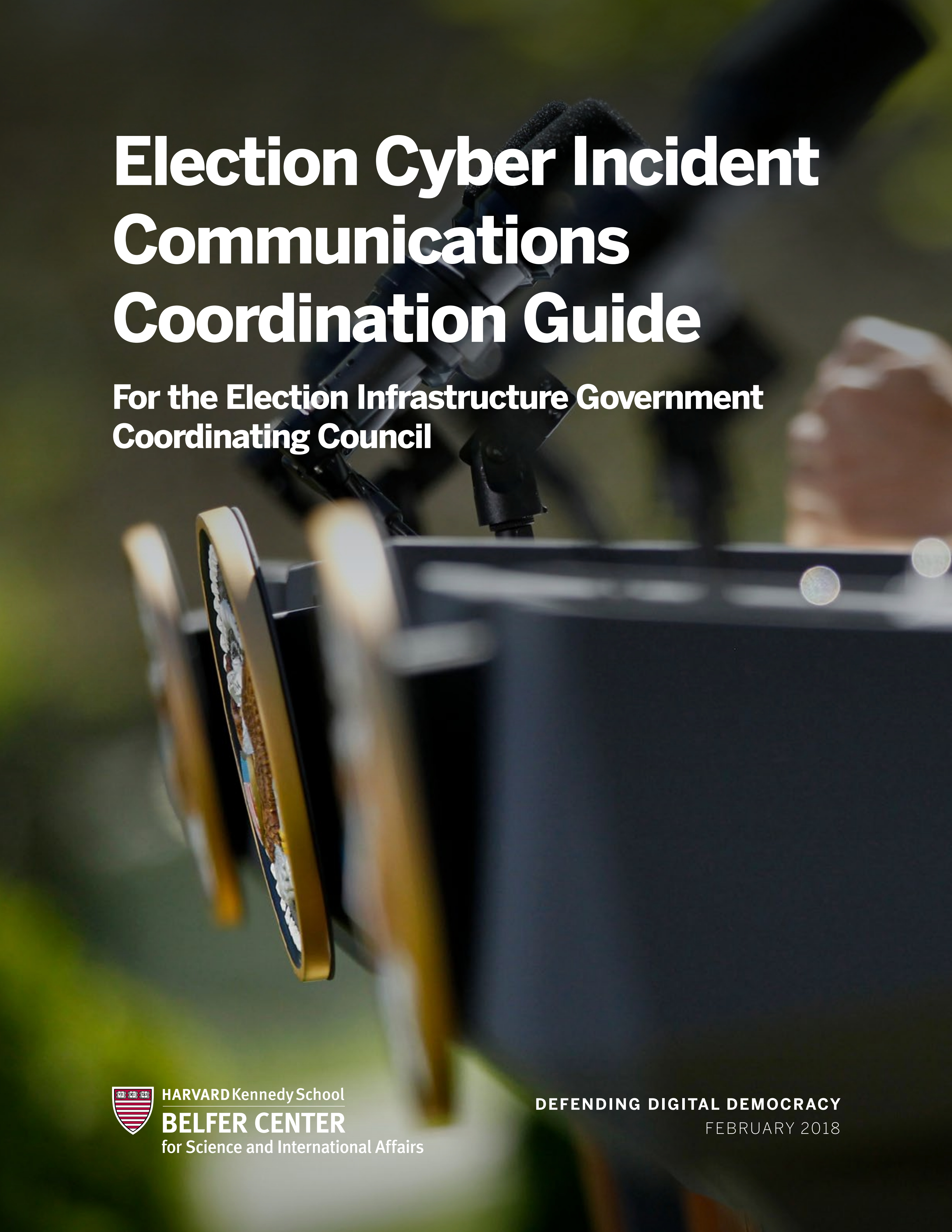


# Election Cyber Incident Communications Coordination Guide

## For the Election Infrastructure Government Coordinating Council

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

DEFENDING DIGITAL DEMOCRACY
FEBRUARY 2018

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

**www.belfercenter.org/D3P**

Statements and views expressed in this document are solely those of the authors and do not imply endorsement by Harvard University, the Harvard Kennedy School, or the Belfer Center for Science and International Affairs.

Design & Layout by Andrew Facini

Cover photo: A view of the podiums during a news conference in the Rose Garden at the White House, Monday, April 2, 2012. (AP Photo/Charles Dharapak)

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

DEFENDING DIGITAL DEMOCRACY
FEBRUARY 2018

# Election Cyber Incident Communications Coordination Guide

## For the Election Infrastructure Government Coordinating Council

## Contents

# Defending Digital Democracy Project: About Us

We established the Defending Digital Democracy Project (D3P) in July 2017 with one goal: to help secure democratic elections against cybersecurity threats and information operations.

There are two groups on the frontlines of defending democracy: (1) political campaigns, which enable citizens to pursue elected office; and (2) election officials, who ensure the election process is free and fair.

Last year, we set out to provide campaign and election professionals with practical guides to the most applicable cybersecurity best practices in advance of the 2018 midterm elections. In November 2017, we released "The Campaign Cybersecurity Playbook" for campaign professionals.

Now, we are releasing a set of three playbooks designed to be used together by election administrators: "**The State and Local Election Cybersecurity Playbook**," "**The Election Cyber Incident Communications Coordination Guide**," and "**The Election Incident Communications Plan Template**." What follows is the Coordination Guide.

D3P is a bipartisan team of cybersecurity and policy experts from the public and private sectors. To better understand the cyber threat and other challenges that election administrators face, our team spent four months interviewing state officials about their communications practices and how they would or would not apply these practices in a cyber incident. We spoke with state and local election officials, as well as key national-level players and members of the Election Infrastructure Government Coordinating Council (EI-GCC).

These interviews exposed the range of challenges election officials confront in the cyber domain. One of the most significant needs we encountered was the ability to communicate consistently across states in the event of a major election cyber incident, in order to maintain public trust.

This Guide is primarily intended for use by the EI-GCC to coordinate multiple voices (and multiple facts) in an election cyber incident that crosses traditional jurisdictions. We are releasing the Guide publicly, because a range of officials may be interested in learning more about how state and local leaders can, and should, coordinate their communications in the event of this type of cyber incident. We hope this Guide becomes a starting point for the EI-GCC to establish its role as a central communications node in the event of an election cyber incident.

Finally, we would like to thank the election officials around the country for whom we wrote this guide You are the frontline defenders of democracy. We hope this effort helps make that tremendous responsibility a little easier.

Good luck,
The D3P Team

# Authors and Contributors

This project was made possible by dozens of people who generously volunteered their time. Special thanks are due to **Siobhan Gorman** for leading the project and who, in addition to **Matt Chandler**, **Meredith Davis Tavera**, and **Chris Farley**, wrote this Coordination Guide.

We are also indebted to the people listed below who invested countless hours in reviewing drafts and providing input.

## SENIOR ADVISORY GROUP

**Eric Rosenbach**, Co-Director, Belfer Center;
Director, Defending Digital Democracy Project

**Robby Mook**, Co-Director, D3P

**Matt Rhoades**, Co-Director, D3P

**Heather Adkins**, Dir. of Information Security and Privacy, Google

**Dmitri Alperovitch**, Co-Founder and CTO, CrowdStrike

**Siobhan Gorman**, Director, Brunswick Group

**Yasmin Green**, Head of Research & Development, Jigsaw (Alphabet)

**Stuart Holliday**, CEO, Meridian International Center

**Kent Lucken**, Managing Director, Citibank

**Debora Plunkett**, former Director of Information Assurance, National Security Agency

**Colin Reed**, Senior Vice President, Definers Public Affairs

**Suzanne Spaulding**, Senior Advisor for Homeland Security, Center for Strategic and International Studies

**Alex Stamos**, Chief Security Officer, Facebook

## CONTRIBUTORS

**Lori Augino**, Director of Elections, WA Office of the Sec. of State

**Matt Chandler**, Partner, Frontier Solutions

**Caitlin Conley**, Executive Director, D3P

**Amy Cohen**, Executive Director, National Association of State Election Directors

**Meredith Davis Tavera**, D3P, Harvard Kennedy School

**David Forsey**, Policy Analyst,  National Governors Association

**Shannon Cortez**, Deputy Director of Elections, WA Office of the Secretary of State

**Chris Farley**, Associate, Albright Stonebridge Group

**David Forsey**, Policy Analyst,  National Governors Association

**Karen Ejiofor**, Staff Assistant, Belfer Center

**Siobhan Gorman**, Director, Brunswick Group

**Eben Kaplan**, Principal Consultant, CrowdStrike

**Jane Khodos**, Senior Director, Comms. and Content, FS-ISAC

**Matthew Masterson**, Commissioner, Election Assistance Commission

**Jeff McLeod**, Division Director for Homeland Security and Public Safety, National Governors Association

**Robby Mook**, Co-Director, D3P

**Matt Rhoades**, Co-Director, D3P

**Eric Rosenbach**, Co-Director, Belfer Center;
Director, Defending Digital Democracy Project

**Michelle Tassinari**, Director/Legal Counsel, Elections Division, Office of the Secretary of the Commonwealth of MA

## BELFER CENTER WEB & DESIGN TEAM

**Arielle Dworkin**, Digital Communications Manager, Belfer Center

**Andrew Facini**, Publications and Design Coordinator, Belfer Center

# Acknowledgments

The D3P team would like to especially thank Heather Adkins of **Google**, Yasmin Green of **Jigsaw**, the **Hewlett Foundation**, the **Democracy Fund**, and the **Belfer Family**; without whom this Playbook would not have been possible. Additionally, we would like to thank the following organizations and offices for sharing their time with us through conversations, simulation participation, or field visits. Your perspectives were critical in shaping our approach to this document.

Department of Homeland Security (DHS)

National Association of State Election Directors (NASED)

National Association of Secretaries of State (NASS)

National Governors Association (NGA)

National Guard Bureau (NGB)

### Election Officials from the Following States and Jurisdictions:

Atlantic County, New Jersey

Nevada County, California

Orange County, California

Santa Clara County, California

State of Colorado

Arapahoe County, Colorado

City and County of Denver, Colorado

State of Connecticut

Escambia County, Florida

Cook County, Illinois

State of Louisiana

State of Maryland

Caroline County, Maryland

Commonwealth of Massachusetts

State of Minnesota

State of Nevada

Clark County, Nevada

State of New Jersey

Mercer County, New Jersey

State of North Carolina

State of Ohio

State of Oregon

Multnomah County, Oregon

Commonwealth of Pennsylvania

State of Rhode Island

State of Tennessee

State of Vermont

Commonwealth of Virginia

State of West Virginia

Harrison County, West Virginia

State of Washington

State of Wisconsin

## How to Use this Communications Guide

This communications guide includes best practices and guidelines to help the Election Infrastructre Government Coordinating Council  (EI-GCC) quickly coordinate the response to an election-related cyber incident that affects more than one state during the early days of the incident. While every cybersecurity incident is unique, this document provides a foundation on which the EI-GCC can build a response that addresses the incident with the goal of maintaining confidence in the election system.

This Guide should be owned by the communications director, or a similar position, at the EI-GCC and be updated at least annually.

### Key topics include:

**Strategy, Mission, and Objectives**: The purpose of the Guide is to help election officials maintain public confidence in the integrity of the U.S. election system in the event of an election-related cybersecurity incident.

**Establishing a Cyber Communications Baseline:** This section explains the importance of educating the public and other key stakeholders on cyber threats facing the election process and steps currently being taken to counter them.

**Cyber Incident Best Practices:** This section includes best practices for communicating with the media and other key stakeholders.

**Communications Process Workflow:** This component includes diagrams that outline who will manage the cyber crisis communications response and serve as spokesperson during an incident.

**Response Checklist:** This checklist broadly outlines steps that should be taken during the first several days after learning about a potential incident.

# Executive Summary and Purpose

What constitutes a “cyber incident” in elections can range from theft of voter registration data to disruption or manipulation of the vote tally. This Guide is designed to help coordinate and align communications across jurisdictional boundaries in an election-related cybersecurity incident that involves more than one state. Its primary purpose is to maintain (or regain) public confidence in the face of such an incident.

This Guide is written to help the Election Infrastructure Government Coordinating Council (EI-GCC) assist state and local election officials, who will need to communicate across jurisdictions if an election-related cyber event has impacts beyond a single state. While every jurisdiction should have its own plan to respond to a cyber incident, many incidents will have implications beyond state boundaries. It is critical to coordinate the response from the outset, so public comments confidently convey that the issue is being addressed and maintain public trust in election systems across the country.

**We recommend the creation of a communications coordination structure within the EI-GCC**, including a communications director, or similar role, who would be a key spokesperson in a cyber crisis.

**A multistate cyber incident could take many forms**. It could be a series of incidents that collectively have a broader impact. It could be one or a few incidents that, because of their strategic significance or other factors, have an impact beyond state boundaries, or receive outsized attention from national media outlets. This could even be a false rumor that requires a coordinated effort to stamp it out.

## This Guide provides:

1. A set of best practices for communicating about an election-related cyber incident

2. A process for coordinating multistate communications decision-making, including spokespeople and communications messages

Additional communications response materials, including a sample escalation process and scenario-planning materials, are available to election officials and can be obtained upon request from the National Association of Secretaries of State, the National Association of State Election Directors, or the U.S. Election Assistance Commission.

# Strategy, Mission, and Objectives

The potential for cyberattacks on our elections systems is an unfortunate reality of our time. Election officials should recognize, and plan for, a possible incident. **The primary objective of this communications guide is to enable the EI-GCC to help election officials maintain public confidence in the integrity of the U.S. election system** in the event of cyber incidents both locally and crossing state boundaries.

Election officials from both parties and at all levels of government agree that there is a shared national interest in preserving the public trust in our election system.

A central component of maintaining trust is providing the public with timely and accurate information. Equally important is dispelling inaccurate information as quickly as possible, especially in today's perpetual cycle of traditional and social media coverage.

Maintaining public trust is most effectively accomplished when election officials—across parties and jurisdictions—speak with one coordinated voice. If federal officials are contradicting state leaders, as occurred in 2016, the public is left confused and it can become all the more difficult to maintain confidence in the election process. Likewise, if federal, state, or local officials are contradicting one another, it is counterproductive and confusing to the public. For these reasons, EI-GCC will play a crucial role in coordinating the response.

All public statements should demonstrate the incident is being handled competently. Any specifics that are provided should be limited only to those that will not change. The scope of the incident, for example, is likely to shift and shouldn't be discussed publicly at the outset. Modifying your story can undermine confidence in the management of the incident and the election system itself.

To institutionalize a means to maintain public trust, **the communications response strategy underlying this Guide coordinates communications messages and delivery among election officials in a multistate cyber incident** to ensure consistency and accuracy of public information. To enable a unified response, we provide communications best practices and coordination processes.

Elections are governed at the state and local level, and there is a national interest in maintaining the integrity of, and confidence in, our elections system. So it is important to have a process that will enable officials from all levels of government to: obtain and analyze the information; decide who will speak about the national implications of the incident; and provide information and communications to all elections officials, so they can communicate accurately, dispel rumors, and reinforce coordinated messages.

Beyond the coordinated multistate process outlined in this Guide, election officials at all levels of government should take measures to prepare for a cyber incident.

## Among the steps you can take immediately are:

- **Establish (or update) a state or local communications response plan** to an election-related cyber incident. For a template state or local cyber communications plan please see the Election Cyber Incident Communications Plan Template.
- **Ensure that the communications plan is aligned** with the corresponding technical response plan, and that both are regularly updated.
- **Test those plans** with simulations.
- **Obtain regular updates** on cyber threats, particularly as they relate to elections.
- **Maintain relationships with officials** who will be relevant to coordinating a response to any cyber incident, including federal officials at the local level and other local community leaders.
- **Coordinate with political parties.** It is much easier to agree to protocols for sharing information about and responding to a cyber incident before the incident and before an election.
- **Educate the public about the work you are doing.** Set the expectation that there will likely be some cyber threat activity during an election and explain how that activity differs from what would be required to interrupt the elections process.

It is important to update and exercise communications response plans frequently—at least every year—to familiarize new players with the process and ensure you apply lessons learned from past experiences and exercises.

# Establishing a Cyber Education Baseline

The public needs to understand the steps state elections officials are taking to counter cyber threats, as well as how difficult it is to execute a cyberattack that will disrupt an election outcome. If the public, and the media, understand the "new-normal," baseline activity of cyber threats targeting elections, they will be less likely to worry unnecessarily about news of small-scale election-related cyber incidents. If you don't have to spend considerable time allaying concerns over inconsequential incidents, you can focus your attention on the consequential ones.

**The main point to make is that cyberattacks are now an issue all election officials must contend with, and the states have taken, and continue to take, steps to mitigate those threats**. However, not every attempt is successful, and even successful ones are very unlikely to impact the outcome of an election.

### Communications in a cyber crisis are most effective when the public has a baseline understanding of:

- The continuing work at all levels of government to counter that malicious activity and try to ensure it does not escalate to a major cyber incident
- The nature of the election data your agency holds, most or all of which is public data
- The malicious, but inconsequential, cyber activity that takes place regularly

**We recommend that the EI-GCC consider taking on some of this public education role, which would address issues that extend across the states**. The council is in a strong position to draw on data from across the country and across levels of government about both threats and actions being taken to enhance the cyber defenses of election systems. For this reason, we suggest that it consider publishing an annual report on the state of election cybersecurity.

The EI-GCC, perhaps in concert with the relevant associations and Information Sharing and Analysis Centers, could provide a regular cadence of cyber threat information, so the public understands how frequently attempts are made by a range of cyber threat actors to target election infrastructure. Making this information common knowledge will mitigate the tendency to treat every reported attempted attack as a reason to question the election system.

The type of information you may want to share could include statements such as: "Based on threat information from the Department of Homeland Security and the Federal Bureau of Investigation (or state/local law enforcement), we are taking the following steps to address and mitigate these threats." If appropriate, this effort could take the form of regular background briefings for the media, as well as online materials and public panels or other educational events for other key stakeholders. The EI-GCC could also consider a joint public panel or forum with representatives of both political parties to discuss measures states are taking to mitigate cyberattacks.

The EI-GCC should also consider sharing limited, aggregate information on successful attacks once they have been addressed, which would establish the EI-GCC as a valuable resource for this type of information.

You should couple the cyber threat data with information on the actions states and localities are taking to strengthen the cyber defenses of election systems. This information should be specific enough to be credible while not being so detailed as to undermine your defenses. Work closely with information security and legal experts to strike the right balance.

We discuss how to establish a communications baseline in more detail in the section on communications process on Page 15.

# Cyber Crisis Communications Best Practices

**Election-related incidents fall broadly into five categories:**

- Online rumors that seek to undermine confidence in an election
- Reconnaissance of election-related systems
- Theft of voter or other election data
- Data manipulation that could affect an election outcome
- Data destruction

The top priority in a cyber crisis will be to maintain public trust. The most effective way to achieve that goal is to respond confidently and quickly. To do this, the EI-GCC will need to prepare, train for, and test its response ahead of time—especially because it is a new organization.

## Planning Ahead

| Near-term Planning | Longer-term Planning |
|---|---|
| • **Determine internal roles and responsibilities**. Make sure there is a clear escalation process for the EI-GCC and the right teams are talking to each other in the event of a cyber incident. Make an individual responsible for ensuring that this process is established and updated.<br>• **Assess the current crisis communications plan** and analyze communications gaps and weaknesses.<br>• **Plan your response to a cyber crisis in advance** with a communications plan, including a decision-making protocol and communications materials.<br>• **Ensure that cyber incident response is part of the operational continuity plan**. Make sure there is a backup communications plan and system in place. | • **Conduct crisis simulation and table-top exercises**, coordinated with legal, technical, and outside advisors, including key senior leaders from multiple states, counties, coordinating bodies, and the federal government.<br>• **Conduct stakeholder mapping and a risk analysis** to understand risks to trust in the election system, priority stakeholders, and how to reach stakeholders to address key concerns. Pay particular attention to outreach to voters and political parties.<br>• **Educate the media** through background meetings and public events on the resiliency of the election system, and the current work to mitigate cyber threats.<br>• **Educate the public** through online channels and public events on the resiliency of the election system and the current work to mitigate cyber threats. |

# Communications Response

## Best Practices

**Be transparent but careful.** Transparent communication builds trust, but in a cyber incident, you will have few facts at hand, especially at the outset. 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 don't 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.** To demonstrate that you are taking the issue seriously, you should talk about the steps you are taking to protect voter information and address any broader risks to the system.

**Provide context.** In an election-system incident, there will be a temptation for public speculation. Counter speculation with facts and context to reduce the risk of undermining public trust. Include metrics whenever possible.

**Be visual**. Cybersecurity can be challenging to understand depending on a person's technical background. The quickest way to get your message out is to pair it with a graphic. 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**. Use social media to dispel rumors. 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 misinformation and inaccuracies.

**Learn from the incident.** Use your and others' experiences to improve your cybersecurity practices and crisis plans.

## Guidelines for Communicating with the Public

**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.

**Demonstrate transparency by communicating with the public on a regular basis.** Establish a regular series of 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.

## Best Practices for Countering Misinformation

**Establish the facts, and double-check them**. You need to ensure that you are operating from a factual position before countering misinformation, so check your facts with multiple sources before citing them publicly. Ask all appropriate questions and put in the work before you speak to be certain that you do not accidentally provide misleading information.

**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.** Misinformation can spread rapidly through social media and broadcast commentary. 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. Demonstrating transparency can help to counter false claims. Opportunities to demonstrate transparency could include inviting reporters "behind the scenes" at a polling place.

**Engage on all platforms.** Misinformation can spread across multiple platforms, including social media and traditional media. To counter misinformation, deliver a clear, factual message on all available platforms.

**Avoid repeating misinformation.** 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.

# Communications Process

Maintaining a coordinated process is critical to effective and efficient communications planning and response to a cyber-related incident. For an incident affecting multiple states, this coordinated communications process outlines:

- Key stakeholders
- Phased planning and response
- Coordination functions
- Feedback loop to incorporate lessons learned

In this communications process, we assume that information and messaging coordination functions will be performed by cross-jurisdictional organizations that have played a similar role in past crises. Further, we recommend that new coordinating functions and mechanisms be created to execute information-sharing and communications.

We recommend that the EI-GCC—with support from other interested parties, such as the National Association of Secretaries of State (NASS), International Association of Government Officials (IGO), the U.S. Election Assistance Commission (EAC), the National Association of State Election Directors (NASED), and the National Governors Association (NGA)—establish a Cybersecurity Communications Response Group (CCRG).

This newly formed entity will provide the EI-GCC and its stakeholders with a communications coordination function that currently does not exist, allowing for collaborative, coordinated public message planning and execution if and when it is needed in the future.

## Phase 1: Baseline Communications Activities

On a regular basis, the CCRG will provide updates to the public and other key stakeholders on current cyber threats and actions being taken to counter them. These baseline updates, whether part of a regular cadence or spurred by suspected nefarious activity, should be developed and coordinated with the expectation that they will be made public. Audiences and stakeholders are catalogued below with recommendations for actions that can be taken now to establish or maintain relationships with them.

Communicating with these groups on a regular basis, before something happens, is key to setting a baseline with critical audiences so that there is a level of understanding around the issue that allows mutual alignment on escalation and coordinated response. In order to provide this ongoing education, we recommend communicating early and often, in addition to when moments of interest (i.e., elections) arise. This baseline work could take the form of behind-the-scenes demonstrations and briefings for your audiences.

**Stakeholders may include:**

**State / Local Comms. Counterparts**

**Law Enforcement**

**Federal / State Lawmakers**

**Media**

**Interested Parties**

**State and Local Communications Counterparts:** Knowing your state and local counterparts is key to the planning and response actions discussed in later phases. The EI-GCC should maintain a "living list" of communications officials and accurate contact information, so these individuals can be reached on short notice for incident coordination and planning.

**Law Enforcement:** In the event of a cyber incident, federal, state, and/or local law enforcement will be involved in the response. Creating and maintaining relationships with key law enforcement officials and associated communicators in law enforcement agencies ensures more seamless coordination and information-sharing before, during, and after an incident.

**Federal/State Lawmakers:** Federal and state lawmakers play an important role in authorizing and overseeing election and cybersecurity measures. They also are likely to speak publicly about an election-related cyber incident, so communication with them is critical before, during, and after an incident. Not only are lawmakers beneficiaries of a safe and secure elections system, but they have a vested interest in maintaining the public's trust in that system. Communicators should build relationships with key figures in Congress and statehouses, including their respective communications staffs, in advance.

**Media:** The media is a key information conduit to voters, providing news and commentary that shapes and defines public opinion and a belief in the election system's integrity. Establishing ongoing relationships with key reporters who cover both cybersecurity and election-related issues at the national, state, and local level will be important in shaping accurate coverage throughout all phases of cyber-related preparation and response.
You should focus on two categories of media:

- **Traditional Media—**Mainstream outlets and reporters;
- **Influencer Media—**This category includes influential bloggers, outlets, and commentators, as well as outlets likely to reach them.

**Interested Parties**: You should develop relationships with voting advocacy and other third-party groups, because they play a role in maintaining the public's confidence in elections. Political parties an campaigns are a critical group with which you should develop a trusted relationship in advance. Third-party groups may also include vendors, researchers specializing in elections, technology service providers, or other industry service providers. We recommend as a next step that the CCRG develop an initial list of key groups, which should be maintained and updated by the team lead.
This list could include:

- **Political Parties and Campaigns**
- **Election Groups**
- **Think Tanks**
- **Academics**

# Phase 2: Communications Planning, Activation, and Coordination

Cyber-related incidents rely on evolving investigations, making their scope and impact difficult to understand, particularly at the outset. This can make communications decision-making, coordination, and messaging even more important for reducing confusion.

Some incidents may be discovered as an attack or breach occurs, while most tend to be discovered after the fact—often after significant time has passed. The key to an effective response is not just coordination but also knowing with whom to coordinate. In any response, there are likely to be multiple voices speaking publicly, at both the national or field level.

In this phase, we assume an anomalous event has been identified, which activates a communications coordination scheme. It may be detected by a range of entities, such as a security researcher, state/local election official, law enforcement, or media.

When an incident occurs, many representatives from a variety of organizations will become involved. The section below outlines resources, coordination mechanisms, lines of coordination, and a checklist to be used in response to, or in advance of, a cyber-related incident.

## Assembling Key Players

***Note:*** *The U.S. Federal Government's National Response Framework outlines public information as an Emergency Support Function (ESF) and includes a framework for public information coordination and action around incidents that involve, or may involve, federal response. This process aligns with the ESF #15 Standard Operating Procedure.*

**CCRG Roles & Responsibilities:** The CCRG should establish the following roles for responding to a multistate cyber incident. These individual roles can be filled by specific people from a variety of interested parties, which may include, but are not limited to, NASS, NASED, IGO, EAC, and NGA.

Please note that as the EI-GCC builds on this Guide, updates should include a table with these roles assigned to individuals, along with their contact information.

**Communications Director**–On behalf of the EI-GCC, oversees the functional coordination resources, processes, and staff. Is responsible for overall operational direction and communications messaging development in cooperation and coordination with EI-GCC and interested parties. The communications director position can be filled by different people on a rotating basis; for example, the EI-GCC could designate a communications director to stand duty quarterly. The role should be filled by a senior communicator from the EI-GCC participants or other interested parties and have the relevant management, crisis, and media operations experience to understand not only their role but also the other roles outlined as part of the CCRG.

**Affected Community Communications Representatives**–Usually senior communicators from affected state or local jurisdictions representing a "field" perspective and providing relevant incident-related information to the coordination process. This may include a communicator from the governor's office and/or communicators from state and/or local elections offices.

**Media Operations Director**–Responsible for communication with reporters and for media monitoring on behalf of a multi-state communications coordinating body. Oversees near-term, "24-hour" communication operations, i.e., execution of communication plans.

**Social Media Director**–Responsible for online communications via ESCC web platforms, as well as coordination with interested parties' digital media teams in order to promote and cross-promote content.

**Communication Plans Director**–Responsible for forward-looking communication plans beyond the immediate "24-hour" period.

**Congressional/Inter-governmental Affairs Liaison**–Responsible for coordinating congressional/governmental briefings for members of Congress, state legislatures, or other elected officials with communications staff. Coordinate through the Affected Community Communications Representative, who is likely to be a member of the ESCC or interested parties' government affairs team.

**Law Enforcement Affairs Liaison**–Responsible for coordinating communications information with law enforcement and affiliated communicators.

**Technical Liaison**–Responsible for being the conduit of technical information between operational and communications teams. Ensures accuracy of technical data being released by communications team and serves as subject-matter expert for all such information.

**Activation of the CCRG:** The CCRG, while regularly communicating in Phase 1 during baseline operations, should plan for and exercise the activation of the CCRG in a crisis. Activation of the CCRG would be at the discretion of the Communications Director, with input from operational leads in response to a verified or potential incident. Additional information on the escalation process is in the Appendix available to election officials and can be obtained upon request from NASS, NASED, or the EAC

Generally speaking, this activation would be executed via a blast email to CCRG members with shareable background information on the incident, direction on the use of coordination mechanisms (discussed below), and next steps. For example, on discovery of a potential incident, the Communications Director would activate the CCRG by hosting an Election Sector Incident Communications Coordination Line call regarding the incident, thereby beginning the communications coordination process.

**Election Sector Incident Communications Coordination Line (ESICCL):** This bridge line is a standing conference call line that can be created to use for coordination before, during, or after a cyber-related incident. The CCRG will maintain a list of relevant contacts from federal, state, and local election offices in order to invite relevant parties to a call, should it be necessary. This resource does not currently exist and it would be incumbent upon the CCRG to coordinate the creation of this standing line at the outset.

**Election Sector Information Center (ESIC):** In the event of a multistate event, the CCRG should create a specific Information Center where communications activity is planned, coordinated, and executed real-time. This should include all the roles above and can reside in one physical location or it could be done virtually through online means. An ESIC would be the functional nerve center of all communications-related activity.

## Using the Election Sector Incident Communications Coordination Line (ESICCL)

As the standing conference call line for election sector cyber-related incidents, the ESICCL can be a key coordination mechanism for communicators to share both operational data, as well as coordinate messaging and communications-related activity.

Upon the activation of the CCRG, the Communications Director will stand up the ESICCL and distribute the time and conference line to invited participants for an initial conference call. This call could include representatives from affected communities, as well as the CCRG roles listed above and any other CCRG participants or outside advisors with relevant subject-matter expertise.

The call agenda can follow a regular rhythm:

- Roll call
- Opening remarks by Communications Director for CCRG
- Brief operations summary (on-scene reps or operations)
- Summary of major communications plans and events
- Invitee comments
- Messaging coordination requirements outlined by EI-GCC Representative
- Conclusion and next steps

## Standing up the ESIC

Should an event rise to the level where ongoing, real-time coordinated public information flow is necessary, the CRCG could stand up either an in-person or virtual ESIC where personnel could work together.

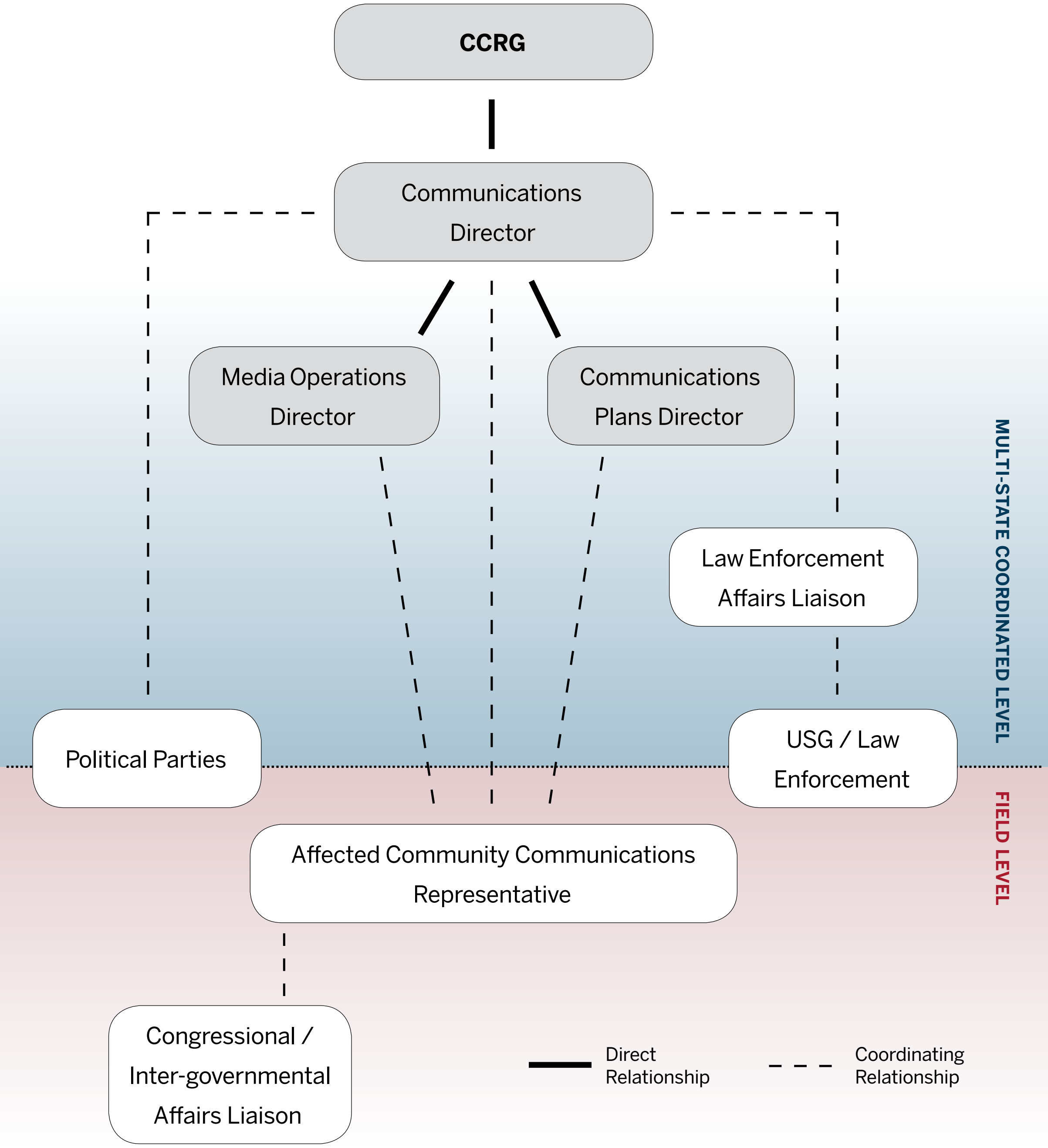
The ESIC would be stood up by the Communications Director, who would make a determination as to the critical personnel needed, as well as the location/online.

The CRCG, as part of steady-state planning, should identify both likely and convenient physical locations where an ESIC could reside should it be needed, as well as functional online collaboration tools to use in the event of a remote ESIC. In general, it is advisable to co-locate the ESIC with any space that is being used to coordinate operational response activity.

## Current Coordination Processes

Should there be current coordination processes that are effective in sharing information, such as regular calls or email listservs, continue to use them–particularly prior to, or during the beginning phases of, activation. However, the scope and volume of an incident may make more direct communications, such as via the ESICCL or ESIC, more useful.

### Lines of Coordination

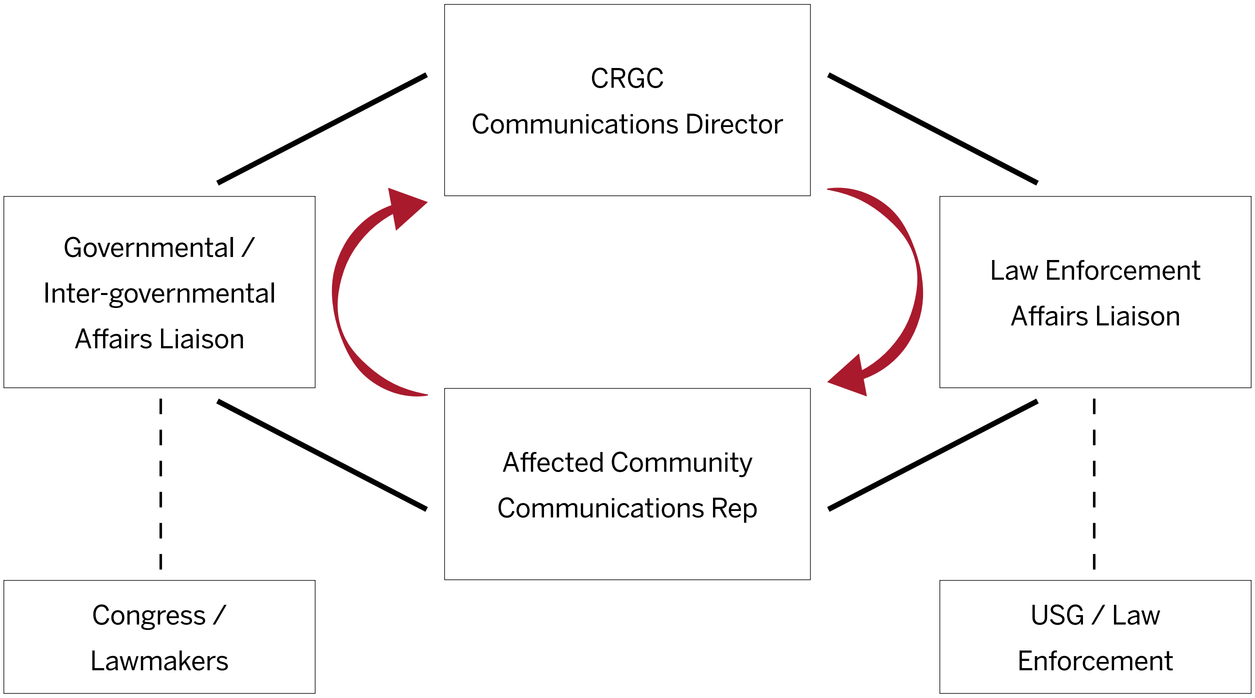

CCRG
Communications Director
Media Operations Director
Communications Plans Director
Law Enforcement Affairs Liaison
Political Parties
USG / Law Enforcement
Affected Community Communications Representative
Congressional / Inter-governmental Affairs Liaison
MULTI-STATE COORDINATED LEVEL
FIELD LEVEL
Direct Relationship
Coordinating Relationship

# Phase 3: Message/Document Drafting, Coordination, and Distribution

## Message/Document Drafting and Coordination

It is best to have some communications materials ahead of time; however, every incident is different and depends on a range of factors, so communicators will oftentimes have to adapt on the fly.

Messaging will need to be adapted, drafted, coordinated, and distributed quickly in order to effectively respond. In addition to the coordination resources, mechanisms, and processes described above, the diagram below shows how that loop may work practically, in and among the various parties who will be speaking publicly.

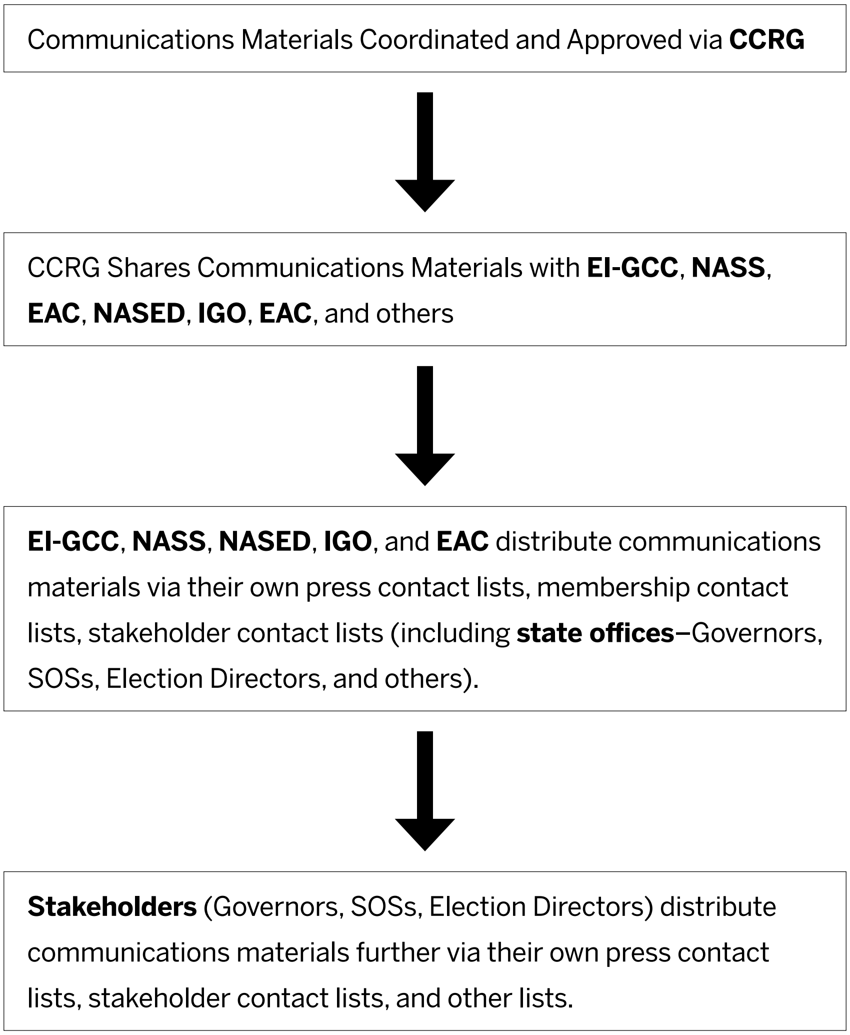

CRGC
Communications Director
Governmental / Inter-governmental Affairs Liaison
Law Enforcement Affairs Liaison
Affected Community Communications Rep
Congress / Lawmakers
USG / Law Enforcement

The CCRG staff will not necessarily retain authority to approve messages emanating from affected communities' communications staffs, nor vice versa; however, the CCRG staff can provide message guidance when needed or warranted. In addition, key inputs should be sought from Congressional/Inter-governmental Affairs and Law Enforcement Liaisons, and approval authority can be retained by those communicators with whom these liaisons work at their home agencies or organizations.

## Distribution

Distribution of approved communications materials to the public and other stakeholders should leverage, and mirror, existing processes to the degree possible. The CCRG, by virtue of its makeup, with communications professionals from a variety of relevant organizations, should coordinate the messaging, but largely leave distribution to the organizational members.

A sample distribution process is illustrated below:



Communications Materials Coordinated and Approved via **CCRG**

CCRG Shares Communications Materials with **EI-GCC**, **NASS**, **EAC**, **NASED**, **IGO**, **EAC**, and others

**EI-GCC**, **NASS**, **NASED**, **IGO**, and **EAC** distribute communications materials via their own press contact lists, membership contact lists, stakeholder contact lists (including **state offices**–Governors, SOSs, Election Directors, and others).

**Stakeholders** (Governors, SOSs, Election Directors) distribute communications materials further via their own press contact lists, stakeholder contact lists, and other lists.

# Phase 4: Evaluation and Feedback

Incorporating both real-time evaluation and feedback, as well as post-incident after-action reviews into your response is critical to both the response you are currently managing, and capturing lessons learned for the future.

## Real-Time Evaluation

While capabilities and resources may differ greatly among affected communities, the CCRG could augment these by providing services that can assist the holistic communications response, including:

**Media Monitoring**–It is critical to understand how the media tone is shaping up. Media monitoring should be compiled at least daily, providing insight on tone and volume and identifying areas for further concentration or strategic/tactical communications changes.

**Social Media Analysis**–Similar to traditional media monitoring, social media listening tools and analysis can provide key insight into which messengers are driving conversation about the incident, as well as how voters are reacting to news and sharing information.

**Call Center Analysis**–If the affected community has a voter call center, it is important to track and analyze the questions and comments received. This information can be a key indicator of misinformation or provide insight into where efforts need to be expanded to get accurate information to voters.

**Polling/Public Opinion Research**–In order to gain more in-depth insights, polling or public opinion research can do much in terms of uncovering voter reactions to an election-related cyber incident, helping shape near and longer-term strategy.

## After-Action Review and Report

Once an incident has concluded, it is important to review communications-related activities, discuss what worked and didn't work, and document those lessons to be incorporated into both steady-state and crisis planning.

Many of the coordination resources and mechanisms described above can be adapted for this purpose, for example the ESICCL call. The after-action process should analyze the incident from start to finish, examining the Plan-Prepare-Respond-Recover communications lifecycle of that incident.

### Your after-action report should include:

- A summary of the incident;
- an overview of the operational response;
- the communications objectives;
- and by phase, with specificity:
  - concern
  - outcome
  - recommendations

This after-action process will assist in building your communications response capability and coordination in a resilient process that can be more effectively utilized when facing future incidents.

# Communications Coordination and Response Checklist

This checklist will help guide actions prior to, and through, the first several days of a multi-state election-related cyber incident.

There are five lists:

- 🟦 **Before a cyber crisis**
- 🟥 **Before a cyber crisis becomes public**
- 🟨 **Multistate Election-Related Cyber Incident Assessment & Activation**
- 🟧 **Coordination/Communications Outreach**
- 🟩 **Products**

## 🟦 Before a cyber crisis

- □ Identify office protocol and a crisis communications team. (Should include IT).
- □ Create a list of terms with common nomenclature for use by all stakeholders.
- □ Set an internal communication plan with elections staff. (How often, when, and where will all staff meet? Information must travel up and down the chain of command with clear boundaries for disseminating information and interfacing with the public/media.)
- □ Ensure that all stakeholders can be reached in a crisis without access to networks or smart phones.
- □ Craft communications materials that can be used in a potential cyber incident. (For examples, elections officials may request sample materials from NASS, NASED, or the EAC.)
- □ Ensure that staff understand their role in a cyber incident. For those who do not have a specific role, ensure they understand why their work matters to the outside world and how they can continue doing their jobs while designated managers handle the cyber incident.
- □ Ensure that communications plans can be accessed and are regularly updated.

## Before a cyber crisis becomes public

□ Obtain technical briefing. (Assess and verify all information.)

□ Decide whether to activate CCRG.

□ Decide whether website can remain online. If you must disable it, launch a microsite (hosted on a different network) in its place.

□ If email is potentially compromised, use an outside communications channel.

□ Consult authorities, if needed.

□ Meet internally in war room; set internal communication schedule.

□ Determine CCRG roles and responsibilities, if you have not done so already.

□ Assess stakeholders.

□ Determine broad communications strategy.

□ Prepare holding statement.

□ Develop communications plan.

□ Draft additional communications required to execute plan, including a communications rollout plan (includes communication with media, stakeholders, and employees).

□ Establish plan for traditional and social media monitoring.

□ Establish media response protocol.

□ Notify affected employees, if necessary. It may be that only a small group of employees are informed initially. Communicate internally, as needed.

□ Notify stakeholders (See list on reverse page), if appropriate, and galvanize support.

## Multistate Election-Related Cyber Incident Assessment & Activation

□ Notification to, and activation by CRCG, of a cyber-related incident or threat.

□ Situation Assessment/Escalation.

   □ **High-Intensity Incident**: Cyber-related incident that triggers reporting obligations, or one that is highly visible requiring response.

   □ **Medium-Intensity Incident**: Cyber-related incident resulting in the loss or compromise of the data or systems, but no formal reporting obligations are triggered. There may be some awareness of the incident, however, spurring proactive communication.

   □ **Low-Intensity Incident**: Cyber-related incident resulting in minor disruptions that may not be visible to public.

□ If Major or Moderate, Media Operations Director and Communication Plans Director identified by Communications Director.

□ Additional Relevant Personnel identified.

□ Contact information for Relevant Personnel distributed.

□ CRCG designates spokesperson, if applicable.

□ Depending on assessment of situation, key messages determined based on specific scenario.

## Coordination/Communications Outreach

- □ Communications Director activates ESICCL call.
- □ Incident Overview.
- □ Affected Communities Communications Representative Update.
- □ Initial Response Communications Plan.
  - □ Designate spokesperson based on type of incident, geography(ies) affected, and scope. In a Major Incident, the spokesperson role may include several people including a EI-GCC representative as well as an Affected Community spokesperson as well to share information at both a field and national level. In a Minor Incident, a single spokesperson may suffice, i.e. an Affected Community spokesperson.
  - □ Prep designated spokesperson for media engagement. This includes review of relevant facts and messaging as well as a peer review session, known as a "murder-board."
- □ Congressional/Inter-governmental Affairs Update.
- □ Congressional/Inter-governmental Affairs activity and plans.
- □ Law Enforcement Liaison Update.
- □ Law Enforcement Liaison activity and plans.
- □ Messaging Coordination outlined by Communications Director.
- □ Battle Rhythm (Daily Schedule).
- □ Conclusion & Next Steps.
- □ Communications Distribution & Rollout.
- □ ESIC activation, if necessary.

## Products

□ Staffing Plan with updates for Communications Director.

□ Battle Rhythm (Daily Schedule).

□ Staffing Matrix and Organization Chart.

□ Communications Plan.

□ Advisories.

□ Press Releases.

□ Traditional and Social Media Monitoring Reports.

□ Regular/Daily update on response activities.

□ Blog and Social Listening Updates.

□ Talking Points.

□ Website updates.

□ Congressional/Inter-governmental Advisories, fact sheets, operations reports and briefing materials.

□ Daily Communication Summary to include next day activity plans.

# Conclusion

As we head into the next election cycle, we hope that this Guide provides additional tools to help the EI-GCC, and by extension election officials across the country, prepare for, and manage, this emerging and evolving cyber risk. As with all communications plans, we recommend that this one be regularly updated by the EI-GCC, as the council further develops and defines its role.

More information is available on different types of communications materials for responding to a cyber incident. Election officials seeking examples of these additional materials can request the communications materials appendix to this document from NASS, NASED, or the EAC.

## Do you see a way to make this Playbook better?

Are there new technologies or vulnerabilities we should address?

**We want your feedback.**

Please share your ideas, stories, and comments on Twitter @d3p using the hashtag #electionplaybook 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**