pg. 30)

☐ Conduct a post-election learning exercise.

☐ Update your response plan to incorporate lessons learned.

☐ Conduct tabletop simulation prior to next election to test updated processes.

Incident Response Team [Template]

This table can act as a starting point for allocating roles and responsibilities as you determine your team set up for responding to mis/disinformation incidents. It should be adapted to your local, specific context.

Include:

- ☐ Name
- ☐ Contact information (phone, email)
- ☐ Backup contact information
- ☐ Contact information of the backup individual responsible in the event that the primary person is unavailable
- ☐ Set responsibilities of the person (e.g. media spokesperson or social media director)

Position	Designated Individual(s) and Contact Information	Designated Backup and Contact Information
Chief Election Official		
Director of Elections		
Communications Team		
Chief Information Officer/IT Director		
Government & Community Relations Director		
Chief Legal Officer		
Law Enforcement Liaison		
Affected County Elections Administrators		

- **Designated communication channel: _____**
- **Back-up communication channel: _____**

"5 Questions of the Election Process" Keywords

Top Targets of Election IO [Template]

WHO? Mis/Disinformation often targets the people that enable elections to run. This may involve impersonating or disparaging elections-related groups or individuals through hacked or fake social media accounts, websites and articles.

The most prominent targets include:	**Example search terms include:**	**Create your list of targets or key words:**
Election officials in your office, or in offices lateral to yours (e.g., county to county) or vertical to yours (e.g., county to state)	Your Election Director's name (e.g., county clerk, state elections director) or names or positions of prominent officials, your office name (ie—X County elections)	
Poll workers and other volunteers, such as signature checkers or ballot counters	*The phrase "poll workers" or "volunteers" or other similar terms*	
External staff, such as those who manage key external systems like Motor Voter	*Acronyms of relevant offices, like "DMV" for Department of Motor Vehicles*	
Vendors, including companies or individuals	*Phrases like "vendor" or the names of actual vendors*	
Third-party or special interest groups with access to large voter bases	*Names of third-party groups (e.g., Get Out the Vote organizations)*	

WHAT? Mis/Disinformation may spread false allegations of disrupted election hardware, software, and infrastructure including vendor-managed systems. This includes allegations of bias, malfunctioning, or hacking.

The most common targets include:	**Example search terms include:**	**Create your list of targets or key words:**
Voter Registration Databases (VRDB)	*Phrases like "Voter Registration Databases" or "VRDB"*	
E-poll books	*Phrases like "E-pollbooks" or "poll books"*	
Vote-casting Devices	*Phrases like "voting machine" or "vote casting" or the actual name of your vote-casting devices*	
Vote Tally Systems	*Phrases like "Vote Tally" or "mis-count" or "recount"*	
Election Night Reporting Systems (ENR)	*Phrases like "Vote Count" or the actual name of your ENR provider*	
Contentious Political Issues	*Terms like "Voter Suppression," "Voter Fraud," or "Illegal Voting"*	

WHEN? Mis/Disinformation often misrepresents facts about key times and dates for elections. Elections can be catastrophically disrupted if voters do not know when they will occur, when to register to vote, or the times of other key events.

The most common targets include:	**Example search terms include:**	**Create your list of targets or key words:**
When Election Day is	*Phrases like "election day" or the actual date of an election (e.g., "November 3rd")*	
When polls open and close	*Phrases like "polls open," "polls closed" or other similar phrases*	
When you register to vote	*Phrases like "voter registration" or other similar phrases*	
When the deadlines are for early voting or absentee voting	*Phrases like "early voting" or "absentee voting" or the actual deadline*	

WHERE? Mis/Disinformation can disrupt elections by reporting false information about locations involved in the elections process, including for voting, registration, or other events.

The most common targets include:	**Example search terms include:**	**Create your list of targets or key words:**
Where you vote on Election Day (or early voting in states that offer it)	*Terms like "Polling Place" or "Vote by Mail" as well as the names of actual polling places (e.g., "Croissant Park Elementary School")*	
Where you register to vote	*Terms like "Voter Registration" or "Online Registration" or the names of actual registration locations*	
Where you return an absentee (or "mail-in") ballot	*Terms like "Mail-in Ballot" or "dropbox"*	

HOW? Mis/Disinformation often misrepresents how key election events like voting or registration occur. This may involve suggesting that voters can vote through a variety of unsanctioned methods (e.g., by text message, social media).

The most prominent targets include:	**Example search terms include:**	**Create your list of targets or key words:**
Voting day processes	*Terms like "Ballot," "Mail-in Ballot," "Polling Place" or "Vote by Mail"*	
Voter registration processes	*Terms like "Voter Registration," "Online Registration," "Same Day Registration" or the names of actual registration locations*	

Reporting Mis/Disinformation to Social Media Platforms

Detailed Reporting Steps

Platforms

Many of the social media companies and internet platforms have taken steps to try to limit the spread and effectiveness of mis/disinformation. Here we look at four of the most important platforms (Facebook, Twitter, Google and YouTube), and how you can best report mis/disinformation incidents to them. We recommend reporting to platforms after first reporting to your chief election official and to EI-ISAC.

Facebook
Top Takeaways
With 1.73 Billion daily active users, Facebook is the most used social media platform in the United States. It is therefore critical to pay attention to Facebook as an election official. However, much of the content on Facebook is private; visibility is limited to users' own social networks and pages. As such, monitoring mis/disinformation on Facebook requires coordination between election officials, state officials, support systems at the federal level, and with the platform itself. It can however be a powerful response tool.
How to Report Mis/Disinformation to Facebook
If you identify Facebook content or accounts that you suspect are harmful mis/disinformation, follow the three reporting steps: Report to Facebook, by emailing reports@content.facebook.com and cc your regional contact (listed below).

FACEBOOK CONTACT INFORMATION (Current as of June 2020)

Region	Contact Name	Contact Email*
All	All	reports@content.facebook.com
Southwest and California (AZ, CO, KS, NE, NM, NV, OK, TX, UT, CA)	Jannelle Watson	jannelle@fb.com
Northeast and mid-Atlantic (CT, DC, DE, MA, MD, ME, NH, NJ, NY, PA, RI, VA, VT, PR)	Khalid Pagan	kpagan@fb.com
Midwest and South (AL, AR, FL, GA, IA, IL, IN, KY, LA, MI, MN, MO, MS, NC, OH, SC, TN, WI, WV)	Rachel Holland	rachelholland@fb.com
Northwest (AK, HI, ID, MT, ND, OR, WA, SD, WY)	Eva Guidarini	eguidarini@fb.com

**Your regional contact can help you get registered for a Blue Badge Account (pg. 11)*

To appeal a decision, coordinate with your Chief election official and supporting national collaborators.

Facebook's Rules: What Content Violates Their Policies?

Facebook bans the following types of content in their terms of service:

- Misrepresentation or fraud relating to voting or the census
- Misrepresenting identity or impersonating others
- Manipulating media to be misleading; harassment
- Other forms of coordinated inauthentic behavior

Most importantly, if you see content on Facebook that misrepresents the "5 Questions" of the election process, that content should be reported.

Recommended Action Steps

- Report mis/disinformation to the platform via reports@content.facebook.com and by ccing your regional Facebook contact.
- Consider whether the "Voting Alerts" messaging feature can support your response to voters.[30]
- Facebook has created a page with tools and information for public officials. Bookmark it in your web browser so that you can reference it throughout the election cycle: https://www.facebook.com/gpa

30 Facebook, "Use Local Alerts and Voting Alerts": https://www.facebook.com/business/help/572490746512593?id=1549080658590154

Twitter

Top Takeaways

Twitter is one of the most widely used social media platforms, with 145 million daily active users. The platform takes mis/disinformation claims seriously. From their terms of service:[31] "any attempts to undermine the process of registering to vote or engaging in the electoral process is contrary to our company's core values."

In May 2020, Twitter expanded it's policy on manipulated media to issues of civic integrity, including elections, and COVID-19 to label messages where people may be mislead by content. Twitter will label Tweets and give additional context for Tweets containing misleading or disputed information. These labels link to other tweets that show factual statements, counterpoint opinions or other public conversation around the issue.[32]

As with other social media platforms, Twitter can help you in your response process and also in your monitoring of mis/disinformation incidents.

How to Report Mis/Disinformation to Facebook

Enroll in Twitter's Partner Support Portal (PSP)

- Chief election officials have access to this special reporting tool. Ahead of November 2020, Twitter is making the (PSP) available for local election officials.
- Contact PSPOnboarding@twitter.com to learn more and to get registered.

Report using the PSP

- The PSP expedites the review of content flagged for potentially violating Twitter's rules around civic events. You can register and report on the PSP regardless of whether your account is verified through Twitter.
- If you are not yet registered on the PSP, notify your chief election official to submit a report for you.
- To appeal a decision, utilize the PSP and coordinate with your chief election official who may be able to engage advocates who are also in touch with the social media platforms.

31 Twitter, April 2019, "Strengthening our approach to deliberate attempts to mislead voters": https://blog.twitter.com/en_us/topics/company/2019/strengthening-our-approach-to-deliberate-attempts-to-mislead-vot.html

32 US House of Representatives Committee Repository, June 2020, "Hearing: Emerging Trends in Online Foreign Influence Operations: Social Media, COVID-19, and Election Security": https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=110805

Alternate Reporting Methods

If you are not registered on the PSP and are unable to coordinate with your chief election official you can report directly to Twitter via the below methods. But note that these methods may not be as efficient as the PSP; report to the EI-ISAC at minimum. **As an official, the PSP is the best mechanism to get content flagged for faster review on a report.**

Twitter Forms: help.twitter.com/forms

You can report via this general reporting form by providing "Integrity Feedback" or "Elections Information." Include the following information:

- Tweet [add detail / link]
- Your name, phone number and email address
- Before submitting, save your submitted text in a separate document.
- Upon submitting, write down the case number in case you need to appeal the decision.

Gov@Twitter.com

Provide mis/disinformation details through gov@twitter.com. This email connects many public service individuals and organizations with Twitter's team. Your email should highlight:

- Links to the tweet, twitter @handles and names, source labels, hashtags, official dates, number of views, screenshots, photos, etc.
- You can appeal decisions by emailing gov@twitter.com, referencing the case number, and parts of your submitted description.

Voting Misinformation Reporting Tool

Report directly from a Tweet or profile via the reporting function that appears when you are in Twitter.

- Select "Report Tweet" from the drop down menu on the tweet, and choose the option reading, "It's misleading about voting." Twitter Safety video and steps.[33]

33 Twitter, April 2019, "Strengthening our approach to deliberate attempts to mislead voters": https://blog.twitter.com/en_us/topics/company/2019/strengthening-our-approach-to-deliberate-attempts-to-mislead-vot.html

Twitter's Rules: What Content Violates Their Policies?

- Twitter Rules have been updated ahead of the 2020 elections. Twitter states that content or accounts that do not comply with the following rules are in violation of its Terms of Service.[34]
  - » You may not use Twitter's services for the purpose of manipulating or interfering in elections. This includes but is not limited to posting or sharing content that may suppress participation or mislead people about when, where, or how to participate in a civic process.[35]

Is the media significantly and deceptively altered or fabricated?	Is the media shared in a deceptive manner?	Is the content likely to impact public safety or cause serious harm?	
✓	✗	✗	Content **may** be labeled
✓	✗	✓	Content is **likely** to be labeled, or **may** be removed.
✓	✓	✗	Content is **likely** to be labeled.
✓	✓	✓	Content is **very likely** to be removed.

(source: Twitter[36])

Recommended Action Steps

- Report mis/disinformation to the platform via the Partner Support Portal.
  - » Contact PSPOnboarding@twitter.com to begin the process to enroll in Twitter's Partner Support Portal.
- If you are not enrolled in Twitter's PSP, coordinate with your chief election official to submit a report on the PSP, report via one of the alternate methods and to EI-ISAC.
- Twitter continuously updates their policies in this space; stay updated by bookmarking this page in your web browser[37] for reference during the 2020 election cycle.

34 Twitter, October 2018, "An update on our elections integrity work": https://blog.twitter.com/en_us/topics/company/2018/an-update-on-our-elections-integrity-work.html

35 Twitter, May 2020, "Civic Integrity Policy": https://help.twitter.com/en/rules-and-policies/election-integrity-policy

36 Twitter, "Synthetic and manipulated media policy": https://help.twitter.com/en/rules-and-policies/manipulated-media

37 Twitter, "We're focused on serving the public conversation": https://about.twitter.com/en_us/advocacy/elections-integrity.html

Google

Top Takeaways

Google is the most widely used search engine worldwide. Every year it handles trillions of user searches. Beyond its core search business, Google has a range of other products and services which are relevant to election officials, including Google Maps and its provision of cloud computing, which may host election-relevant web content.

Google's ranking systems aims to elevate legitimate sources and not amplify misinformation; providing additional context on search and ad results; enhancing the security of campaigns; and making it easier for voters to find authoritative information about the upcoming elections. In addition, Google's policies prohibit a number of misrepresentative behaviors across services like Google News, Google Ads, or Google Play.

For example, Google's algorithms and its spam removal team work in collaboration to detect, demote or remove information Google defines as spam, disruptive behavior or content, which may interfere in its systems' recognition of quality webpage content.[38]

How to Report Mis/Disinformation to Google

Google advises that election authorities use its public facing reporting tools to report mis/disinformation. Google's processes for reporting mis/disinformation concerns on its platform are product specific. If you have a concern about misleading information appearing in any of the below products, you should follow the corresponding link to report it.

Product name and reporting link	Product description
Google Maps[39]	Navigation and mapping tool
Google Ads[40]	Adverts that appear alongside search results or on partner websites
Webspam[41]	Results that appear artificially high in search results
Google Groups[42]	Discussion fora
Blogger[43]	A publishing platform
Phishing sites or email[s44]	Sites or emails that try to steal personal information

38 Google, "How we fought Search spam on Google": https://webmasters.googleblog.com/2020/06/how-we-fought-search-spam-on-google.html

39 Google, "Report an error on the map": https://support.google.com/maps/answer/3094088?hl=en&ref_topic=3093612

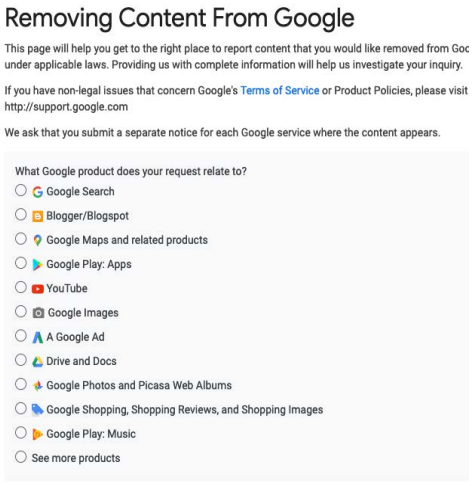
40 Google, "Report an ad": https://support.google.com/google-ads/troubleshooter/4578507

41 Google, "Search console": https://www.google.com/webmasters/tools/spamreport?pli=1

42 Google, "Report abuse or legal issue": https://support.google.com/groups/answer/81275

43 Google, "Help keep the web a welcoming place to create": https://support.google.com/blogger/answer/76315

44 Google, "Report a Phishing Page": https://safebrowsing.google.com/safebrowsing/report_phish/



If you are unsure which product is in use, the tool for requesting a legal removal of information from Google's platforms is user friendly and simple to follow. It can be found on Google's Support Site.[45]

Google does not have a specific target turnaround time to respond to reported content. However, it is likely to be responded to more quickly if you accompany your report with as much detail as possible, including screenshots and URLs of where you saw the mis/disinformation.

If you have any questions about which tool you should be using to report mis/disinformation, the Google Civics team can be contacted directly at: civics-outreach@google.com.

Google's Rules: What Content Violates Their Policies?

Each of Google's different products has specific terms of service. Running throughout these terms of service are restrictions on hateful and misleading behavior/content. This is most emphatically stated in their policies for Google News:

"We do not allow sites or accounts that impersonate any person or organization, or that misrepresent or conceal their ownership or primary purpose. We do not allow sites or accounts that engage in inauthentic or coordinated behavior that misleads users. This includes, but isn't limited to, sites or accounts that misrepresent or conceal their country of origin or that direct content at users in another country under false premises. This also includes sites or accounts working together in ways that conceal or misrepresent information about their relationships or editorial independence."

The key take away from these terms of service is that Google is eager to help in cases of alleged mis/disinformation.

Recommended Action Steps

- Familiarize your teams with Google's reporting tools.
- Register key election officials' Google accounts with the Advanced Protection program.[46]
- Establish your election authority's Google business profile.[47]
- Reach out to the Google Civics team with questions on reporting or with issues reporting: civics-outreach@google.com.

45 Google, "Removing content from Google": https://support.google.com/legal/troubleshooter/1114905

46 Google, "Google Advanced Protection Program": https://landing.google.com/advancedprotection/

47 Google, "My business": http://google.com/business

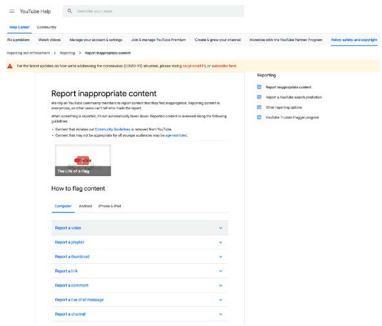
YouTube

Top Takeaways

YouTube is a video sharing platform, where over one billion hours of videos are watched by users daily. It is owned by Google. As it is a video hosting platform, YouTube videos may be shared through other media, including social media, messaging services, and embedded in websites or blogs.

Recognizing that YouTube has played host to misleading content in the past, in preparation for the 2020 elections the company says it has taken several positive steps.[48] These include elevating authoritative information on YouTube via dedicated information panels, news shelves, and in search results; taking steps to reduce the recommendations of borderline content and content that could misinform users in harmful ways.

How to Report Mis/Disinformation to YouTube



Election officials should be prepared to report mis/disinformation that appears on YouTube, using their in-platform reporting mechanisms. These reporting mechanisms can be found on Google YouTube's Report Inappropriate Content Site:[49]

YouTube is owned by Google. If you have any questions about which tool you should be using to report mis/disinformation, the Google Civics team can be contacted directly on civics-outreach@google.com.

YouTube's Rules: What Content Violates Their Policies?

YouTube's Community Guidelines[50] prohibit, amongst other things, impersonation and deceptively manipulated media. This includes *"Using the title, thumbnails, description, or tags to trick users into believing the content is something it is not".*[51] YouTube also has policies in place that prohibit content designed to suppress voter participation, as well as spammy video comments where the sole purpose is to gather personal information from viewers or perform any of the prohibited behaviors noted in their Community Guidelines. As of August 2020, YouTube will remove hacked information shared on its platform intended to interefere with democratic processes.[52]

Recommended Action Steps

- Familiarize your teams with YouTube's reporting tools.[53]
- Reach out to the Google Civics team with questions on reporting or with issues reporting: civics-outreach@google.com.

48 YouTube, February 2020, "How YouTube supports elections": https://youtube.googleblog.com/2020/02/how-youtube-supports-elections.html

49 Google, "Report Inappropriate Content": https://support.google.com/youtube/answer/2802027

50 Google, "YouTube's Community Guidelines": https://support.google.com/youtube/answer/9288567

51 Google, "Spam, deceptive practices & scams policies": https://support.google.com/youtube/answer/2801973

52 New York Times, "YouTube says it will remove 'hacked information' meant to interfere with the election.": https://www.nytimes.com/live/2020/08/13/us/biden-vs-trump?referringSource=articleShare#youtube-says-it-will-remove-hacked-information-meant-to-interfere-with-the-election

53 Google, "Report Inappropriate Content": https://support.google.com/youtube/answer/2802027

Sample Incident Reporting Email [Template]

This form is intended to assist local election officials in reporting mis/disinformation incidents. As email is often the most common form of reporting to EI-ISAC, Social Media Platforms and other collaborators this template is intended to help include specific information, like the "5 Questions of Reporting," in submitting a report. These same details may also help with portal-specific reporting.

- **Who:** Document the account names, pages, and hashtags that are spreading mis/disinformation.
- **What:** Take screenshots of false posts and document their URLs links to them if possible.
- **When:** Record the dates and times that false posts appeared.
- **Where:** Many mis/disinformation events occur on multiple platforms at once. Document which platforms have been affected.
- **How:** Document how the mis/disinformation event is impacting elections, or risks impacting them.

INCIDENT REPORTING EMAIL

Title your email:
[Type of incident] Incident-[County, State]-[date of incident]

(e.g., Disinformation_Incident-LeonFL-05152019)

My Contact Information:
Name: [REQUIRED], Position or Job Title: [REQUIRED]

Your location: [County, State]

Email address: [REQUIRED], Telephone Number: [(XXX) XXX-XXXX]

Date and Time Information:

When, approximately, did the incident start (e.g., when was the Tweet posted on Twitter)?

When was this incident detected (e.g., when did you first see the Tweet)? (REQUIRED)

Briefly describe the incident, including the following elements (REQUIRED):

[ADD Documentation Information You've Collected]

1. Who detected it and/or witnessed it?
2. What was targeted?
3. Where did the incident take place? If it was online, which platforms were used (e.g., Twitter, Facebook, Instagram, Whatsapp, Snapchat, Reddit, 4chan) and what is the URL of where it occurred?

Insert hyperlinks to online content and copy and paste screenshots or images below.

Best Practices for Responding to Mis/Disinformation

Mis/Disinformation incidents are varied and unique. Although each incident may offer a different challenge in considering your response, your engagement in assessing the incident and ultimate response remains important. Below are general best practices to keep in mind as you develop your response plan.

- **Be accurate.** You need to ensure you are operating from a factual position before countering mis/disinformation, so check your facts with multiple sources before citing them publicly. Ask all appropriate questions and ensure you do not accidentally provide misleading information. Remember that your office is not responsible for attribution or scope. You likely cannot say exactly who is responsible or whether they are part of a widespread coordinated campaign (versus a solo actor).

- **Develop a simple, accurate, counter-message.** Develop a short, clear statement that contains only the facts and actions you are taking. Avoid complex messages. You can provide additional nuance later.

- **Do not repeat mis/disinformation.** Instead focus on providing accurate facts first and do not lead or repeat false messages. Think carefully about the benefit of reposting the false information as an example of what you are sharing correct information about—it could give it renewed oxygen.

- **Be visual.** False information on social media is often compelling because it is paired with engaging images. When appropriate, getting your message out with your own compelling image or well-designed graphic can capture voter's attention. **Do not** use the screen-shot of the image to re-share, unless you have carefully planned the intent. Screen-sharing an incident can further its spread. **Do** use screen-shot for reporting!

- **Be transparent.** Caveated, incomplete, or "no comment" responses can fuel conspiracy theories by making it appear your organization has something to hide. Be clear about the processes you have gone through and how seriously you are taking the issue. Demonstrating transparency can help counter false claims.

- **Engage on all platforms.** Mis/disinformation can spread across multiple platforms, including social media and traditional media. To counter mis/disinformation, deliver a clear, factual message on all available platforms. Ask your stakeholders and other validators to share your message on these platforms as well.

- **Develop and deploy validators.** Given many communities' distrust for institutions like government and media, develop relationships with stakeholders from your mapping process, like community leaders, in advance and formally ask them to be validators in case of an incident like this. Having validators in both parties will also prove to be advantageous in the case of a mis/disinformation incident. For example, if voters are concerned an election is being rigged to benefit one side, having the party they support assure them that is not the case is very effective.

Do you see a way to make this Playbook better?

IO threats are evolving, is there new information we should address?

We want your feedback.

Please share your ideas, stories, and comments on Twitter @d3p using the hashtag #IOplaybook or email us at connect@d3p.org so we can continue to improve this resource as the digital environment changes.

Defending Digital Democracy Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 John F. Kennedy Street
Cambridge, MA 02138

www.belfercenter.org/D3P