HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

October 2020
belfercenter.org/D3P

DEFENDING DIGITAL DEMOCRACY PROJECT

MIS/ DISINFORMATION AND CYBER INCIDENT COMMUNICATIONS RESPONSE
TOP TAKEAWAYS

The top priority in a cyber crisis or in the face of mis and disinformation, will be to maintain public trust. The most effective way to achieve that goal is to respond confidently and quickly. **Although response to both types of incidents will differ, there are a number of common best practices you can apply in your preparation ahead of election day.** This summary guide helps detail common and specific responses to each type of incident.

Steps You Can Take Before Election Day

Step 1. Educate the Public and Set Expectations

Make an effort to engage with the public and help set the expectation that there are known cyber and information threats to the election. *For cyber incidents*—Explain how that activity differs from what would be required to interrupt the elections process. Share how you've prepared to date.

Ideas for simple, yet effective outreach includes:

- Have a background conversation with local media.
- Make sure your website is clear and updated—same for any social media channels you operate.
- Reach out to any *existing* validators you already have (by phone or email, and on social media) and let them know you may be asking them to share further information with their networks as the election progresses. Examples of potential validators include:
    - Leaders in key constituencies in your area that may not be typically reached by your communications, official bodies, advocacy groups.
    - Other voices that are influential in those communities. *E.g. community specific publications, famous and other public figures, community activists.*
    - Media covering elections in your area.
    - Your current stakeholders.
- Share insights from any public briefings on mis/disinformation trends or cyber threats (like CISA's public briefings) with community groups and local media.

Step 2. Review Your Response Plan

Update your communications response plan to be used across likely threat scenarios. Make sure your plan details communications coordination roles and responsibilities. Get your response team(s) together to do a final review of your response plan. A good response plan should include:

- Who is on your team
    - Clear roles and responsibilities: Make sure the right teams are talking to each other in the event of either type of incident.
    - Your stakeholders (internal and external) and contact information.
- A clear approval process
- Details for your internal communications (Secure them and create a PACE plan.)
- *Specific for Mis/Disinformation:* Process for social media monitoring
- *Specific for Cyber:* Alignment of your communications response plan with the corresponding technical plan
- Your draft responses to worst case scenarios you're anticipating (or from D3P's Non-Public Planning Guides, *email connect@d3p.org.*)

Key Response Steps

Step 1. Assessing a Mis/Disinformation Incident

It can be hard to know which mis/disinformation incidents to respond to and how broadly to respond. Start by assessing the severity of an incident by considering the following:

- Established Voice: Who is sharing the mis/disinformation? Is it more likely to be trusted based on the voice?
- Credibility: Are voters likely to share the information being shared?
- Volume: How prominent is the mis/disinformation? Assess the momentum.

Building on your assessment of an incident, assign it a severity level. If needed, activate your incident response team and respond or monitor it.

Risk level	Severity Assessment	Activate the IRT?
High	*Incident threatens to significantly undermine voter confidence in the integrity, process, and outcome of elections. (e.g. is changing voting behavior, has the potential to disturb the election process or outcome)*	**Yes** – urgent activation of IRT necessary.
Medium	*Incident has the potential to negatively affect voter confidence in elections. (e.g. may hinder turnout, may gain traction but is not necessarily severe in nature)*	**Yes** – activation of IRT necessary.
Low	*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. Report the incident.*	**No** – activation is not necessary, unless the it graduates to medium. Monitor it.

Step 2. Reporting and Response

These processes should happen simultaneously. *Reporting* is important for potential support in stopping an incident from gaining further traction and in contributing to national security efforts to track targeted campaigns large-scale. *Response* is the process you can control in countering an incident. Both are important.

Reporting:

[Mis/Disinformation Incidents]	**[Cyber Incidents]**
1. Chief Election Officials and State Election Organizations (Varies by State) *for mis/disinformation incidents these officials often have certain reporting access on the platforms and can help in your response.*	Coordinate with your local and state jurisdictions.
2. Authorities: **EI-ISAC: misinformation@cisecurity.org** *Additional:* *DHS/CISA: NCCICCustomerService@hw.dhs.gov* *Your local field office or cywatch@fbi.gov.*	Report to EI-ISAC: SOC@cisecurity.org
3. Platforms:* **Facebook** **reports@content.facebook.com** *See the D3P Election IO Playbook Toolkit to get your regional contact's email and cc them 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 **For questions on reporting tools: civics-outreach@google.com** **See detailed reporting information in the playbook, (p. 44-53).*	Additional contacts: CISAServiceDesk@cisa.dhs.gov, cywatchfbi.gov
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.	

Response:

[Mis/Disinformation Incidents]

Best Practices for Countering Mis/Disinformation:

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, short counter-message. Develop a clear statement that contains only the facts. Avoid complex messages. You can provide additional nuance later.

Respond quickly. Mis/Disinformation can spread rapidly. Your counter-message should be ready to disseminate as soon as possible.

Be transparent. Caveated, incomplete, or "no comment" responses can fuel conspiracy theories by making it appear your organization has something to hide.

Engage on all platforms. Mis/Disinformation can spread across social media and traditional media. To counter mis/disinformation, deliver a clear, factual message on all available platforms.

Avoid repeating mis/disinformation. Focus on providing accurate facts and do not repeat the false messages. For example, if false rumors circulate that lines at the polls are many hours long, avoid saying that rumors of long lines are circulating. Instead, your message should be that lines are short and moving quickly. 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.

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.

[Cyber Incidents]

Best Practices for Communicating with the Public Around Cyber Incidents:

Be transparent but careful. Public comments should demonstrate that you are taking the issue seriously but avoid providing any details that may change as the investigation progresses, so you do not have to correct yourself down the line. Avoid speculation on the perpetrator of the incident.

Focus on actions you are taking to address the issue. Talk about the steps you are taking to protect voter information and address any broader risks to the system.

Provide context. Counter speculation with facts and context to reduce the risk of undermining public trust. Include metrics whenever possible.

Be visual. Connect with design teams who can provide you infographics and develop a library of graphics and photos you can draw from.

Use the right digital tools. When a cyber incident strikes, social media is now a go-to source of immediate information. In practice, this means using it selectively to counter mis/disinformation and inaccuracies.

Focus your communications on your most important stakeholder—the public. You will be tempted to discuss the components of the incident. Instead, talk about what you are doing to address public needs or concerns in this given situation.

Speak plainly. Cybersecurity can be off-putting to nontechnical audiences. Use anecdotes and examples to demystify cybersecurity issues whenever possible.

Establish communications with the media and the public about the cybersecurity measures you are taking now, so that the first time they hear from you is not in a crisis. Knowing current potential cyber threats, share how you've been preparing to mitigate this threat before election season to counter these threats before election day.

Additional Information:

Resources to help you determine potential scenarios. *With less than one week, doing scenario planning can be too time consuming.* Below are examples of potential scenarios you could review with your team ahead of election day. If someone from your team has capacity, you can use D3P's Non-Public Cyber and Mis/Disinformation Scenario Guides (*Exclusive for Officials*) to help you prepare to respond more quickly to incidents: **Election Cyber Incident Communications Plan Template Private Appendix** and **D3P Election Influence Operations Playbook Part 3: Mis/Disinformation Scenario Plans**. *Get access to these documents here or by emailing connect@d3p.org.*

Potential Scenarios:

[Mis/Disinformation Incidents]	**[Cyber Incidents]**
Top Targets of Election Interference: The "Five" Questions Disinformation targeting elections, and resulting misinformation, typically falls into one of the five questions of how elections run—*the who, what, when, where, and how of the election process*. **While mis/ disinformation incidents can vary these narratives reflect a range of incidents you may encounter:** • False voter ID requirements spread online • Congestion causing poll workers to turn voters away • Accusations of fraudulent voting • Claims of vote count improprieties • Claims that polling places closed due to COVID-19 concerns • False claims of a judicial delay to election date due to COVID-19 • Concerns of voter intimidation and violence at polling places (*new*)	**Election-related incidents fall broadly into five categories:** 1. Online rumors that seek to undermine confidence in an election (and claims of a successful cyber-attack, despite proof of success) 2. Reconnaissance of election-related systems 3. Theft of voter or other election data 4. Data manipulation that could affect an election outcome 5. Data destruction.

Additional Resources:

Mis/Disinformation Incidents: Reference the D3P Election Influence Operations Playbook Part 2: Mis/Disinformation Response Plan and Part 3: Mis/Disinformation Scenario Plan.

- Assess Incident Severity & Know When to Activate Your Response Team (p. 20,21)
- Incident Severity Escalation & Response (p. 26-29)
- *Response* Recommendations (p. 6-8, p.22-29, p. 54 and Part 3)
- *Reporting* Recommendations (p. 23-24)
- Detailed Reporting Steps for Reporting to Social Media Platforms (p. 44- 53)

Cyber Incidents: The Election Cyber Incident Communications Coordination Guide and the Response Checklist, (p.26).