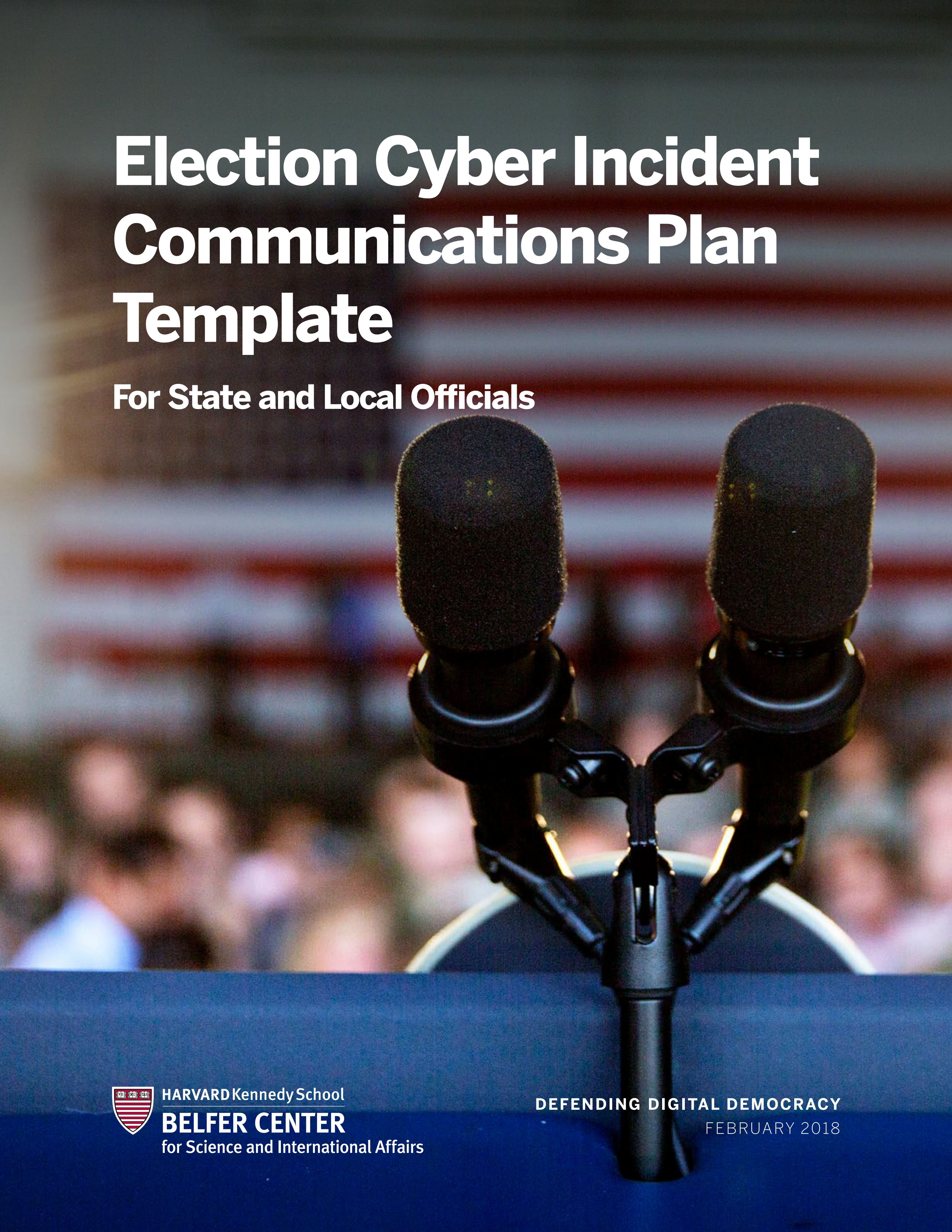


Election Cyber Incident Communications Plan Template

For State and Local Officials

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: Microphones sit on a podium following Vice President Mike Pence's speech at an event at Dobbins Air Reserve Base in Marietta, Ga., Friday, June 9, 2017.
(AP Photo/David Goldman)

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

DEFENDING DIGITAL DEMOCRACY
FEBRUARY 2018

Election Cyber Incident Communications Plan Template

For State and Local Officials

Contents

Defending Digital Democracy: 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 Communications Plan Template.

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 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 state and local officials' request for guidance on how to communicate in a cyber crisis, because they saw cybersecurity issues as unfamiliar territory. They asked specifically for help with developing a communications plan for a potential cyber incident in their jurisdiction.

This Plan Template document is primarily intended for use by state and local election officials as a basis for developing their own communications response plans, which include best practices for use in an election cyber incident. We are releasing the Template publicly, because election officials are among those best prepared and always looking for industry best practices, as well as practical checklists. This template will aid in that effort.

We hope this Plan Template becomes a starting point for state and local election officials to prepare for 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**, who led the project and who, in addition to **Shannon Cortez**, wrote this plan.

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

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

Meredith Davis Tavera, D3P, Harvard Kennedy School

Karen Ejiofor, Staff Assistant, Belfer Center

Chris Farley, Associate, Albright Stonebridge Group

David Forsey, Policy Analyst, National Governors Association

Siobhan Gorman, Director, Brunswick Group

Eben Kaplan, Principal Consultant, CrowdStrike

Jane Khodos, Senior Director, Communications and Content, FS-ISAC

Matthew Masterson, Commissioner, Election Assistance Commission

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

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

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

Executive Summary and Purpose

A cyber incident can span a wide spectrum of malicious cyber activity, and for the elections system, it could range from theft of voter registration data to disruption or manipulation of the vote tally. Given the growing cyber threats to elections globally and in the U.S., state and local elections officials are preparing for how to respond in a "cyber incident" on all fronts, including external communications.

To prepare for possible incidents, election officials have requested guidance on how to build their own communications plan for election-related cybersecurity incidents. This document provides a template and guidance to do so.

The potential for cyberattacks on our election system is an unfortunate reality of our time, and officials should recognize, and plan for, a possible incident. There has been growing interest in using cyber means to spy on or disrupt U.S. elections, dating back at least to 2008 and culminating in the high-profile cyber incidents in 2016.

That trend has rightly caused concern for state and local election officials administering and overseeing elections for all levels of government. In future cycles, the efforts to compromise elections may extend to state and local races. Every relevant agency, as part of their overall security strategy, should incorporate a cyber crisis communication plan.

When a cyber incident occurs, elections officials should be generally prepared to manage the crisis, because they have prepared ahead of time for other types of crises, such as a natural disaster. However, there are elements of a cyber incident that require additional preparation, because a cyber crisis is different from other situations in key ways:

> **High Degree of Uncertainty:** You will know very few facts when you first have to communicate about an incident, and you will need to demonstrate you are confidently and competently managing the incident with relatively little information.

> **Well-Sourced Journalism:** The journalists covering the cyber beat know technical and policy issues and are well sourced, so they may learn about details before you do.

> **Cross-Functional Impact:** Cyber incidents require coordination across a range of state agencies that may not normally work together.

Cross-Boundary Implications: Cyber incidents targeting elections systems can have effects that cascade across traditional jurisdictional boundaries.

Potential to Undermine Trust: A cyber incident has the potential to undermine public trust in the U.S. election system, so communicating in a way that avoids creating undue alarm is critical.

The Plan Template that follows outlines key components of a communications plan that state election officials can build out and tailor to the needs of their jurisdiction. It can also be used at the local level, particularly for large counties. This Plan Template is designed to be used in concert with the State and Local Election Cybersecurity Playbook and the Election Cyber Incident Communications Coordination Guide.

The sections that follow are suggestions only and should be retained, amended, or deleted based on the needs of your jurisdiction. The pages that follow will be in a template format, including bracketed text where the name of a jurisdiction, or other jurisdiction or situation-specific details, can be filled in. The template starts with the first component of a plan: how to use this communications plan. It then outlines best practices and key communications processes. An Appendix of additional communications materials is available to elections officials upon request from the National Association of Secretaries of State, the National Association of State Election Directors, or the U.S. Election Assistance Commission.

How to Use this Communications Plan

[STATE / LOCAL JURISDICTION'S] communications plan includes guidelines and template materials to help our election officials respond to an election-related cyber incident quickly and in a coordinated fashion during the first several days of a cybersecurity incident.

While every situation is unique, this plan provides a foundation on which election officials can build an appropriate response that addresses the incident with the goal of maintaining confidence in the election system.

This plan should be owned by one organization and updated at least annually.

Key components include:

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 crisis response, serve as spokesperson, and manage day-to-day crisis communications 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.

Establishing Baseline Communications: It is important to integrate cybersecurity into your jurisdiction's ongoing communication and set a public baseline understanding of the steps your jurisdiction it taking to mitigate exposure to cyber incidents. This section provides an example.

Scenario Planning and Materials: This section will include communications materials that could be used in different scenarios. [Additional 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.]

Cyber Crisis Communications Best Practices

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 lead confidently, election officials need to prepare, train for, and test responses ahead of time. In today's dynamic political and data environment, every official will likely have to respond to a cyber challenge at some point. Whether preparing for a cyber incident or another type of crisis, this plan can assist the state or local election official will develop a well-thought-out plan and response. That response will be central to preserving public trust.

Communications Coordination

Set guidelines for communicating with outside parties in an incident.

Elections officials should create a communications plan that provides escalation thresholds for reporting an incident internally and publicly. The guidelines should address who is responsible for communicating to key external stakeholders, such as the media and law enforcement. It should also spell out the timeframe for these communications and key individuals involved in communications response from the incident response team, such as public affairs, legal, and agency management.

Guidance on escalation decision processes is available Additional communications response materials are available to election officials in the Appendix 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.

Establish connections between the incident response team and communications officers.

Every situation will require collaboration and cooperation of multiple team members and groups. The relationships between, and credibility of, each player is vital to a successful post-incident recovery.

Encourage intra-state, cross-state, or cross-country communication and collaboration.

Key organizations to designate for regular communications include: Election Infrastructure Government Coordinating Council, the National Association of Secretaries of State, the U.S. Election Assistance Commission, the National Association of State Election Directors, the National Governors Association, the Department of Homeland Security, the Federal Bureau of Investigation, and other national organizations. Develop good working relationships between state and county registrars, clerks, and/or auditors.

Planning Ahead

Near-term Planning	Longer-term Planning
• **Determine internal roles and responsibilities.** Make sure there is a clear escalation process within `[JURISDICTION ELECTION AGENCY]` and the right teams are talking to one another in the event of a cyber incident. Designate an individual to be responsible for ensuring that this process is established and updated. • **Assess the current crisis communications plan** and analyze communications gaps and weaknesses. • **Plan your response to a cyber crisis in advance** with a communications plan, including a decision-making protocol and communications materials. • **Ensure 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 across `[JURISDICTION]`. Also consider a multistate drill, including officials from multiple states, counties, coordinated bodies and the federal government. • **Conduct stakeholder mapping and a reputational risk analysis** to understand your cyber risks, priority stakeholders, and how to reach them to address key concerns. • **Educate the media** through background meetings and public events on the resiliency of the election system, and the current work to mitigate cyber threats. • **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.

Coordinate with the Governor's Office beforehand and agree on if/how the Governor's Office should be involved or not. Election officials who want governors to remain silent in a cyber incident should seek agreement from the governor early on.

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 cyber 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 andinaccuracies.

Learn from the incident. Use your and others' experiences to improve your cybersecurity practices and crisis plans. Conduct an after-action briefing to evaluate the response and suggest improvements.

Guidelines for Communicating with the Public

Make your communications about your most important stakeholder—the public. There will be a temptation to discuss the components of the incident. Instead, talk about what you are doing to address public needs or concerns in this specific situation.

Speak plainly. Cybersecurity can be off-putting to nontechnical audiences. Use anecdotes and examples to demystify relevant 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 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 ensure 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 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 the accurate facts and do not repeat the false messages. For example, if rumors circulate that lines at the polls are hours long, avoid saying that rumors of long lines are circulating. Instead, your message should be that lines are short and moving quickly.

State Election Communications Development & Approval Process

Even a rumor of online election meddling can trigger a communications crisis and sow distrust in the elections system. The good news is that much can be done ahead of time to prepare for such a crisis and get everyone on the same page. We cannot stress enough how much time this will save later in trying to determine how to respond.

Maintaining a coordinated process establishes effective and efficient communications planning and response to a cyber-related incident.

The communications process outlines:

- Establishing a Cyber Incident Response Team (CIRT)
- Establishing a Cyber Communications Response Team (CCRT)
- Phased planning and response
- Coordination functions
- Feedback loop to incorporate lessons learned

Establishing a Cyber Incident Response Team

To manage a cyber incident effectively, the overall state response to the incident should integrate communications officials into the process. The following organizational structure will ensure that communications is part of the decision-making process.

Cyber Incident Response Team (CIRT) Organization

Cyber incident response should use, to the degree possible, the processes [JURISDICTION] already has to respond to other elections-related crises. It should make adjustments for the specific differences involving cyber meddling—particularly the key personnel involved and the potential for any incident to become high profile and raise questions about the integrity of the elections process as a whole.

The Chief Election Official and Director of Elections are responsible for consulting and activating [JURISDICTION'S] cyber incident response plan. You should have delegated executives who are backups and can decide whether to activate the plan. Each executive should have the necessary contact information and follow that sequence.

States may be able to suspend, delay, or postpone voting in an emergency situation, which may include a court order, legislative action, or the emergency powers of the Governor. At the local or regional level, lower courts may cancel, postpone, or extend Election Day polling place hours by issuing a court order.

[INSERT HERE JURISDICTION'S POSITION ON OPTIONS THAT APPLY IN THE EVENT THAT A CYBER INCIDENT DISRUPTS THE ELECTION PROCESS OR OUTCOME IN YOUR JURISDICTION.]

This table should be updated regularly as part of the annual plan review.

[Note: the table below represents a starting point and should be adapted to your organizational structure.]

Position	Designated Individual and Contact Information	Designated Backup and Contact Information
Chief Election Official		
Director of Elections		
Communications Director		
Chief Financial Officer		
Chief Information Officer		
Director of Operations and IT		
Human Resources Manager		
Government & Community Relations Director		
Attorney General		

Establishing a Cyber Communications Response Team (CCRT)

Your Cyber Communications Response Team will support your [Director of Communications] assigned to the CIRT. Here are the steps you can take to ensure your Cyber Communications Response Team has the right people at the table.

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.

`[JURISDICTION]` should establish the following roles for responding to a state-level cyber incident:

Note: Counties should adapt accordingly for their structure. Depending on a jurisdiction's organizational structure, you may choose not to include the Chief Election Official, Director of Elections, and Chief Information Officer on the Cyber Communications Response Team.

> **Chief Election Official**—Responsible for coordinating communications information with local elected officials and administrators in `[JURISDICTION]`.

> **Director of Elections**—Responsible for coordinating communication information with local elected officials and administrators in `[JURISDICTION]`.

> **Jurisdiction Local IT Director/CIO**—Responsible for the `[JURISDICTION]` IT systems and the security of the systems.

> **Communications Director**—Oversees the functional coordination resources, processes, and staff for communications in `[JURISDICTION]`. Is responsible for overall operational direction and communications messaging development in cooperation and coordination with key internal and external stakeholders.

> **Affected Local Elections Administrators**—Usually local auditors / clerks or other officials from affected local jurisdictions representing a "field" perspective and providing relevant incident-related information to the coordination process.

> **Media Operations Director**—Responsible for communication with media and media monitoring on behalf of national-level communications coordinating body. Oversees near-term "24-hour" communication operations, i.e., execution of communication plans.

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

Legislative/Inter-Governmental Affairs Liaison—Responsible for coordinating governmental briefings for members of state legislatures, county commissioners or other elected officials. Coordinate through the Communications Director.

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.

Cyber Communications Response Team List

Position	Designated Individual	Designated Backup
[Chief Election Official]		
[Director of Elections]		
[Jurisdiction IT Director/CIO]		
Communications Director		
Affected County Elections Administrators		
Media Operations Director		
Communications Plans Director		
State Homeland Security Advisor		
Legislative/Inter-governmental Affairs Liaison		
Technical Liaison		

> **Incident Communications Coordination Line (ICCL)**: This bridge line is a standing conference call line that can be created for coordination before, during, or after a cyber-related incident. The Communications Response Team will maintain a list of relevant contacts from federal, state, and local election offices (and officers) to invite relevant parties to a call, should it be necessary.
>
> > `[JURISDICTION SHOULD INSERT BRIDGE LINE DETAILS HERE]`

Developing a Response Process

The following steps will guide you as you start up a Cyber Communications Response Team and develop a process for drafting and approving messages.

> **Step 1: Decide on team.** Select the individuals who will fill the roles previously listed. Outline their roles and identify the decisions around messaging and communication that they can make in real time.

> **Step 2: Security alignment.** With your IT or security team, take inventory of your data assets and potential risks, and conduct an impact assessment. You should understand the attacks to which you are most vulnerable. You should also understand how security tactics are tied to the way your elections office manages risk. Your IT team's early monitoring and detection functions should be aligned to the agency's most critical assets, such as elections results servers. Establish who will be the liaison on the IT team to the CCRT.

> **Step 3: Disclosure alignment.** Determine and document exactly what you are obligated to disclose. Develop a decision-making process to assess the public posture—proactive or reactive—you will take in a given situation. Take into account both legal implications and public opinion.

> **Step 4: Stakeholder analysis.** Assess and prioritize your key stakeholders, based on their influence on voters, because public opinion can turn very quickly during a cybersecurity crisis. Establish ongoing relationships with these stakeholders BEFORE a crisis hits. Your stakeholders may include:
>
> > Voters
>
> > Federal, state, and local elections communications counterparts
>
> > Law enforcement

- State and federal lawmakers, including the Governor’s Office
- Media (cybersecurity and election/political beat reporters)
- Political parties and campaigns
- Third-Party advocacy groups

Step 5: Select a spokesperson or spokespeople. Establish ahead of time who will speak for `[JURISDICTION]` in a cyber incident, and make sure that they have received media training. You may choose different spokespeople for different audiences. Your head of IT might be best equipped to post a response on a vendor site or address hardware concerns, while the Chief Election Official, the director of elections, or your Chief Information Security Officer or Public Information Officer might be the best person to speak to the media. Consider factors such as who has the best communication skills, prior experience with the media, authority in the agency, and relationships with stakeholders.

Step 6: Establish a drafting and approval process for key messages and include diagrams of this process in your communications plan. This process will be specific to `[JURISDICTION’S]` Cyber Communications Response Team structure but will likely follow this basic outline, tailored to your organizational structure:

Step 7: Decide what baseline information you can communicate now. Establish a baseline understanding among key stakeholders of `[STATE’s]` work to implement cybersecurity best practices well ahead of the next election. In the event of a cyber incident, this effort will position `[STATE]` to make the case that `[STATE]` has been implementing best practices, but unfortunately cyber incidents do still sometimes occur.

Step 8: Establish a feedback loop. Establish a means—both during and after an incident—to incorporate feedback from voters and other key stakeholders into your response. During an incident, this work could take the form of media and social media monitoring as well as polling. After an incident, you should conduct an after-action report and ensure that lessons learned are incorporated into this Cyber Communications Plan Template Your after-action report should include:

- A summary of the incident (keeping in mind it could be subject to public disclosure);
- an overview of the operational response;
- the communications objectives;
- and by phase, with specificity:
  - concern
  - outcome
  - recommendations

Activation of the Cyber Communications Response Team (CCRT)

Cyber-related incidents vary in size and severity, which makes it important to have a process to ensure the appropriate steps are calibrated to the significance of the incident. All incidents can be categorized under one of the following severity levels:

1. **Low**: Cyber incident that involves no PII and/or minor system disruptions that will likely not be visible to the public or affect the elections process.
2. **Medium**: Cyber incident resulting in the loss or compromise of voter data or VR systems, but formal notification obligations may not be triggered. The issue begins to become public.
3. **High**: Cyber incident that triggers U.S. or international reporting obligations, affects a large amount of voter information, and/or is destructive to election operations.

In a medium-intensity incident, [CHIEF ELECTION OFFICIAL] will need to make a judgment call about whether to activate the CCRT, but if the incident is likely to become public and raise questions about trust in the election systems, [CHIEF ELECTION OFFICIAL] should err on the side of activation. You can always deactivate if the intensity declines. Once activated, [CHIEF ELECTION OFFICIAL] along with [DIRECTOR OF ELECTIONS], will decide which level applies, based on an initial assessment. Once [CHIEF ELECTION OFFICIAL] activates the CCRT, all key response team members will be notified of the activation [INSERT STATE'S METHOD OF REACHING TEAM MEMBERS].

Coordination Mechanisms

Using the Incident Communications Coordination Line (ICCL)

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

Upon activation of the Cyber Communications Response Team, the `[COMMUNICATIONS DIRECTOR]` will stand up the ICCL 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 CCRT roles listed above and any other CCRT participants or outside advisors with relevant subject-matter expertise.

The call agenda can follow a regular rhythm:

- Roll call
- Opening remarks by `[COMMUNICATIONS DIRECTOR]`
- Brief operations summary (on-scene reps or operations)
- Summary of major communications plans and events
- Invitee comments
- Messaging coordination requirements outlined by national-level coordinating body representative
- Conclusion and next steps

If this incident has the potential to escalate to an event that crosses state lines, please contact the Cyber Communications Response Group at the Election Infrastructure Government Coordinating Council. `[INSERT CONTACT DETAILS FOR CCRG REPRESENTATIVE]` More information on the CCRG can be found in the Election Cyber Incident Communications Coordination Guide.

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

Communications Process for a Cyber Incident

If a cyber crisis happens, it will demand its own communications plan. The steps below will help you assess the situation and take basic actions while you develop a more detailed communications plan. Each situation must be fully assessed on its own merits before a particular strategy is executed. The following are general guidelines:

Step 1: Activate the CCRT and obtain a technical briefing from the CIO or technical liaison.

Step 2: Only if absolutely necessary, and in consultation with IT specialists, decide if you need to disable agency website and launch a microsite outside of the agency's network. This will be a decision for `[JURISDICTION ELECTIONS DIRECTOR/LOCAL COUNTY AUDITOR OR CLERK]`. Notify key staff members. If website remains active, a message on the website may need to be posted.

Step 3: If necessary, contact law enforcement or federal authorities.

Step 4: If media are calling or showing up at the office, CCRT responds to reporters. If needed, you can issue a holding statement.
[Additional communications response materials are available to elections officials on request in the appendix to this document 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.]

Step 5: Notify key people: Chief Election Official, State Elections Director, Assistant Election Officials, Deputy Election Officials, IT Team, Communications Team, Elections Team.

Step 6: Inform entire agency of developing crisis, agency response, and agency policies that apply.

Step 7: Inform stakeholders / Legislature / Auditors.

Step 8: If you have not done so already, consider whether you need to inform the media/ public about the incident. Make sure you inform the media only of confirmed facts that you are confident will not change (very few facts will fall into this category).

Step 9: Begin monitoring media coverage.

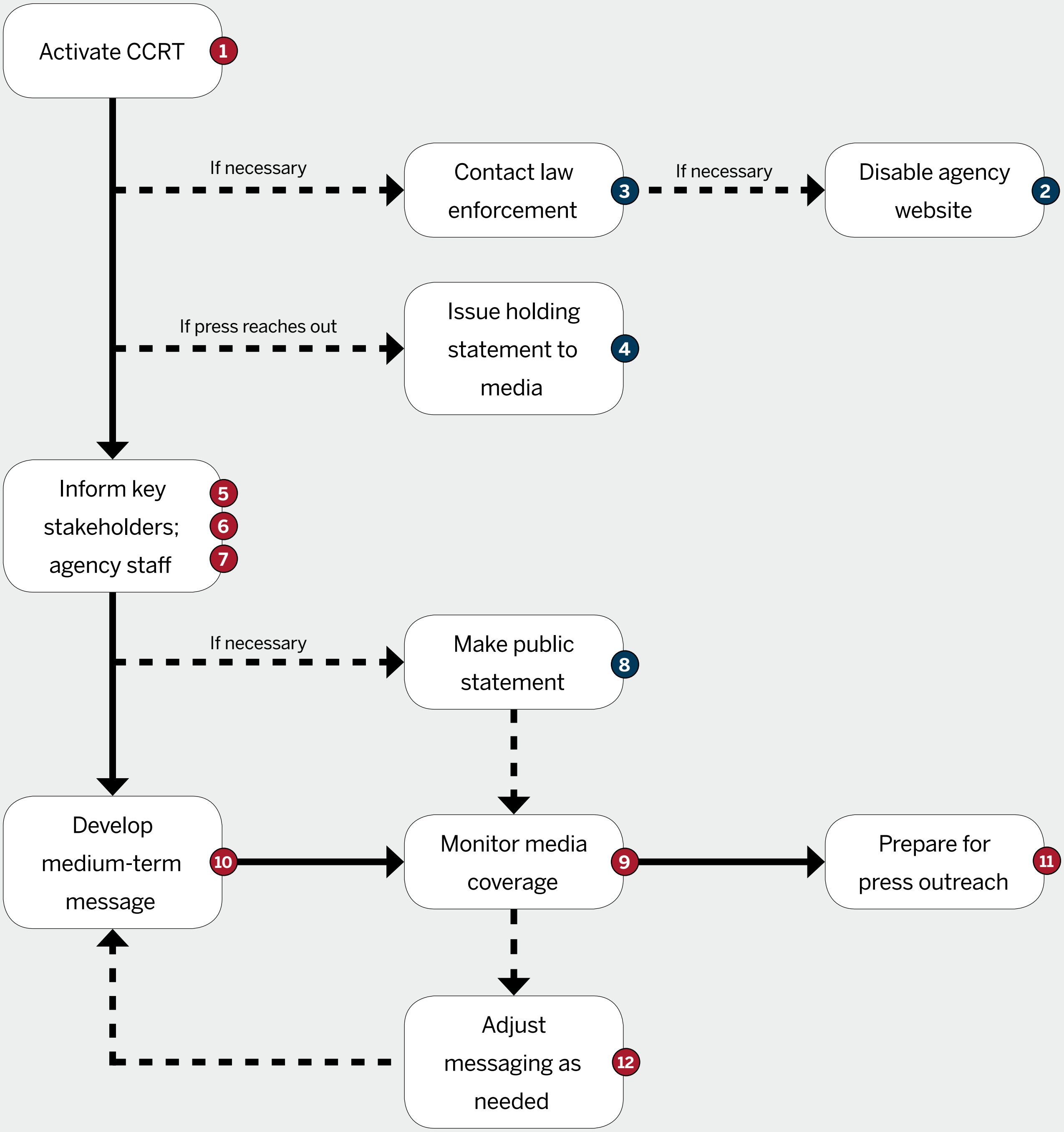
Step 10: Develop medium-term message.

Step 11: Prepare for press outreach/briefing and media schedule.

Step 12: Develop feedback loop from media monitoring or polling and incoming queries from media to determine if you need to recalibrate messages.

Communications Process for a Cyber Incident

Numbers below correspond to steps outlined in prior page



Communications Coordination & Response Checklist

Elections Crisis Communications Checklist

A cyber crisis has the potential to cast a negative light on the `[CHIEF ELECTION OFFICIAL]` or a local county elections office—as well as to undermine faith in the elections system. If you are uncertain whether a situation could escalate into a crisis, err on the side of standing up response teams, because you can always stand down if the incident does not escalate. (Consult `[JURISDICTION'S]`—Continuity of Operations Plan—in crises that impact operations.)

The checklists below can be adapted to your jurisdiction's processes. They provide guidance on actions to be taken in the lead up to, and days following, a cyber incident.

Action: 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 dissemination and interfacing with the public/media.)
- □ Ensure that all stakeholders can be reached in a crisis without access to the `[CHIEF ELECTION OFFICIAL]` network or smart phones.
- □ Craft communications materials that can be used in a potential cyber incident. For examples, elections officials may request sample materials from the National Association of Secretaries of State, the National Association of State Election Directors, or the U.S. Election Assistance Commission.)
- □ Ensure that staff understand their role in a cyber incident. For those who do not have a specific task to carry out, reassure them that their work is important and inform them 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.

Action: Before a cyber crisis becomes public

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

□ Decide whether to activate CCRT.

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

□ 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 [CHIEF ELECTION OFFICIAL] 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 next page), if appropriate, and galvanize support.

Action: Once a cyber crisis becomes public

□ Fact check: Make sure communications materials reflect current facts.

□ Execute rollout plan, including informing media, if appropriate.

□ Determine if microsite/web page is needed.

□ Record an office greeting for phone system, if necessary.

□ Maintain a record of inbound media inquiries and responses.
[ADD BULLETS ON FEEDBACK INFO FORM COVERAGE, CONVERSATIONS WITH REPORTERS AND OTHER DATA ON EXTERNAL REACTION]

□ Begin media (social and traditional) monitoring.

□ Review and revise messaging, as needed, based on feedback.

General Media Inquiries Checklist

Gather basic facts:

□ Story topic/angle/deadline

□ Platform (blog, newspaper, television, radio, etc.) plus request content and images

□ Other potential interview subjects

□ Remember: Only designated spokespeople should speak or provide content.

□ Remember: You have rights when you communicate with journalists, especially when asked about technical details you wouldn't be expected to know. "Let me see what I can find out for you" is always an option for a response. This response may mean that you return to the reporter without any additional information. You are not obligated to provide details.

□ Remember: Reporters are under pressure from their editors and may shift the pressure to you. Do not speculate to fill gaps for them.

Notify key people:

□ Meet internally.

□ Craft media plan. Includes internal plans for staff and stakeholder communications.

- □ Designate key spokespeople and content providers. Assign tasks.
- □ Assist in crafting messaging. Reflect key audiences, people affected now, and those who will be affected in the future.
  - □ Voters
  - □ Counties
  - □ Candidates
  - □ Campaigns
  - □ Media
  - □ Other government offices
  - □ Vendors
  - □ General public
  - □ SOS employees and their families (if necessary)
- □ Demonstrate leadership by describing the steps you are taking to address this cyber incident. Consider contacting stakeholders who may be affected, especially if you think they may dislike or disagree with your messages.

Key Messages for Baseline Communications

You need to set a baseline understanding for the public that your [JURISDICTION] is taking cybersecurity seriously, and integrating best practices throughout the elections process. Below [are a few/is one example/s] of these baseline communications. In addition to a standing website message, develop key messages for [JURISDICTION'S] cyber preparedness activities and integrate them into current web content and future public remarks by [JURISDICTION'S] elections officials.

Below is one example of baseline communications. For your state, add relevant additional communications.

Sample State Website Message Emphasizing Cybersecurity

Note: Counties can modify to fit their jurisdiction.

Welcome to [STATE] State Elections. We are honored to serve you, the voters of [STATE]. Our mission is to ensure accessible, fair, and accurate elections.

Our office facilitates federal, state, and local elections conducted by all [X NUMBER OF] county election departments. We maintain voting equipment and software integrity, provide training and certification for election administrators, and support the statewide voter registration database.

Through educational programs and materials, we help all eligible [STATE] residents register to vote and cast an informed ballot. This website is one of many ways we provide information about [STATE'S] unique election system, our [INSERT DETAIL ON SYSTEM THAT SETS IT APART]. It provides [STATE] voters the power of citizen legislators, and the special services available to military voters, college students, voters with disabilities, and minority language communities.

We're proud that [STATE] is at the forefront of elections by embracing technology and innovation to better serve voters. Some of our achievements include:

[INSERT COMBINATION OF ACCOMPLISHMENTS ON TECHNOLOGY AND SECURITY:]

- Second state to provide online voter registration
- First to provide voter registration via Facebook
- Ranked second for election administration in 2010 by the PEW Election Performance Index
- Annual security audit of election equipment
- Paper backup for electronic voting to provide auditable trail of voting records
- Daily review of change log to identify unusual activity
- One of first states to work with Homeland Security to provide cyber hygiene security scans and risk and vulnerability assessments

[STATE] State Elections is passionate about bringing access and transparency to the elections process. I hope you register and vote in our great state!

[CHIEF ELECTION OFFICIAL OR STATE ELECTIONS DIRECTOR]

Conclusion

As we head into the next election cycle, we hope that this Plan Template provides a running start for elections officials who are seeking to develop a cybersecurity communications response plan. We hope the guidance and format of this template helps officials prepare for, and manage, this emerging and evolving cyber risk to our elections process. As with all communications plans, we recommend that you regularly update your plan to account for changes in agency structures and personnel.

More information is available on the type of information communications materials should include. Election officials seeking examples of additional communications 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 #CyberPlaybook 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