Election Cyber Incident Communications Plan Template

For Political Parties and Campaigns

International Edition

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

DEFENDING DIGITAL DEMOCRACY
MAY 2018

Adapted in partnership with

NDI

IRI International Republican Institute

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

www.belfercenter.org/D3P

International Edition partners:

The National Democratic Institute
www.ndi.org

The International Republican Institute
www.iri.org

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: Adobe Stock

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

DEFENDING DIGITAL DEMOCRACY
MAY 2018

Election Cyber Incident Communications Plan Template

For Political Parties and Campaigns

Contents

Welcome

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 several groups on the frontlines of defending democracy: (1) political campaigns; (2) political parties, (3) election officials, and (4) non-governmental organizations.

Over the past year, we set out to provide campaign, political party, and election professionals with practical guides to the most applicable cybersecurity best practices in advance of the 2018 midterm elections in the United States. In November 2017, we released "The Cybersecurity Campaign Playbook" for campaign professionals. In February 2018, we released a set of three U.S. elections playbooks designed to be used together by U.S.-based election administrators: "The State and Local Election Cybersecurity Playbook," The Election Cyber Incident Communications Coordination Guide," and "The Election Incident Communications Plan Template."

Following the release of those playbooks, we heard from international organizations about the need for similar preparation globally. To respond to this need, we are releasing the "Election Incident Communications Plan Template" for a global audience. Wherever election cybersecurity incidents occur, political parties, campaigns, and others supporting democratic elections should be equipped with the tools to communicate quickly and effectively to maintain confidence in the democratic election system.

D3P is a bipartisan team of cybersecurity and policy experts from the public and private sectors, as well as professionals with deep experience in political campaigns. We collaborated with the International Republican Institute (IRI) and the National Democratic Institute (NDI) to develop a communications response playbook adapted for the international election landscape.

One of the most significant requirements we encountered was a request for guidance on how to communicate in a cyber crisis, because many political parties, campaigns, and other democratic election organizations see cybersecurity issues as unfamiliar territory.

This Template is primarily intended for use by political parties or campaigns as a foundation from which they can develop their own tailored communications response plans, which include best practices, recommended external response processes, and scenarios to anticipate an election cyber incident.

We hope this Template becomes a starting point for political organizations in all countries to prepare for their response to an election cyber incident.

Finally, we would like to thank the political parties, campaigns, election officials, and organizations for whom we wrote this Template and the others in the series. You are the frontline defenders of democracy. We hope this effort helps make that tremendous responsibility a little easier.

Authors and Contributors

This project was a collaboration between the D3P, IRI and NDI. Since their creation in 1983 by an Act of Congress, which established the National Endowment for Democracy, IRI and NDI have responded to the aspirations of people around the world to live in democratic societies that protect basic human rights. The non-partisan Institutes have worked with political parties, civic groups, and parliaments in more than 100 countries to strengthen democratic institutions, safeguard elections, advance citizen engagement, and promote open, accountable government.

This project was made possible by dozens of people who generously volunteered their time. Special thanks are due to Siobhan Gorman, Chris Farley, and Meredith Davis Tavera, who wrote the plan. We would also like to thank Sarah Moulton and Jesper Frant of NDI and John Tomaszewski and Sam LaHood of IRI for working with us to internationalize this Template.

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

DEFENDING DIGITAL DEMOCRACY

Eric Rosenbach, Co-Director, Harvard Kennedy School Belfer Center; Director, Defending Digital Democracy Project

Robby Mook, Co-Director, D3P

Matt Rhoades, Co-Director, D3P

Caitlin Conley, Executive Director, D3P

Meredith Davis Tavera, D3P, Harvard Kennedy School

Mari Dugas, Project Coordinator, Defending Digital Democracy, Harvard Kennedy School Belfer Center

Chris Farley, Associate, Albright Stonebridge Group

Siobhan Gorman, Partner, Brunswick Group, D3P Senior Advisory Group

ADDITIONAL AUTHORS AND CONTRIBUTORS

Steve DiPangrazio, International Republican Institute

Jesper Frant, National Democratic Institute

Sam LaHood, International Republican Institute

Sarah Moulton, National Democratic Institute

John Tomaszewski, International Republican Institute

Frank White, Independent Communications Consultant

BELFER CENTER WEB AND DESIGN TEAM

Arielle Dworkin, Digital Communications Manager, Harvard Kennedy School Belfer Center

Andrew Facini, Publications and Design Coordinator, Harvard Kennedy School Belfer Center

Executive Summary and Purpose

In the last few years, the threats of election meddling through cyber means have escalated and become more diverse—and potentially disruptive—to the voting process. An election-related cyber incident can span a wide spectrum of malicious cyber activity. During a political campaign, it could range from theft of campaign data or malicious actors breaking into a party or candidate's website, to spreading misinformation in an effort to tip an election. The goal is often to undermine trust in, and support for, democratic institutions.

Given the growing cyber threats to elections globally, political parties and campaigns are preparing for ways to respond to a cyber incident on all fronts, including external communications. Effective communications in a cyber incident, demonstrating that the affected organization is managing the incident to preserve the integrity of the election, are critical for maintaining trust in democratic systems.

The primary objective of this document is to enable political parties and campaigns to maintain public confidence in the integrity of their democratic election system in the event of a cyber incident. This document provides a template and guidance for political parties and campaigns to build their own communications plans for election-related cybersecurity incidents. It includes a set of best practices and provides a structure for a communications response playbook that political parties can then build out and tailor to their own country and circumstances.

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 trust is most effectively accomplished when party officials—across affiliations and jurisdictions—speak with one coordinated voice.

The potential for cyber incidents on campaign infrastructure, such as websites, donor and party member databases, and social media accounts, is an unfortunate reality of our time. 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.

At the same time, government officials and civic leaders across Europe have focused on cyber incidents targeting major democratic institutions at least since the widely publicized intrusion into the systems of the German Federal Parliament (the Bundestag) in 2015. Concern mounted into the major election year of 2017, in which both the Netherlands and Norway decided to conduct their national vote counts on paper in case electronic systems were to be disrupted, French presidential candidate Emmanuel Macron's campaign was the "victim of a massive and coordinated hack," and Germany scrambled to protect its systems after incidents targeting think tanks closely associated with the country's two major parties.

That trend has rightly caused concern for political parties and campaigns involved in elections all over the world. In future cycles, the efforts to compromise elections may extend to new countries or involve new tactics. Every political organization, as part of their overall security strategy, should therefore incorporate a cyber crisis communications plan.

That plan should enable party officials to demonstrate confidence as they manage a cyber incident. All public statements should demonstrate that party officials are handling the situation competently. Any specific details they provide should be limited to those that will not change. The scope of the incident, for example, is likely to shift and party officials should not discuss this aspect publicly at the outset. Modifying the story can undermine confidence in the management of the incident and the election system itself.

Further, there are elements of a cyber incident that require special preparation, because a cyber crisis is different from other crises in key ways:

- You will likely know very few facts when you first have to communicate about an incident, and you will need to demonstrate that you are managing the incident confidently and competently with relatively little information.
- Many journalists covering cyber-related stories know technical and policy issues and have a variety of knowledgeable and trusted sources, so they may learn about details before you do.
- Cyber incidents may require coordination across a range of government and non-government institutions that do not normally work together.
- Incidents targeting political campaign infrastructure can have effects that cascade across traditional jurisdictional boundaries.
- A cyber incident has the potential to undermine public trust in a candidate, political party, or even the democratic election system itself. It is important to communicate honestly but in a way that avoids creating undue alarm.

The Template that follows outlines key components of a communications plan that political parties and campaigns can build out and tailor to their needs. This Template is designed to be used together with the **Cybersecurity Campaign Playbook European Edition**.

The sections that follow are suggestions only and should be retained, amended, or deleted based on your needs. **They will be in a template format, including bracketed text to insert the name of your organization or situation-specific details.**

The Template starts with how to use this communications plan. It then outlines best practices, key communications processes, and scenarios against which you can prepare.

Beyond the coordinated communications process outlined in this Template, your party officials should take additional measures to prepare for a cyber incident. Among the steps you can take immediately are:

- Align the communications plan with the technical response plan, and update both regularly.
- Test those plans frequently with simulations at various levels of your party.
- Obtain regular updates on cyber threats, particularly as they relate to elections.
- Maintain relationships with officials and experts who will be relevant to investigating and coordinating a response to any cyber incident.
- Educate the public, where possible, 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 communications response plans frequently—at least every year—to familiarize new players with the process and ensure that you apply lessons learned from your experiences and those of other countries.

How to Use this Communications Plan

[ORGANIZATION's] communications plan includes guidelines and template materials to help us 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 we can build an appropriate response that addresses an incident with the goal of maintaining confidence in the candidate, party, and the electoral process.

[ORGANIZATION] should own this plan exclusively and update it at least annually, especially as new cyber threats evolve and emerge.

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 the crisis response, serve as spokesperson, and manage day-to-day crisis communications during an incident.

Response Checklist: This checklist broadly outlines steps we should take during the first several days after learning about a potential incident.

Establishing Baseline Communications: It is important to communicate the steps we are taking to mitigate exposure to cyber incidents. Doing so will set a public baseline understanding of the risks and the good-faith efforts your organization has made to mitigate them. This section provides an example.

Scenario Planning Guidelines and Materials: This section includes possible scenarios we may face and guidelines for responding to them.
[It also includes communications materials for possible use in different scenarios. PLEASE NOTE THAT YOUR ORGANIZATION WILL NEED TO DEVELOP THESE MATERIALS USING THE GUIDELINES PROVIDED IN THE TEMPLATE.]

Cyber Crisis Communications Best Practices

One of the top priorities during a cyber crisis will be to protect the integrity of the `[campaign [and/or] the party]`. The most effective way to achieve that goal is to respond confidently when the incident has become, or is about to become, public.

To lead confidently, political organizations need to prepare, train for, and test responses in advance. In today's dynamic political and data environment, every organization 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 in developing a well-thought-out plan and response. That response will be central to protecting our `[campaign/party]`.

Communications Coordination

Set guidelines for communicating with outside parties in an incident. Create a communications plan that provides internal and external thresholds for escalating incident reporting. The guidelines should identify the individual or team responsible for communicating to key external stakeholders, such as the media, party members, and law enforcement. They should also provide the timeframe for these communications and key individuals involved in communications response from the incident response team, such as public affairs, legal representatives, and senior leadership or the candidate.

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 inter-party and international communication and collaboration. Where practical, develop and use good working relationships with other political parties and organizations on cybersecurity issues. This could include coordination and sharing of information about external or domestic threats and/or developing codes of conduct or norms regarding the use of stolen information.

Planning Ahead

Near-Term Planning	**Longer-Term Planning**
• Determine internal roles and responsibilities. Make sure there is a clear escalation process within [ORGANIZATION] 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. • Plan your response to a cyber crisis in advance with a communications plan, including a decision-making protocol and communications materials. • Regularly assess the current crisis communications plan and analyze communications gaps and weaknesses. • Ensure cyber incident response is part of your contingency planning. Make sure there is a backup communications system in place in case an incident takes out communications infrastructure.	• Where practical, conduct crisis simulations, coordinated with legal, technical, and outside advisors, including key senior leaders across [ORGANIZATION]. • Prioritize stakeholders in advance and conduct a reputational risk analysis to understand your cyber risks. • Educate internal stakeholders about cyber threats and your organization's planning and response. • Where possible, educate the media and the public through online channels, background meetings, and public events on the resiliency of the political party or campaign, and the current work to mitigate cyber threats.

Communications Response

Responding to a cyber incident can be different in some key ways from responding to other types of crises. When responding publicly to an election-related cyber incident, keep in mind the following best practices:

Communications 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 (i.e., the type or amount of information stolen), so that you do not have to correct yourself later. Avoid speculation on the perpetrator of the incident and always be truthful with the information you do share.

Determine whether and how to coordinate with government authorities. Political organizations that have an adversarial relationship with the current party in power may have special considerations about how to engage with the government. Nonetheless, it is important to understand the government bodies responsible for investigating and prosecuting cybercrimes.

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 campaign or party information and address any broader risks to the system (e.g., how this affects voters or the integrity of the electoral process).

Provide context. In an election-related cyber incident, there will be a temptation for public speculation. Counter this speculation with facts and context to reduce the risk of undermining public trust. Where possible, include context like investigation timelines to demonstrate the seriousness with which you are taking the issue.

Use Third-Party Validators. Using outside experts to investigate and validate your actions will help build credibility with key stakeholders, including the media. Be careful, however, to make sure these experts do not appear to speak for your organization—but rather serve as validators of your efforts.

Use the right tools, both digital and traditional. Use social media to dispel rumors. When a cyber crisis strikes, social media is now a go-to source of immediate information. In practice, this means using it selectively to counter misinformation and inaccuracies. At the same time, it is important to identify alternative means for communication in case the organization's social media accounts or websites are not usable.

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, identify best practices and lessons learned, and suggest improvements.

Guidelines for Communicating with the Public

Focus your communications on your most important stakeholder—the public. Your 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 specific situation.

Speak plainly. Technical cybersecurity terms and processes can be off-putting to non-technical 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 Disinformation

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 communicating too many messages at once and using complex language. You can provide additional nuance later.

Respond quickly. Misinformation can spread rapidly through social media and broadcast commentary. Your counter-message should be ready for dissemination as soon as possible. Designate specific members of your team to manage this process to ensure you are responding as quickly as you can.

Be transparent. Caveated, incomplete, or "no comment" responses can fuel conspiracy theories by making it appear that 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 campaign event. Also, if you do not know something during an interview or public statement, tell the public and journalists that you will get back to them when you have more information.

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. Also, coordinate whenever possible with allies and partners to help spread your message on their social and traditional media platforms as well.

Avoid repeating false information. Focus on providing the accurate facts and do not repeat the false or negative messages. For example, if rumors circulate that the candidate has connections to a nefarious group, avoid saying that rumors about the candidate and his close ties are circulating. Instead, your message should focus on the candidate's legitimate work, such as meetings with locals and addressing the issues that are important to his or her constituents

Best Practices for Social Media Response

Evaluate planned social media activities. Assess whether you should suspend planned social media communications or campaigns in light of the situation.

Use social media reactively and sparingly. Because social media can take unpredictable turns, use it to direct the public back to your statement on the issue, which should be posted on your website.

Watch your tone. The tone of social media communications is casual, but in a cyber crisis, you should use a more formal, just-the-facts approach while maintaining your organization's voice.

Promote your posts, if necessary. Depending on the social media chatter about the incident, you may need to pay to promote your posts to elevate above the noise.

Developing Response Teams

Even a rumor of an online attack, data breach, or voting process issues can trigger a communications crisis and sow distrust in the electoral process. The good news is that you can do advance work 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 determining how to respond.

Maintaining a coordinated process establishes efficient and effective 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 (CIRT)

Effective communications requires an effective overall incident response for `[ORGANIZATION]`. In turn, effective incident management requires a team to coordinate the organization's response to this incident. That response goes well beyond communications but should integrate communications leadership into the process.

The following organizational structure will ensure that communications is part of the overall decision-making process. It assumes the best-case situation where a party has sufficient staffing and leadership. You should adjust the structure to match the resources of your organization.

The cyber incident response should use, to the degree possible, the processes `[ORGANIZATION]` already has on hand to respond to other elections-related crises. This guide can provide assistance in setting up a process if a crisis response plan does not yet exist. 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 [ORGANIZATION LEADER] is responsible for consulting and activating [ORGANIZATION's] cyber incident response plan. You should have designated executives who are backups and can decide whether to activate the plan. Each executive should have the necessary contact information and follow that sequence.

In the event of a significant cyber incident—such as a data breach that may affect the outcome of the election—the government or election management body may seek to suspend, delay, or postpone voting in an emergency, which may include a court order, legislative action, or the emergency powers of the government.

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

It is important to update this table regularly as part of the annual plan review.

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

Role	Designated Individual and Contact Information	Designated Backup and Contact Information
Organizational Leader		
Communications and External Outreach		
Security Leader		
Information Technology Leader		
Legal advice		
Government and Community Relations		

Note: Organizations should adapt accordingly for their structure. In some cases, it may make sense for organizations to seek outside support for IT security and research. Or, in smaller organizations, on individual may be required to play multiple roles.

> **Organizational Leader -** Responsible for coordinating the cyber crisis response in `[ORGANIZATION]`. Depending on the situation, this role should probably be filled by the same person who fills the leader role on the CCRT (discussed below).

> **Communications and External Outreach -** Responsible for coordinating the cyber crisis communications response in `[ORGANIZATION]`. Depending on the situation, this role should probably be filled by the same person who fills the Communications Director role on the CCRT (discussed below).

> **Security Leader -** Responsible for overseeing the IT security of the organization.

> **Information Technology Leader -** Responsible for coordinating IT needs for the organization, including equipment.

> **Legal Advice -** Responsible for providing a legal perspective on any cyber incident, especially around incidents involving sensitive data or data that triggers reporting obligations.

> **Government and Community Relations -** Responsible for outreach to government entities (such as law enforcement) where necessary and appropriate. Also responsible for informing key internal and external stakeholders as needed.

Establishing a Cyber Communications Response Team (CCRT)

Your Cyber Communications Response Team will support your [Communications Lead], who is assigned to the CIRT. Here are the steps you can take to ensure your CCRT has the right people at the table. [ORGANIZATION] should establish the following roles for responding to a cyber incident:

Note: Organizations should adapt accordingly for their structure. In some cases, it may make sense for organizations to seek outside support for IT security and research. Or, in smaller organizations, on individual may be required to play multiple roles.

Political Organization Leader - Responsible for coordinating communications information with [ROLE] in [ORGANIZATION].

IT Director/CIO - Responsible for the [ORGANIZATION'S] IT systems and the security of the systems.

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

Affected Local Affiliates - Usually local party or organization officials from affected areas representing a "field" perspective and providing incident-related information to the coordination process.

Media Operations Director - Responsible for communication with media and media monitoring. Oversees near-term "24-hour" communication operations, i.e., execution of communication plans.

Communications 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 elected officials. For example, for a political party, the liaison might provide briefings to the party's MPs.

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

Role	Designated Individual	Designated Backup
Political Organization Leader		
IT Director/CIO		
Communications Director		
Affected Local Affiliates		
Media Operations Director		
Communications Plans Director		
Legislative/ Intergovernmental Affairs Liaison		
Law Enforcement Affairs Liaison		
Technical Liaison		

Incident Communications Coordination:

Establish your best line of communication. Identify the app or technology you will use to communicate if you think cyber criminals have breached your systems. For example, if your email is hacked, you may want to rely on a secure messaging app such as Signal or Wickr. Communication during a breach is essential, but you do not want your adversaries to know what you are saying—or even that you are responding to their actions. The Communications Response Team will maintain a list of relevant contacts from headquarters, local offices and affiliates, and government contacts to invite relevant parties to a call or meeting, should it be necessary.

`[ORGANIZATION SHOULD INSERT TECHNICAL DETAILS HERE]`

Communications 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. If resources do not permit you to take all of these steps, focus on the least expensive, highest impact steps: 1, 3, 4, and 5.

Step 1: Decide on team. Select the individuals who will be responsible for the tasks 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, or with a trusted vendor, take an inventory of your data assets and potential risks, and conduct an impact assessment. You should understand the incidents to which you are most vulnerable. You should also understand how security tactics are tied to the way your organization manages risk. A process for early monitoring and detection functions should be aligned to the organization's most critical assets, such as donor and party member databases, written correspondence, or donation histories. Establish who will be the IT liaison 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
- Party members
- Election authorities
- Election monitoring groups
- Law enforcement
- Lawmakers
- Media (cybersecurity and election/political beat reporters)
- Other political parties and campaigns
- Third-party advocacy groups

Step 5: Select a spokesperson or spokespeople. Establish ahead of time who will speak for [ORGANIZATION] in a cyber incident, and make sure that they have received media training. You may choose different spokespeople for different audiences. For example, your head of IT might be best equipped to post a response on a vendor site or address hardware concerns, while [ORGANIZATION LEADER] or your Communications Director might be the best person to speak to the media. Consider factors such as who has the best communications skills, prior experience with the media, authority in the organization, 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 [ORGANIZATION'S] CCRT structure but will likely follow this basic outline, tailored to your organizational structure:

- [INSERT ORGANIZATION OUTLINE]

Step 7: Decide what baseline information you can communicate now. Establish a baseline understanding among key stakeholders of [ORGANIZATION'S] work to implement cybersecurity best practices well ahead of the next election. In the event of a cyber situation, this effort will position [ORGANIZATION] to make the case that it has been implementing best practices, but unfortunately, 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 your incorporate lessons learned into this Cyber Communications Template. Your 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 calibrate the appropriate steps to the significance of what is taking place. You should, therefore, categorize all incidents under one of the following severity levels:

1. **Low:** Cyber incident that involves no Personally Identifiable Information (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 but may not trigger formal notification obligations. The issue begins to become public.
3. **High:** Cyber incident that triggers reporting obligations, affects a large amount of voter information, and/or is destructive to the organization's operations.

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

Communications Coordination

Once you have decided on the best method of communication for cyber-related incidents, that means of communicating can be a key coordination mechanism to share operational data, as well as coordinate messaging and communications-related activity.

Upon activation of the CCRT, `[Communications Director]` will alert the team to use the preferred communications technology to communicate securely with the group. 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.

When convening calls, the 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
- Conclusion and next steps

[Note: If your organization has current coordination processes that are effective in sharing and coordinating information, such as regular calls, secure group messaging, or 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 direct communications, such as via Signal, 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 to assess the situation and take basic actions while you develop a more detailed communications plan. You should fully assess each event 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 necessary, consider whether to take down [ORGANIZATION'S] website and, in consultation with IT specialists, decide if you need to launch a separate website or use the organization's social media accounts to communicate externally. This will be a decision for [ORGANIZATION LEADER]. Notify key staff members. If the website remains active, it may be necessary to post a message about the situation.

Step 3: If necessary and possible, contact law enforcement or other 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, which includes an initial comment designed to respond to questions from the public. It lets the public know that you are addressing the incident without providing much detail.

Step 5: Notify key people from your **Cyber Communications Response Team List**

Step 6: Inform entire organization of developing crisis, organization response, and organization's policies that apply.

Step 7: Inform stakeholders.

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/social media coverage.

Step 10: Develop medium-term message(s).

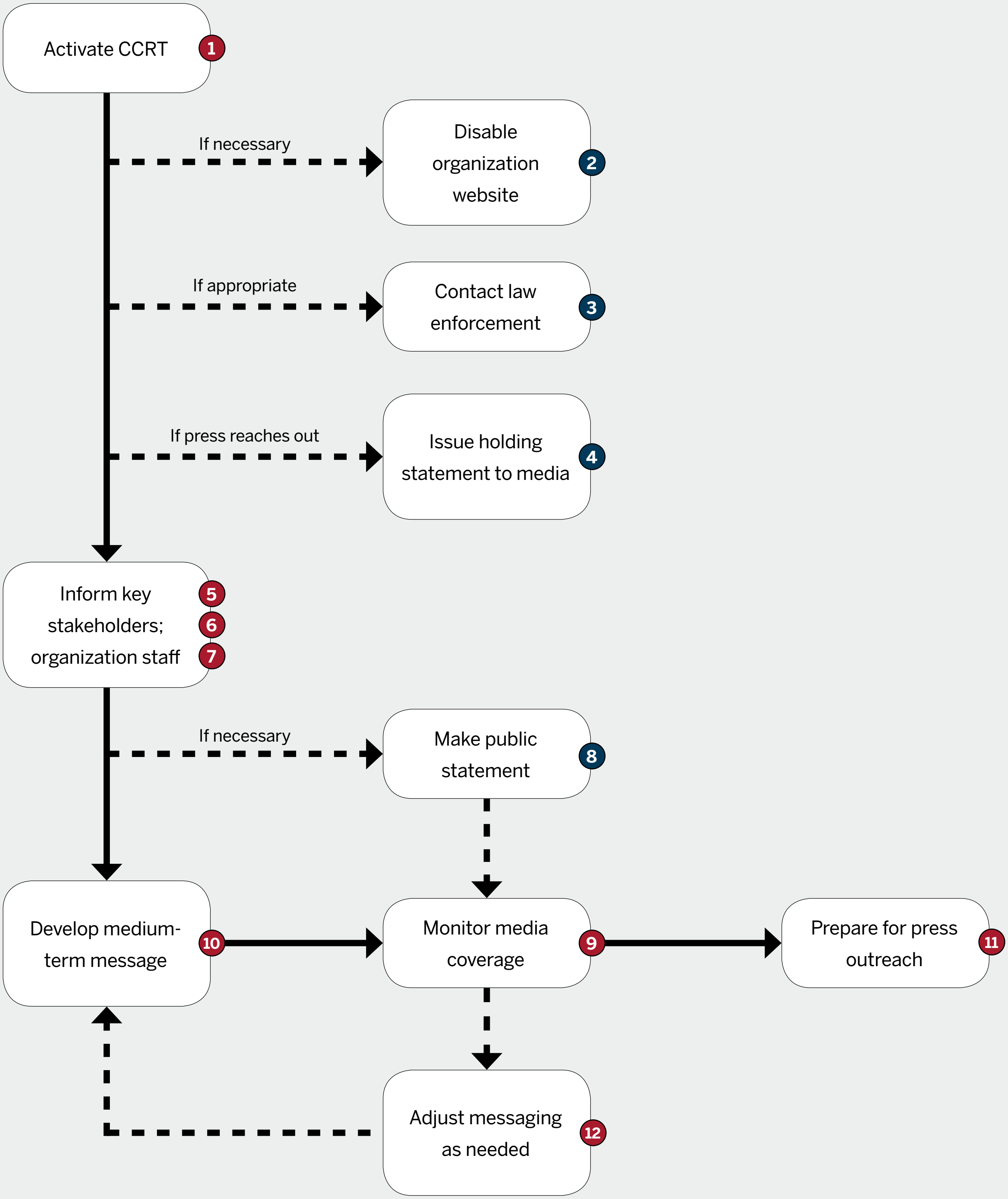
Step 11: Prepare for press outreach/briefing and media schedule.

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

Note: Numbers in chart on following page below correspond to steps outlined above.

Communications Process for a Cyber Incident

Numbers below correspond to steps outlined in prior page


Activate CCRT
1
If necessary
Disable organization website
2
If appropriate
Contact law enforcement
3
If press reaches out
Issue holding statement to media
4
Inform key stakeholders; organization staff
5
6
7
If necessary
Make public statement
8
Develop medium-term message
10
Monitor media coverage
9
Prepare for press outreach
11
Adjust messaging as needed
12

Communications Coordination & Response Checklists

Elections Crisis Communications Checklist

A cyber crisis has the potential to cast a negative light on the [ORGANIZATION]—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. (If you have one, consult [ORGANIZATION'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 days leading up to, and days following, a cyber incident.

Action: Before a cyber crisis

- □ Identify office protocol and the memberships of the CIRT and CCRT. (Should include IT staff).
- □ Create a list of terms with common cyber incident nomenclature for use by all stakeholders.
- □ Set an internal communication plan with key 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 [ORGANIZATION'S] network, including smart phones.
- □ Where appropriate and possible, establish contact with the government agency or agencies responsible for protecting the cybersecurity of campaigns. Also, understand in advance the legal obligations regarding the personal and/or sensitive data held by the organization.
- □ Establish contact with your technology providers about potential threats, and ensure that they know the technical and policy support functions available to them.

□ Conduct briefings for members of the media.

□ Get your social media account verified, because it will provide priority access to the helplines if your profile is compromised. Use social media to show how your organization is preparing.

□ Raise awareness of tactics used in disinformation campaigns.

□ Craft communications materials that can be used in a potential cyber incident, including social media messages.

□ 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 and social media accounts can remain online. If you must disable them, launch a microsite (hosted on a different network) in their place.

□ If email is potentially compromised, use an outside communications channel such as a secure messaging app with end-to-end encryption, like Signal or Wickr.

□ Consult authorities, if needed.

□ Meet internally in central meeting room; set internal communication schedule.

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

□ Determine and identify the appropriate stakeholders for the incident response.

□ Determine broad communications strategy.

□ Prepare holding statement based on language you have already drafted. [SEE PAGE # IN TEMPLATE LANGUAGE YOU WILL DEVELOP FOR LATER IN DOCUMENT]

□ 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 [ORGANIZATION] 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.

□ Begin media (social and traditional) monitoring.

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]

□ Continue 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, or radio) 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 may mean that you return to the reporter without any additional information. You are not obligated to provide details.
- □ Remember: Reporters are under pressure to produce a story 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
  - □ Party members and staff
  - □ Media
  - □ Government offices
  - □ Vendors
  - □ General Public
- □ 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.

General Key Messages and Baseline Communications

We need to set a baseline understanding for the public that `[ORGANIZATION]` is taking cybersecurity seriously and integrating best practices throughout the elections process. Below `[are/is one (or more) example(s)]` of these baseline communications. In addition to a standing website and social media message, develop key messages for `[ORGANIZATION'S]` cyber preparedness activities and integrate them into current online content and future public remarks by `[ORGANIZATION'S]` leaders.

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

Sample Website Message Emphasizing Cybersecurity

`[INSERT GENERAL CYBERSECURITY MESSAGE FROM POLITICAL PARTY.]`

Key Types of Communications Materials

The following materials can be used in any election cyber crisis:

> **Core Holding Statement:** The core holding statement is a generic response to be shared with the media or other stakeholders. This statement will not go into detail but will acknowledge that your organization is investigating a cyber incident and working to recover from it. Because this statement is written and cleared before a crisis strikes, you can make any necessary modifications and distribute quickly when the need arises.

> **Key Messages**: The basis of all internal and external communications materials throughout an incident. This document is the only source of information from which media statements, Q&As, website and social media copy, employee emails, and other communications materials should be drafted. As new information becomes available, the key messages should, in turn, be updated and circulated to relevant officials.

> **Master Q&A:** The Q&A should be used for those dealing with members of the media and other stakeholders. It should be updated and expanded as specific narratives or lines of questioning emerge, and as more information is known about the incident.

General Draft Holding Statement and Master Q&A

The draft holding statement and Master Q&A will provide a basis for communications about any election-related or campaign/party-related cyber incident. They can be used as interim messages while additional facts are gathered. Answers to the Master Q&A can be used in conjunction with the scenario-specific Q&As.

General Cyber Incident Holding Statement

[INSERT HERE TEMPLATE LANGUAGE THAT YOU CAN ADAPT IN A GENERAL ELECTION-RELATED CYBER INCIDENT. IT SHOULD INCLUDE AN ACKNOWLEDGMENT THAT YOU ARE INVESTIGATING A [POTENTIAL] CYBER INCIDENT, YOU ARE WORKING WITH RESPECTED OUTSIDE EXPERTS, AND WHERE RELEVANT, WORKING WITH AUTHORITIES. IT MAY ALSO PROVIDE LIMITED DETAILS OF WHAT HAPPENED TO THE DEGREE THAT DETAIL IS REQUIRED TO MAINTAIN PUBLIC CONFIDENCE IN THE ELECTION PROCESS/SYSTEM. IF POSSIBLE, IT WILL DESCRIBE STEPS BEING TAKEN TO REMEDY THE PROBLEM.]

Master Q&A

[INSERT HERE ANTICIPATED QUESTIONS YOU WILL RECEIVE FROM A RANGE OF STAKEHOLDERS, POPULATED WITH ANSWERS DRAWN FROM THE KEY MESSAGES ABOVE.]

Scenarios

This section is designed to help organizations anticipate different potential scenarios that would require a cyber crisis communications response. The response will vary depending on the specifics of the incident, but planning for scenarios, and rehearsing a communications response, will help organizations identify bottlenecks and develop generic materials that can be modified as circumstances require.

Scenario Components

For each scenario, develop the following response materials:

> **Holding Statement:** Template response for the media and other stakeholders if news of a cybersecurity incident leaks and an immediate response is needed.

> **Specific Q&A:** Anticipated questions and draft answers specific to this scenario, which are derived from the holding statement and aligned with key messages.

> **Key Messages**: Points similar to the holding statement that facilitate guided conversations about a specific cyber situation.

> **Sample Tweet:** Sample tweet that can be adapted for other social media posts.

> **Other Key Stakeholder Communications:** Communications developed for other stakeholders, such as counterparts in other parties or countries.

Sample Scenarios

Organizations should consider the types of scenarios that are most likely to occur or that would have the highest impact.

[NOTE: Some possible scenarios follow, as well as bracketed recommendations on how to approach the response. This Template does not include sample response materials (holding statement, Q&A, etc.) because they will differ widely among organizations. Organizations should develop these materials and include them as part of scenario planning.]

Scenario 1: Insider Threat

A member of your organization's staff with privileged access to sensitive materials, including political strategy documents, opposition research, personnel records, and other materials becomes disillusioned with the organization. The staffer publishes the documents online.

> **Possible Response:** Response should acknowledge that your organization has been the victim of a malicious cyber incident but should avoid describing the magnitude of the breach or discussing any leaked documents in detail. It will take time to fully investigate the incident, so any statement you make about the extent of the problem could later be proven incorrect. Remind the media that these documents were taken by a malicious actor with a hidden agenda. You may also consider ways to update and, if possible, reassure your organization's supporters.

Scenario 2: Social Media Accounts Targeted

Your organization uses social media as a primary means of communicating with supporters. Despite your best security precautions, a malicious actor gains access to your social media (i.e., Facebook or Twitter) account(s) and begins posting messages designed to alienate your supporters.

> **Possible Response:** Your initial statement should identify the compromised account(s) and redirect followers to a different, trusted source. It may take time to restore access to your account, so in the meantime, use all other channels—such as television, radio, and other social media accounts—to disseminate your message. Avoid speculating about the identity or motives of the malicious actor who compromised the account; early information can be inaccurate.

Scenario 3: Tampering with Election Reporting

Malicious actors gain access to the online platform that election officials use to report vote totals to the public on Election Day. While the true count shows that your party is likely to gain a large number of seats, the election website is showing false results that put your party significantly behind. Before the issue can be corrected, the media uses the incorrect information to report that your party is expected to lose ground to opposition parties.

> **Possible Response:** The goal of your statement is to stop the media from reporting the false results as fact and to avoid a situation where the public believes the inaccurate results. The election authorities will likely have their own communications response as well. Your initial statement should be cautious, as you need to avoid undermining confidence in the election as a whole, while also raising awareness that there is a serious inaccuracy. Speed is essential: if the public begins to believe the false results, then the true results could be perceived as fake. Your statement should state that the election authority website appears to have been compromised and differs substantially from the correct vote tally.

Scenario 4: Tampering with Voting Process

As polls open on Election Day, a malicious actor exploits a vulnerability in electronic pollbooks that causes them to fail simultaneously. Poll workers are forced to use a limited number of paper backups, creating long lines at polling places, frustration, and concern about the potential impact on the election. Moreover, the electronic pollbook failures appear to be concentrated in areas that are expected to vote for your party.

> **Possible Response:** Unlike the previous scenario, this one could have a possibly determinative effect on the election outcome. Your initial statement should still be cautious, as additional information may change your view of the incident (i.e., if it later becomes apparent that the pollbook failures were widespread and equally affected areas that tend to support opposition parties). Additionally, an incautious response could provoke a strong—and even violent—response from supporters. The statement should say that you are monitoring the situation and have concerns about the effect of the pollbook failures on the election results but that the information is still preliminary. Once the true extent of the incident is clear, later statements can advocate for appropriate remedies.

Scenario 5: Disinformation Campaign

On Election Day, a large number of social media accounts post false information about the conduct of the election. The posts appear to be intended to suppress turnout and damage public confidence in the results. Claims made in the posts include: long lines in specific polling places, where there are no lines, and election workers are discarding ballots marked for a particular candidate, when they are not. Journalists begin reposting some of these false posts. One of the candidates in the race begins to amplify the false information, saying that the reports are evidence that the election is rigged.

> **Possible Response:** Your goal is to counter disinformation with accurate, reliable information. Your statement should draw attention to the fact that there is an organized disinformation campaign underway but should be careful not to repeat or amplify the disinformation. The statement should highlight the facts rather than repeating and rebutting each false claim. It should also be short, concise, and distributed via every possible platform (social media, television, radio, etc.) See also the "Best Practices for Countering Disinformation" section.

Conclusion

We hope that this Template provides a good start for political parties and campaigns that are seeking to develop a cybersecurity communications response plan. We also hope the guidance and format of this Template helps organizations prepare for, and manage, the 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 organizational structures and personnel.

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