ELECTION INFRASTRUCTURE INCIDENT RESPONSE COMMUNICATIONS GUIDE

Introduction

When an incident occurs that impacts election operations or security, communication to the public is essential to ensuring confidence in the integrity of the election process. Events such as severe weather, physical threats, cyber incidents, equipment malfunctions, or potentially criminal uses of disinformation that distribute false information regarding the time, place, or manner of elections, can quickly introduce disruptions to the election process. Partners and the public look to election officials as the authoritative sources for timely, accurate, and clear information about what has happened, how election operations may be impacted, and what is being done to mitigate these impacts to keep election operations running. Preparing your office for how to communicate during an incident is a critical step to ensure an impactful response that maintains public confidence.

The Cybersecurity and Infrastructure Security Agency (CISA) and the U.S. Election Assistance Commission (EAC) created this guide to help election officials build their own election infrastructure incident communications playbook before an incident occurs. It includes the core components of an incident response playbook and outlines the key steps election offices can take to communicate effectively during an incident.[1] The guide also includes customizable templates with instructions and considerations for effective communication, maintaining transparency, and ensuring accurate and timely updates during an election incident.[2]

Building Your Election Infrastructure Incident Response Communications Playbook

The following steps will help you build out your organization's incident response communications playbook.

1. **Identify the key members of the incident response communications team.** The first step is identifying who you need to be a part of the core incident response team responsible for communications. The incident response communications team should bring together members from across the organization who, in addition to communications practitioners, can provide critical information about the incident itself, situational awareness of the larger information environment and the election process, and knowledge of mitigation measures likely to employed. Whether you have a dedicated communications team, or you are a one- or two-person office, you will need to identify which team members will have communications responsibilities and ensure those individuals are brought into the incident response process.
    - *Document* roles and responsibilities for incident response, including identifying communications leads. Ensure the incident response communications team contains at least one elections representative and one operational expert (i.e., for cyber incidents ensure the team includes an information technology (IT) specialist).

2. **Develop your "common terms" list.** During an incident it is critical all team members understand the situation at hand and are using the same language to accurately describe the situation as it evolves.
    - *Put a list together of common terms* the team can use to familiarize themselves with that would be relevant if an incident occurs. For example, define common types of incidents like "ransomware" or "distributed denial of service," as well as mitigation or response terms that are likely to be used like "off-line back-ups."

3. **Establish your internal staff communications plan and external communications approval process.** Identify how often the incident response team will meet to discuss updates, who will be responsible for communicating with external stakeholders, and the process for getting those external messages cleared and approved.

[1] This guide is significantly based on the Harvard Belfer Center's 2018 publication: belfercenter.org/publication/election-cyber-incident-communications-plan-template

[2] An interactive video training series with short activities designed to illustrate core concepts related to public communication is available on the EAC's YouTube channel.

- *Establish reporting mechanisms and the frequency* with which communications situational updates will be prepared and disseminated across the organization. For example, determine processes to let the organization know how many media inquiries have been received, the status of responses, and updates to talking points or holding statements.
- *Document the external messaging approval process* so everyone knows who is involved and who gives final clearance with what messages are shared externally.

4. **Identify and test your communications assets.** Identifying the technology you need to communicate during an incident is a crucial part of incident response planning for ensuring continuity of operations.
   - *Help your information technology (IT) team* identify which systems and equipment are critical for your crisis communications.
   - *Develop a PACE (Primary, Alternate, Contingency, and Emergency) plan* that specifies multiple backup methods of communication. These methods may include internet-, cellular-, and radio-based methods for sharing information. Practice using each method when testing incident response procedures; when one fails, turn to the next one.
   - *Conduct tabletop exercises* to test and fine-tune incident response communications plans. Plan for adverse events, such as weather events or cyberattacks, that could impact your operations and availability of communication systems.
5. **Develop a template for communicating during an incident response.** While the types of incidents to which an election office may respond will vary, the key components of communication for any incident will be the same. The Appendix of this document provides communications templates.
   - *Develop draft talking points and holding statements in advance* that address the most likely incident scenarios your office could encounter at the different phases of the election process. Remember to clearly mark these documents as “drafts” to prevent confusion if they are released outside of an actual incident response scenario.
   - *Create a key stakeholder contact list* with principal media and external stakeholder contacts. For each of your stakeholders, establish and maintain a regular point of contact and/or communication cadence so you are not connecting for the first time during a crisis. Offer media contacts education and training on election processes and security measures.

Key Steps for Communicating During an Election Infrastructure Incident

1. **Gather the Facts.** If your office has just observed or received report of an incident that could impact election operations, take a moment to gather accurate information and assess before activating your incident response plan. This helps ensure that your first steps are appropriate for the severity of the incident. Before responding, answer the following questions:
   - *What information do you have?* Determine what you do know, what you do not know, and what you need to know.
   - *What is the credibility of your information?* Some information sources are more trustworthy than others. Have established mechanisms in place to verify any information received. Keep in mind bad actors use tactics like swatting that involve reporting false or alleged incidents to deliberately disrupt operations.
   - *Where does this report come from?* Knowing the source of information can help you prioritize which stakeholders to engage first.
   - *What is the current severity and impact of the incident?* Draw on your incident planning to make these determinations.
2. **Activate Your Response Communications Process.** Once your office becomes aware of a potential or actual incident and determines to the incident warrants considering external communications, activate your incident response communications plan.
   - *Activate your crisis communications team*. In your Incident Response Communications Playbook (described above), you have already identified which team members will have communications responsibilities during a crisis. Activate those members as part of your incident response team.
   - *Activate emergency communications assets.* If needed (for example, because routine communications assets are either inoperable or insufficient), activate additional emergency communications assets that were identified in your planning.
3. **Notify Key Internal Stakeholders and Partners.** As the situation unfolds, keep your team, internal stakeholders and partners informed of developments. Keep in mind your staff is likely affected by the incident too. Not all members of your organization will be directly involved in the immediate response to the incident. Ensuring your staff is

appropriately informed equips them to respond to questions and do their jobs effectively. (See *Initial Incident Notification Template*.)

- *Tell your team* what has happened as quickly as possible and keep them updated.
  - Distribute an internal holding statement to your team (see *Holding Statement Templates*) stating known facts and response plans. Include any relevant office standard operating procedures staff should follow.
  - Distribute talking points to your public-facing teams, such as your team answering the phones and election judge/manager/head poll worker during voting periods. Update these talking points as new information becomes available.
- *Notify and coordinate with internal stakeholders and partners* to ensure a unified communications response. In addition to potentially being required to assist in navigating the incident, internal partners may also play a role in sharing and amplifying accurate and reliable information with voters.
  - Consider activating or standing up a communication operations group. Such a team would facilitate regular communication with key contacts from other organizations with equities in the event, such as local law enforcement or emergency management departments. These groups provide a forum for coordination of facts, talking points, and other incident-relevant information and can assist in amplifying and reinforcing official communications during the incident.
  - Examples of key internal stakeholders and partners include the Chief Election Official, State Elections Director, Governor, County Commissioners, County Administrator, IT Team, Legal Team, Communications Team, and other departments that support your operations.

4. **Communicate to Key External Stakeholders***.* Identify and contact key external stakeholders such as political parties, candidates, and community groups. Keep in mind once external stakeholders are notified it increases the potential for the information to be made public, if not already. Discuss internally the best sequencing for this step and issuing your first public communication about the incident.

5. **Consider issuing an initial public statement***.* When your office should make an initial public statement will vary with each incident. Communicating early, accurately, and consistently, even if the entirety of the incident is unknown, will help establish your organization as an authoritative source and ensure the public is aware of the most accurate and relevant information. Consider criteria such as immediate public danger, visibility of the incident, and impact to elections operations when deciding when to first communicate to the public. Also consider notifying key external stakeholders of public statements in advance to ensure coordination when appropriate.
   - The public statement should only include confirmed information and should indicate additional information will be provided as it becomes available. Priorities for early communications should include ensuring the public remains safe and affected voters are aware of relevant continuity-of-operations measures, such as alternate voting sites, the availability of provisional ballots, or other procedures for voting in an emergency.
   - See *the Public Update Checklist Template* and *Public Information Release Template – Talking Points Guide*.

6. **Maintain Continuous Public Communications Updates.** Accurate information should be front and center in any response. Share updated information with the public on a regular basis as the situation unfolds. Specifically, when it comes to public confidence in the security and integrity of the election process, your subsequent updates should provide greater detail on the incident so the public can better understand what exactly was and was NOT impacted. This includes explaining critical security measures or controls that may have been in place to help mitigate or contain the incident.
   - *Routinely communicate updates.* Establish a regular cadence to receive updates from incident responders. As new information becomes available, distribute updated talking points to key stakeholders in a timely manner. Determine the appropriate methods and cadence for communicating via each medium, such as press statements, email distribution lists, and, if applicable, official social media accounts. If you establish regular calls with media, for example, these calls should be held at the stated time even if your organization does not have any new information. These established calls not only provide you the important opportunity to deliver information to the public through the media, but also allow the media the opportunity to engage with you on the issue and ask questions that are of interest to the public.
   - *Use Websites and Social Media Channels to keep the public updated.* Official websites, blogs, social media sites, text messages (SMS), and smartphone applications are effective tools to advise and inform the public in a timely manner at scale. These channels should be used in concert with other non-digital communication channels. Branding content consistently, including official logo, font, and other formatting, is an important visual signal the messages are legitimate.

7. **Gather External Feedback and Adjust Communication Delivery.** Take steps to understand how your message is being received and consider how to adjust public communications moving forward to ensure that those who need the information are receiving it where they are and can act on it immediately.
    - *Update your messaging appropriately.* As more information becomes available, or as the situation evolves, the initial talking points developed should be updated and, if necessary, tailored for stakeholder groups that are impacted in more specific ways.
    - *Create a feedback loop.* Monitor coverage of your press releases or briefings via television, social media, print, and radio to understand if your messaging is getting traction and, if not, adjust your public messaging as appropriate to ensure that your communication is effective.
    - *Create after-action reports.* Your after-action report should address the incident, the cause of the incident, mitigations taken, how the incident was communicated, and future planning steps to increase resilience to such an event in the future. Release this report publicly and brief key stakeholders. Doing so will help maintain and rebuild public confidence in your election process moving forward. See the *Post-Incident Report Template* for further information.

Additional Resources

- CISA and EAC's *Enhancing Election Security through Public Communications.* Election officials are the primary sources of official information about elections. This guide helps election officials apply communication best practices to election processes, including providing a suite of templates to support election officials in developing their own communication plan for use in everyday activities.
- EAC's *Communications for Election Officials 101*. This video training series on YouTube, was developed to supplement training local election administrators receive from their state officials and associations. These short, practical resources incorporate topics like writing key messages, identifying spokespeople, and choosing appropriate communication channels. The series' guidance is broadly applicable and useful no matter the size or location of the election office.
- CISA's #PROTECT2024 website provides a range of informational resources designed to enhance the security and resilience of election infrastructure by helping stakeholders understand and mitigate risks to elections.

Appendix: Templates

These templates are available to election officials to help manage communications during incidents that impact election operations or security. Each template includes instructions and considerations for effective communication, maintaining transparency, and ensuring accurate and timely updates. Customize the templates with specific details relevant to the incident and your organization. These templates are designed to align with the best practices outlined in this guide. The following templates are included:

1. **Initial Incident Notification Template**
   - **Purpose:** Quickly inform key stakeholders about an incident and initial details.
   - **Use:** Internal and external partners and stakeholders only; not for public dissemination.
2. **Public Statement Template**
   - **Purpose:** Acknowledge an incident and provide initial public-facing information.
   - **Use:** Broader audience including the public and media.
3. **Public Update Checklist Template**
   - **Purpose:** Checklist to determine when to update the public.
   - **Use:** Ensure timely and necessary updates to the public.
4. **Public Information (Press) Release Template – Talking Points Guide**
   - **Purpose:** Ensure consistent and accurate public communication.
   - **Use:** Media interactions and public updates.
5. **Post-Incident Report Template**
   - **Purpose:** Document and analyze the incident, response actions, and lessons learned.
   - **Use:** Comprehensive report for continuous improvement and transparency.

Initial Incident Notification Template (Non-Public)

Purpose

This template is designed to quickly inform internal and external partners and stakeholders about an incident impacting election operations or security. It ensures timely, accurate, and concise communication during the critical early stages of an incident response, specifically for those directly involved in managing the incident, not for public dissemination.

Instructions/Considerations

Before sending the notification, ensure you have verified the key facts about the incident. Keep the message brief but informative, focusing on essential details. Tailor the message for different stakeholders as needed, ensuring all relevant parties receive appropriate information and emphasizing that information should not be disclosed publicly.

Email

Subject: Immediate Notification of Election Incident

Date and Time: [Insert Date and Time]

From: [Election Office/Official Name]

To: [List of Recipients - Internal Stakeholders, Law Enforcement, CISA, etc.]

Good [Morning/Afternoon/Evening],

Our office has [observed/received a report of] an incident that could impact election operations. While our office is in the process of gathering additional details, we are writing to provide a brief update about what we know currently. This information is for your awareness only and not for further dissemination or public release.

Incident Summary Type of Incident: [Severe weather, cyber incident, equipment malfunction, etc.]

- **Date and Time of Incident:** [Insert date and time]
- **Location:** [Insert location]
- **Current Status:** [Brief description of incident status]

Known Facts: [Only include information that is available and appropriate to share at this time.]

- **What Happened:** [Brief description of the incident]
- **Impact on Operations:** [Details about how the incident has affected or may affect election operations]
- **Immediate Actions being Taken:** [Description of any immediate steps taken to address the incident (i.e., who has been notified; assessment of critical comms systems; coordination with law enforcement and state and federal partners, as necessary.]

As per our incident response plan, we have activated the necessary protocols to respond to the incident. We will continue to investigate the incident and provide updates as more information becomes available. Our priority is to ensure the integrity and continuity of the election process while keeping all stakeholders informed.

Points of Contact For further information or to report additional details, please contact:

- **Primary Contact:** [Name, Title, Phone, Email]
- **Secondary Contact:** [Name, Title, Phone, Email]

Thank you for your patience and cooperation.
[Election Office Contact Information]
[Email Signature]

Holding Statement Templates

Purpose

A public statement, or holding statement, serves as an initial incident notification to a broader audience, including voters and the public. A holding statement is used after an incident has been initially reported, but before complete information is available. Holding statements provide a way to keep stakeholders and the public informed while incident response is underway. The statement acknowledges the incident, assures the public and stakeholders that it is being addressed, and reiterates commitment to providing further updates as the situation develops.

During active voting periods, it is critical that holding statements include clear instructions to affected voters on how the incident may or may not impact election operations.

Instructions/Considerations

Before sending a holding statement, ensure you have verified the key facts about the incident. Keep the message brief and avoid including every detail. The purpose is to alert stakeholders and the public you are aware of the incident and are actively responding to it. Be mindful these communications are public facing, ensure the information shared is accurate and an appropriate level of detail for public consumption. The statement should include any pertinent information for voters, specifically if, during an active voting period, the incident will have an impact on the voting process. Plan to provide follow-up updates as more information becomes available.

Social Media Posts

X (formerly Twitter):
We are aware of an incident affecting [insert brief description here such as: voting at a polling location, the state-wide voter registration website, etc.]. Our team is responding and coordinating with [insert the appropriate authorities]. Your safety and the security of your vote are our top priorities. [If appropriate, provide voters specific instructions, such as whether they should continue voting as normal or other instructions] For further details, visit [Election Office Website].

Facebook:
We are aware of an incident affecting [insert brief description here such as: voting at a polling location, the state-wide voter registration website, etc.] and are actively responding along with [insert the appropriate authorities]. Our top priorities are your safety and ensuring the integrity of the election process. [If appropriate, provide voters specific instructions, such as whether they should continue voting as normal or other instructions] We will provide updates as more information becomes available. For further details, visit [Election Office Website].

Instagram:
We are aware of an incident affecting [insert brief description here such as: voting at a polling location, the state-wide voter registration website, etc.] and are actively responding along with [insert the appropriate authorities]. Our top priorities are your safety and ensuring the integrity of the election process. [If appropriate, provide voters specific instructions, such as whether they should continue voting as normal or other instructions] We will provide updates as more information becomes available. For further details, visit [Election Office Website].

Website Alert/Banner

Content: We are aware of an incident affecting [insert brief description here such as: voting at a polling location, the state-wide voter registration website, etc.] and are actively responding along with [insert the appropriate authorities]. Our top priorities are your safety and ensuring the integrity of the election process. [If appropriate, provide voters specific instructions, such as whether they should continue voting as normal or other instructions] We will provide updates as more information becomes available. Contact: [Primary Contact Information]

Contact Information:

- **Primary Contact:** [Name, Title, Phone, Email]
- **Secondary Contact:** [Name, Title, Phone, Email]

Thank you for your patience and understanding.

Email

Subject: Incident Acknowledgement and Initial Response
Date and Time: [Insert Date and Time]
From: [Election Office/Official Name]
To: [List of Recipients - Internal Stakeholders, Law Enforcement, CISA, Public, etc.]
Good [Morning/Afternoon/Evening],
Our office is aware of an incident which as occurred affecting our [insert brief description here such as: voting at a polling location, the state-wide voter registration website, etc.]. At this moment, our team continues to actively look into the situation and take necessary response actions. Here is what we know so far:
Incident Summary:

- **Incident Type:** [Severe weather, cyber incident, equipment malfunction, etc.]
- **Date and Time of Incident:** [Insert Date and Time]
- **Location:** [Insert Location]

Current Status: [Only include information that is available and appropriate to share at this time.]

- **Description of Incident:** [Brief description]
- **Immediate Actions Taken:** [Any immediate steps taken (i.e., activated incident response plan; coordinating with law enforcement)]

Next Steps: We will provide additional information as it becomes available. Further updates will be communicated through [specific channels, e.g., email, website, social media, press releases]. We want to assure the public that we are taking this incident seriously and are committed to maintaining the integrity of the election process.
Points of Contact: For any inquiries, please contact:

- **Primary Contact:** [Name, Title, Phone, Email]
- **Secondary Contact:** [Name, Title, Phone, Email]

Thank you for your patience and cooperation.
[Election Office Contact Information]
[Email Signature]

Public Update Checklist Template

Purpose

This checklist template helps determine when to provide updates to the public during an ongoing incident. It ensures timely and necessary communication with the public.

Checklist

Initial Incident Notification:

- □ Has the incident been confirmed and assessed for impact?
- □ Has the incident response communications team been activated?
- □ Has an official agency spokesperson been identified?
- □ Have immediate response actions been initiated?
- □ Have internal and external stakeholders been initially informed?
- □ Have the initial set of talking points been drafted?
- □ Has an initial public statement been made/press release issued?

Incident Communication Updates:

- □ Has a regular cadence of public communication updates been established?
- □ Are there significant developments in the incident that provide new details to share with stakeholders and the public?
  - ○ Have response actions changed or escalated?
  - ○ Is there new information about the impact on election operations?
  - ○ Are there any changes to continuity measures or voting procedures?
  - ○ Are there updates on coordination with law enforcement and relevant authorities?
- □ Have internal and external stakeholders been informed of the latest developments?
- □ Have you communicated to the public how they should expect to receive incident response updates?
- □ Have you conducted the public updates?

Additional Public Communication Actions:

- □ Have talking points been updated for media interactions?
- □ Is additional guidance needed for public-facing teams?
- □ Are communication update methods prepared to provide periodic updates (i.e., have you established a website dedicated to incident response, are you using a hashtag for the public to follow social media updates, etc.)?

Final Update and Resolution:

- □ Has the incident been resolved or contained?
- □ Have final updates been communicated to all stakeholders?
- □ Have final updates been communicated to the public?
- □ Is there a need for a comprehensive after-action report?

Public Information Release Template - Talking Points Guide

Purpose

This template provides key talking points to use when communicating with the media and public during an incident. These points ensure consistent and accurate messaging and are aimed at maintaining public confidence and transparency.

Instructions/Considerations

Before using these talking points, ensure they are updated with the most current and accurate information about the incident. Be mindful of the public facing nature of these communications, and tailor the level of detail accordingly.

Talking Points

Incident Overview:

- We are aware of an incident affecting [insert brief description here such as: voting at a polling location, the state-wide voter registration website, etc.] and are actively responding.
- Our priority is to ensure the security and integrity of the election process.

Current Status:

- Incident Type: [Brief description of the type of incident]
- Date and Time: [Insert Date and Time of the incident]
- Location: [Insert Location]

Impact on Operations:

- We are assessing the impact on [insert brief description here such as: voting at a polling location, the state-wide voter registration website, etc.] and will provide updates as more information becomes available.
- [Specific impact details, e.g., changes in voting locations, delays, etc.]
- As applicable, outline security measures in place to ensure the integrity of the process to put the incident in context for the public.

Response Efforts:

- We have activated our incident response plans.
- [High level response activities that are underway, e.g., we are coordinating with law enforcement; we are in communication with staff on location and receiving regular updates]
- As applicable, outline how your actions are continuing to ensure the security and integrity of the process.

Public Assurance:

- The safety of voters and staff, and the security of the election, are our top priorities.
- We are committed to transparency and will provide timely updates as the situation develops.

Responding to Speculation and Next Steps:

- Our office is actively coordinating with [insert appropriate authorities] to [insert appropriate action like investigate, restore service, etc.].
- We appreciate your patience as we address the situation and ensure that necessary actions are taken to ensure the safety and security of our elections.
- We will continue to assess the situation and respond accordingly.
- Further updates will be communicated through our website and social media channels.

Contact Information:

- For further inquiries, please contact [Primary Contact Name, Title, Phone, Email].

Post-Incident After Action Report Template

Purpose

The Post-Incident After Action Report template is designed to enable a post-incident review of actions taken to identify lessons learned and inform future incident responses.

Content

Executive Summary: Provide a high-level overview of the incident, key actions taken, and primary outcomes.

Incident Description:

- **Type of Incident:** [Severe weather, cyber incident, equipment malfunction, etc.]
- **Date and Time of Incident:** [Insert Date and Time]
- **Location:** [Insert Location]
- **Description:** [Detailed narrative of what happened]

Response Actions:

- **Initial Response:** [Description of initial actions taken]
- **Ongoing Management:** [Details on continued response efforts]
- **Coordination:** [Information on coordination with law enforcement, CISA, and other partners]

Impact Assessment:

- **Operational Impact:** [Details on how the incident affected election operations]
- **Stakeholder Impact:** [Effects on internal and external stakeholders]
- **Public Impact:** [Description of the incident's effect on voters and public perception]

Communication Efforts:

- **Internal Communication:** [Summary of communication with internal stakeholders]
- **Public Communication:** [Overview of public and media communications, including press releases, social media updates, and public statements]

Lessons Learned:

- **Strengths:** [Aspects of the response that were effective]
- **Challenges:** [Issues encountered and areas for improvement]
- **Recommendations:** [Suggestions for improving future incident responses]

Future Planning:

- **Resilience Measures:** [Steps taken to enhance resilience against similar incidents]
- **Training and Exercises:** [Plans for future training and tabletop exercises]
- **Policy Adjustments:** [Any changes to policies or procedures based on the incident]

Contact Information: For further information or questions, please contact:

- **Primary Contact:** [Name, Title, Phone, Email]
- **Secondary Contact:** [Name, Title, Phone, Email]

[Election Office Contact Information]

Incident Response Team Roles and Responsibilities

Incident response requires a whole of organization approach and it helps to have perspectives from across the organization to help ensure positioning and messaging are accurate, timely and helpful. Understanding that teams are often small, many of these functions may be filled by the same person.

Public Communication Functions to consider for the Incident Response Team:

- Lead Spokesperson - During an incident consider a senior leader in the organization who can speak on the record, with authority and has a good understanding of not only the incident, but the framework and processes potentially impacted.
- Onsite-Incident Lead – this individual would be onsite to interface with the individuals managing the response,
- Communications Planner(s) – (e.g., Incident, strategic, internal)
- Digital (Website / Social Media) Manager
- Legislative, Intergovernmental Affairs Liaisons