

The Elections Battle Staff Playbook



HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

DEFENDING DIGITAL DEMOCRACY
DECEMBER 2019



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.

Cover photo: Voters line up in voting booths to cast their ballots at Robious Elementary School in Richmond, Va. on Tuesday, Nov. 8, 2016. The mural in the background was painted by 3rd and 4th graders at the school in preparation for Veterans Day. (Shelby Lum/Richmond Times-Dispatch via AP)

Copyright 2019, President and Fellows of Harvard College



The Elections Battle Staff Playbook

Contents

Welcome.....	2
Authors and Contributors	3
The Playbook Approach	4
Top 10 Take-Aways for Building Your Battle Staff	6
Introduction: The Current Operating Environment	7
Building an Elections Battle Staff	8
1. People and Purpose.....	8
2. Situational Awareness Through Communications.....	16
3. Taking Action: Election Incident Tracking, Analysis, and Response	24
4. Bringing it All Together: The Operations Center.....	32
Next Steps: Making It All Happen.....	36
Appendix A: Get Prepped Checklist	37
Appendix B: Operations Center Physical Layout Models.....	39
Appendix C: Leadership and Teamwork in Action	40

Welcome

The 2016 elections changed our nation's consciousness on election security and how malicious actors can influence our democracy. While the threats were not new, for most of us they were newly realized. The vulnerabilities in our democratic process—from campaigns to elections operations—combined with efforts to spread false or deliberately misleading information, have weakened the public's faith in the integrity of elections. Yet that faith is vital to our democratic process, so we must work to restore and sustain it.

Democratic governance is a right we have as Americans, but like freedom, democracy is not free. It takes people willing to stand up and defend the process. Ensuring election security is our collective responsibility as Americans, but election officials, campaigns, and others involved in advancing the democratic process carry the greatest weight as its frontline defense. That's why we established the Defending Digital Democracy Project (D3P): to equip those on the frontlines of democracy with tools and resources to be successful against constantly evolving threats.

With 2020 around the corner, we know adversaries who seek to undermine our democracy are preparing, and so must we. The American people and the world are watching. We must show them how seriously we take the threats and how committed we remain to the cause.

Despite the enormous challenges ahead, we know that democracy is in good hands because we have spent the past two-and-a-half years working together with dedicated American election officials like you. We have visited and/or trained officials from 45 states and countless counties. We have spent time in your spaces, met your teams, listened to your ideas, noted your concerns, reviewed your preparation, observed your operations, and identified ways in which we can continue to help.

Our previous Playbooks have focused on the threats posed by cyber attacks and information operations. This latest Playbook has a broader scope, and equips you with strategies to operationalize the guidance from past Playbooks through effective preparation, communication, incident tracking, and team organization. By compiling best practices from private and public sector actors, we hope to enhance the capacity of your election team, regardless of your staff or jurisdiction size. It will better prepare you to identify issues and respond to incidents of all types during election operations.

We hope this Elections Battle Staff Playbook empowers you to take defending election operations to the next level.

Good luck,
D3P

Authors and Contributors

AUTHORS

Meredith Berger, D3P

Gabriel Cederberg, D3P

Caitlin Conley, D3P

Katie Kendall, D3P

Kunal Kothari, D3P

Ryan Macias, D3P

Zara Perumal, D3P

Jonathan Pevarnek, D3P

Anu Saha, D3P

Sarah Starr-Douglas, D3P

CONTRIBUTORS

Daniel Bartlett, D3P

Eben Kaplan, CrowdStrike

Ashley Miller, D3P

Joel Moehler, CrowdStrike

Heather Adkins, D3P Senior Advisory Board

Eric Rosenbach, Co- Director, Belfer Center; Director, D3P

Maria Barsallo Lynch, Executive Director, D3P

Maya Nandakumar, Project Coordinator, D3P

Andrew Facini, Publishing Manager, Belfer Center

The Playbook Approach

This Playbook is written for election officials to help operationalize their election staff by turning them into a Battle Staff. The Playbook gathers best practices from public and private sector actors who also share the challenge of leading resource-constrained organizations in high-stakes, complex environments. The recommendations that follow combine applied operational leadership philosophy frameworks, decades of practical operational leadership experience in high-risk fields, and the knowledge and insights gained while working with and learning from the elections community. These recommendations apply to all jurisdictions, regardless of resources or size. Understanding that election officials are already doing a lot with a little, this approach integrates these new concepts into existing resource environments.

The Election Battle Staff Playbook's Goal

Provide election officials tools to efficiently and effectively organize people and processes to enable informed decision-making with resources in order to preserve the integrity of elections during voting periods.

This Playbook begins with the **Current Operating Environment**: how the growing threats against our elections system and increased scrutiny toward the elections process means we need to do more to defend our democracy and preserve public trust. The rest of the Playbook walks you through **Building an Elections Battle Staff**.

A **Battle Staff** is a military headquarters element activated to support ongoing operations across multiple echelons (levels of organization). A Battle Staff optimizes decision-making by improving cross-functional collaboration and increased understanding of the operating environment in order to ensure mission critical processes are reliable, repeatable, and efficient.

1. First, we focus on **People and Purpose**. This section outlines how to organize your elections staff to optimize key roles, while standardizing methods to reduce human error and increase team efficiency.
2. Second, we break down the importance of **Shared Situational Awareness through Communication** and how to achieve it. This section discusses how to integrate communication upward, downward, and laterally, to provide data, perspective, and solutions to leaders at every level so that they can make informed, effective decisions.

3. Third, we explore **Taking Action: Incident Tracking, Analysis, and Response**. This section explains how to set up information flows critical to managing time-sensitive election operations, including an incident tracking system and trend analysis to inform decision-making and improve team performance.
4. Fourth, we bring these concepts together and put them into action in setting up **Your Election Operations Center (Ops Center)**. This section explains the physical setup of an Election Operations Center—your nerve center—where the necessary people, equipped with the right processes and information, work together to confront and resolve issues that arise during the voting period.

The Playbook focuses on the role of staff during the voting period; however, you need to plan and prepare beforehand if you want to execute well. Throughout the document, you will see callout boxes titled “Get Prepped” highlighting key actions you can take before the voting period to set your team up for success. These are collected and outlined in Appendix A.



Get Prepped: Preparation requires setting up systems in advance, teaching people the purpose and intent of what they are doing, and allowing them to practice in order to better understand their roles and those of others. These boxes will alert you to key actions you'll want to take.

At the end, a series of appendices provides additional tools and resources to build on the guiding principles, philosophies, and strategies that support the Playbook's recommendations.

Now let's get started!

Top 10 Take-Aways for Building Your Battle Staff

People and Purpose

1. **Map out your elections ecosystem** and identify the types of relationships between various people/entities: Operational Control or Coordinating.
2. **Build out your broader team** through alliances and augmentees (temps, interns, recruits from other state/county agencies, etc.). Expand your staff on the frontline then train and equip them with SOPs to manage simple but common problems.
3. **Assign all Battle Staff members a role along with task and purpose** that they are best suited for based on their skill sets and level of expertise. Those with specific skills or expertise (rovers and IT staff) can tackle complicated problems, while the Battle Staff focuses on more complex problems.

Comms

4. **Establish Communication Paths:** identify **who** needs to communicate with whom, **how** they are going to do it (in method and in format), and **when**. This applies for both internal (“down and in”) and external (“up and out”) communication.
5. **Develop a PACE plan** and create formats for scheduled and non-scheduled communication.

Incident Management

6. **Identify your Critical Information Requirements (CIRs)** that address the full scope of issues that impact election operations or election integrity. Structure criticality levels to prioritize CIRs based on the incident’s impact to critical operational systems and the overall operating environment.
7. **Develop an Incident Tracking System to consolidate and monitor CIRs.** Train all staff members on the appropriate tools needed to collect and analyze the data, and perform stress tests to ensure that reporting on the information collected is sufficiently structured to deliver the intended value. Develop a dashboard to visualize important data and signals that enable the staff to remain focused on priority items. Identify the most important things to monitor—they may be different for each member of the Battle Staff.

Bringing It All Together

8. **Build your Operations Center.** Find a physical space and develop a plan for integrating people, processes, and information. The layout should provide greatest situational awareness while also enabling ease of communication among Battle Staff members. Develop your Ops Center battle rhythm to include scheduled information sharing events.
9. **Establish SOPs.** A clear response plan for the “knowns” will leave space to think about and react to the “unknowns.” Identify anticipated incidents based on past election experiences. Develop and implement SOPs for methodical logging, troubleshooting, resolution, and communication of common, recurring incidents.
10. **Practice!** Rehearse all of the above prior to the voting period. Utilize early voting periods, to iterate on your processes, techniques, and communication strategies in advance of peak voting periods.

Introduction:

The Current Operating Environment

Elections succeed when they are carried out in a fair and transparent manner that maintains voters' confidence in the process. Today, protecting and preserving people's confidence is more challenging than ever. Election officials have to continuously ensure that the election infrastructure is secure, the information is accurate, every ballot is counted, and the results are reported quickly. At the same time, bad actors have an increasing number of threat vectors—from social media bots to cyber attacks—with which they can attempt to discredit the process on both the micro- and macro-levels.

Over the past decade, these actors have increasingly used their resources and abilities in both crude and sophisticated ways to exploit vulnerabilities and undermine our democracy. Unfortunately, a malicious actor does not have to subvert the entire elections process to put the American voter's confidence in the system at risk. In reality, a successful attack on one election jurisdiction—or merely the perception that a successful attack has occurred—can have effects that ripple across the country.

Recent attacks such as these have brought election integrity to the forefront of our national consciousness, and ever-evolving tools and tactics make defending our democracy even more challenging. Election officials know the complexities and vulnerabilities of the election process better than anyone else. No jurisdiction or state can take on this challenge alone. With effective information sharing—both within election teams and vertically between different levels of the election leaders—we can make our decentralized election system a strength rather than a vulnerability. Ultimately, this Playbook seeks to mitigate growing threats against our elections by optimizing election operation processes and enhancing our ability to cooperate among leadership teams across the country.

Building an Elections Battle Staff

In simplest terms, operationalizing your staff comes down to connecting people, information, and processes with the operating environment so that your organization can perform effectively and efficiently when stakes are high. At the core of coordinating and managing election operations is the Battle Staff—a select group of individuals in the Operations Center that has the expertise and critical thinking skills to focus on complex problems and coordinate large-scale operations.

Typically a Battle Staff is a military headquarters that supports frontline troops conducting tactical operations by providing them with resource coordination, contingency planning, and cross-unit deconfliction and coordination. The Battle Staff, located in the Operations Center, is able to holistically see what is happening in the operating environment to better support tactical units in the field while mitigating risk to the mission and forces.

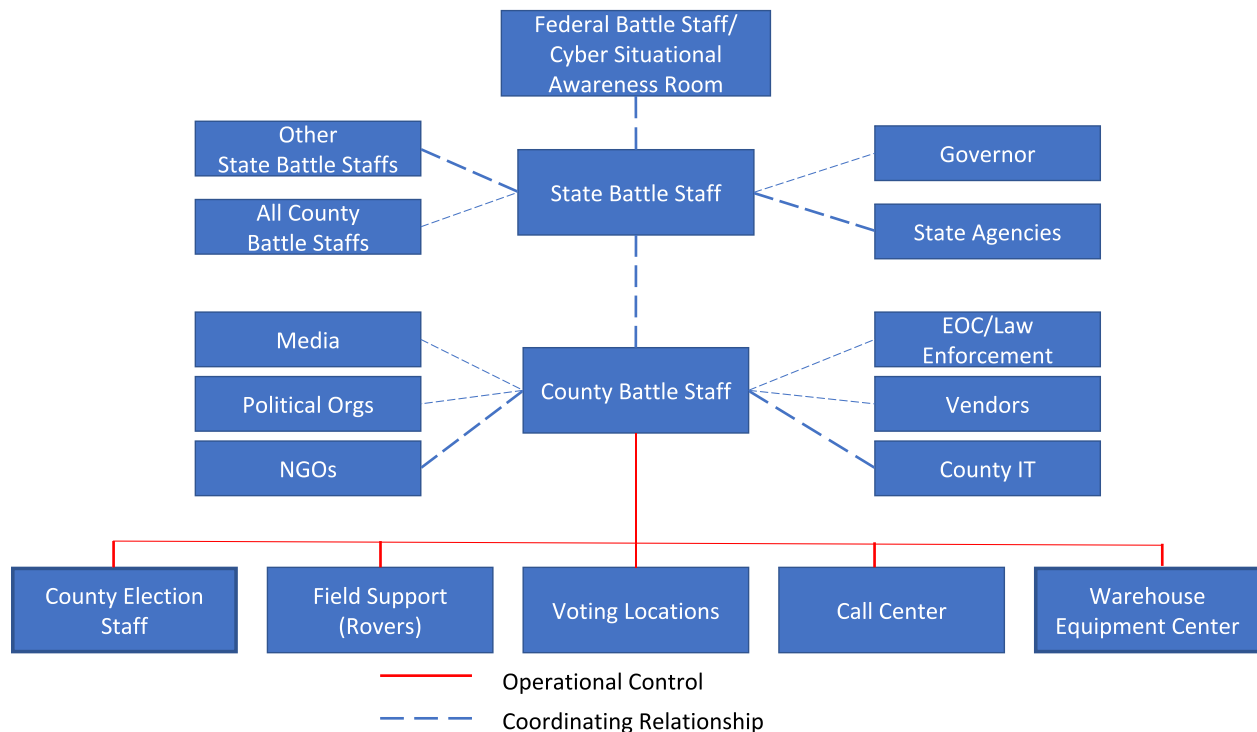
In the following sections, you'll walk through how to turn your election staff into a versatile, operational task force prepared to manage and mitigate the spectrum of crises you face, digitally and physically. It will challenge you to look at operational management differently while still operating within your resourcing constraints.

1. People and Purpose

At the end of the day, *people* make elections successful. While responsibilities vary, everyone, from leaders to team members, plays an equally important role. While your Battle Staff is at the center of this process, successful management of people and responsibilities requires involving the broader election ecosystem. Start by **mapping out your jurisdiction's election ecosystem** and identifying what type of relationship it has with each entity during the voting period: is it operational control or coordinating?

- *Operational Control* means being able to assign people their tasks and define their purpose. Example: an elections office has operational control over its own staff, staff augmentees from other government offices, field support teams (rovers), warehouse equipment centers, call centers, and election workers.

- *Coordinating* applies to an entity over which you do not have immediate control but will need or want to engage with in the conduct of election operations. These entities can provide key services, information updates, and specialized assistance. Coordination also includes reporting relationships with those entities above and below you that you have a responsibility to keep informed.



Get Prepped: Map out your election ecosystem. Identify what entities the elections office has operational control over or a coordinating relationship. In coordinating relationships, identify where liaisons already exist and where new ones are needed to fill gaps.

Sharing the Load: Distributing Lines of Effort Across the Team

Effectively organizing tasks across the elections team to streamline operations requires a common understanding of how each role contributes to the big picture. **Assign all staff members the tasks and purpose for which they are best suited**, based on their skill sets and level of expertise. This applies not only to the Battle Staff but also to all elements the election office operationally controls and, when possible, even those with which they coordinate.

Incidents or problems encountered during election operations generally can be divided into one of three categories, which in turn drives who is responsible for resolution based on the level of expertise required. Identifying who is responsible for what ensures that all critical functions are carried out and your key responsibilities (no-fail missions) are completed while avoiding costly redundancy and maximizing your team’s effectiveness.

Simple	Complicated	Complex
An expected problem with a known solution that does not require expertise to resolve	A problem (expected or unexpected) that requires expertise to solve	A problem that involves too many unknowns for standard procedures to resolve, and requires both expertise and critical thinking

Simple issues can be handled by less-experienced-but-trained people using standard processes. In elections, these individuals are your “Firstline Staff,” typically your call center employees or poll workers, who may lack the technical knowledge or subject matter expertise of full-time election or IT staff, but can resolve the overwhelming majority of simple issues by following standard operating procedures (**SOPs**). Then you have your more technically trained and skilled experts—your IT staff, election coordinators, or election field support teams (**rovers**)—who can address the complicated issues. The complex problems are reserved for your subject matter experts—your Battle Staff—who are the core of coordinating and managing election operations at all levels. For example, fielding calls from the public to answer basic questions such as whether they are registered or where their polling place is should be answered by a call center and NOT by the staff in your Operations Center. Save the Battle Staff for the hard stuff!

Standard Operating Procedures: SOPs are step-by-step instructions to perform routine operations for common or anticipated events. SOPs help teams perform efficiently and effectively while reducing miscommunication, inconsistency, and the chances of important information slipping through the cracks. A good SOP is concise, easily repeatable, unambiguous, and clearly defines what is flexible or inflexible. Developing and implementing SOPs will increase bandwidth across your operations by reducing issue resolution time, subjectivity, and overall potential for human error.

Rovers: Teams deployed to the field by election offices to provide on-site assistance at voting locations. They can range from IT and voting equipment specialists to overall election office staffers who are knowledgeable about field operations.



Get Prepped: Identify your entire election staff: frontline, staff, and battle staff. Organize your staff so that each element has a clearly defined task and purpose. For those on the frontline, use, develop, and implement SOPs to assist with managing known issues in a consistent and efficient way. Develop an SOP for incident reporting that will inform the task and purpose of different staff members—this will be addressed later in Section 3.

Battle Staff in Action: Roles and Responsibilities

An Elections Battle Staff contains three components: a core team, an extended team, and liaisons. The core team is the staff's central nervous system—the select individuals directly responsible for overseeing election operations. The extended team consists of other specialty roles participating in election operations, but that likely come from other state and local government staff. The liaisons are representatives of the other agencies and entities that the elections office coordinates with, but that are not immediately involved in election administration. It is always best to have liaisons physically present in the Operations Center as members of your Battle Staff; however, if that's not possible, then at a minimum, integrate them virtually through predetermined times and methods of contact.

Let's walk through an example of how to organize an elections office by people and their purpose. This model will not be the best option for all jurisdictions, but provides an example of how you could delegate tasks based on a six-person core Battle Staff along with the extended Battle Staff and liaisons from coordinating agencies.

KEY ROLES AND RESPONSIBILITIES

Core Battle Staff

Title	Description	Key Responsibilities
Director	The Chief Election Official responsible for operations and mitigating risk. Her/His time and focus needs to be insulated from routine matters, and is only directly involved with the issues of highest importance.	<ul style="list-style-type: none"> Interface with the senior leaders (i.e., elected, government, coordinating agency leadership); Provide operational oversight, risk mitigation, analysis, and response to complex problems; Engage the media to be an authority on, and provide insight and transparency into, the conduct of election operations.
Deputy Director	The trusted advisor to, and authorized deputy of the director. The deputy director serves as the leadership touch point for the rest of the staff and shields the director from all non-complex issues.	<ul style="list-style-type: none"> Manage Battle Staff and incident resolution; Provide internal staff guidance on most issues and ensure that critical issues are elevated to the director; Coordinate logistical support internally and with other necessary agencies/entities.
Field Support Team	The individuals responsible for direct communication and coordination with rovers and, when necessary, the voting location chief poll worker. Ideally, have experience in field operations. Provides initial issue triage.	<ul style="list-style-type: none"> Designated Battle Staff touch point for field representatives (rovers and, when necessary, poll chiefs); Triages (receives, reports, and resolves/delegates) issues from staff and field employees; Monitor and manage the deployment of rovers or field staff.
Incident Response Team	The individuals responsible for overseeing the incident tracking system and incident response measures. They conduct action officer level coordination with external entities for incident resolution, and inform the deputy when senior leader assistance is needed.	<ul style="list-style-type: none"> Oversee issue delegation and resolution across the entire staff and, when necessary, elevate or report complicated and complex incidents. Monitor incidents via the incident tracker and through the media (traditional and social); Analyze incidents to understand the threat landscape, assign or validate criticality, and identify anomalies and patterns.

Extended Battle Staff

Title	Description
Legal Advisor	Provide legal assistance for any issues; advise and assist the elections director and/or communications officer on engagements with external stakeholders.
Data Analyst	Assist the Incident Response Team in analyzing incident reports and validate or reassign criticality as necessary.
Equipment and Logistics Expert	Address malfunctioning equipment, serve as staff subject matter expert on equipment processes, and dispatch needed supplies.
Media and Communications Manager	Manage basic communications to the public, help monitor media, and coordinate formal communications or briefings.

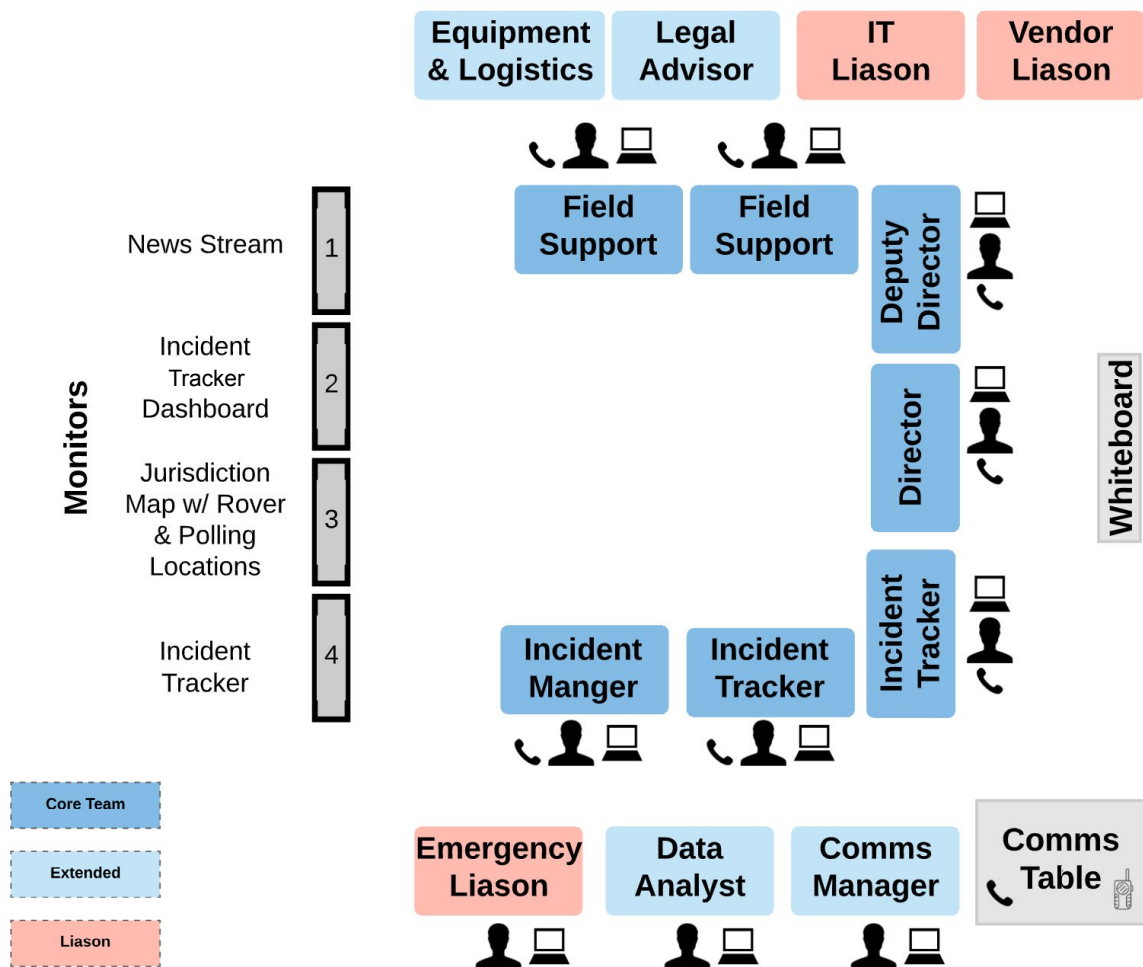
Battle Staff Coordinating Liaisons

Title	Description
Government IT Internal Liaison	Much of the election infrastructure is outside of the election office's control (i.e., county or state networks), so it is critical to have someone on hand to quickly resolve IT issues on those networks and coordinate necessary external resources.
Emergency Operations Liaison	The connection to the state/municipality emergency operations center who can share information and coordinate with emergency operators on incidents that the election official does not have the resources to address; assists with maintaining situational awareness of conditions throughout the jurisdiction.
Election System Vendor(s) Liaison	Provides technical subject matter expertise on voting equipment and systems for issues that are more complicated than your staff can technically resolve. Having vendors in the Operations Center could cause potential legal complications so it is best to keep them adjacent and/or easily accessible.



Get Prepped: Identify who will be filling each staff role in advance, including liaisons from external entities. In some jurisdictions, one individual may have multiple roles. In others, many people might be required per role. Have a staff roster published and distributed in advance so people know who the appropriate touch points are.

Election Operations Center



Resourcing and Capacity Building

During the voting period, there are critical tasks that need to be executed and responsibilities that need to be fulfilled, no matter what. Not every election operation will have the same level of resourcing available, but resourcing does not limit the tasks at hand, nor the need to accomplish those tasks.

If you don't have an internal staff that is large enough, be creative and look for hidden resources and talent. You can elevate less experienced, but very capable, members of your staff to your Battle Staff or other positions by giving them specific tasks. Also, consider looking to adjacent organizations and teams to borrow capacity—make them your allies invested in the process and its success.



Pro tip: There are several of out-of-the-box ways to increase your staff bandwidth. Establishing strategic alliances well in advance of elections can pay significant dividends for your capacity during the election period. Every jurisdiction is different, but you may be able to borrow resources from other departments and agencies to assist during key time periods.

Here are a few ideas:

- Borrow resources with special skill sets such as software development, social media, or communications, to augment your capabilities in advance of the voting period.
- Borrow resources from outside of the core elections team for temporary windows of time to support your Battle Staff, help field calls, coordinate logistics, or address tactical issues during the surge periods.
- Pull in people from partner organizations as liaison officers who can be incorporated into the Battle Staff—their understanding of processes and personnel in their respective departments, combined with training on your election operations and processes, can make them invaluable assets during the voting period.

Just keep in mind—making this work requires investing in knowledge transfer, training, and clear SOPs well in advance.

2. Situational Awareness Through Communications

Elections' decentralized nature makes it difficult for teams to obtain and analyze information in order to understand the on-the-ground reality unless a communications plan is in place to guide what is shared, with whom, how, and when. Communicating during periods of high stress is one of the hardest tasks your team will face. This makes pre-planning communication pathways critical.

Critical information sharing needs to occur across two distinct but equally important planes of communication:

- **Local (“down-and-in”)** communication to make your election operations happen effectively and to manage your team in real time.
- **External (“up-and-out”)** communication to share information beyond your team (think state and national level) to help identify broader trends.



Case in Point: Sharing “Up-and-Out” Can Make the Critical Difference in Defense

In 2010, when Google witnessed a sophisticated targeted attack on its corporate networks, it also learned that at least 20 other companies had been targeted by the same attackers. While fixing its own systems, Google also reached out to the other companies that had been affected by the attack. They shared what they were learning so that others could better detect the actor penetrating their systems. Additionally, by deciding to work within the larger community, solutions were identified and implemented that resulted in a more secure Internet overall.

The following walks through three principles for communication planning: identifying **who** needs to communicate with whom, **how** they communicate with each other, and **when** they communicate. Section 3 of the Playbook builds on your groundwork here to identify **what** information should be shared for incident tracking.

Step 1. Identify Communication Paths—Who Needs to Communicate with Whom


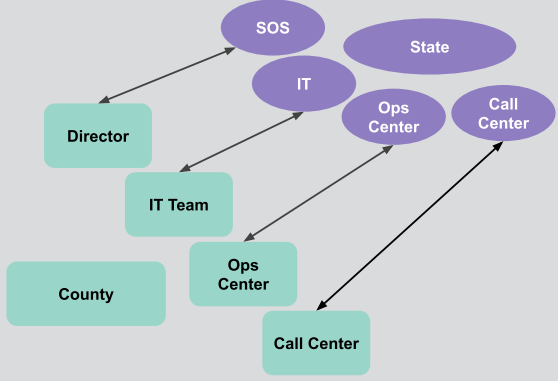
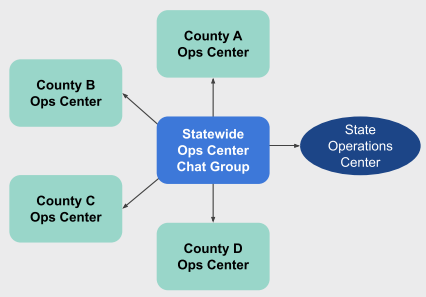
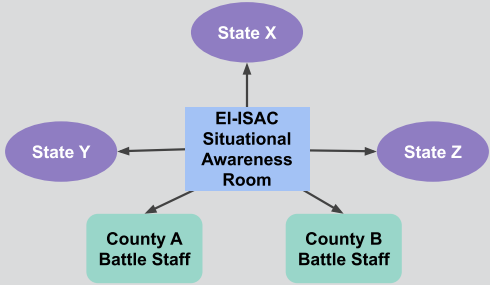
Earlier, you mapped your elections ecosystem. Now, use that map to identify your communication paths: identify *who* needs to communicate with whom. A path may be between as few as two individuals (like an election director and the Secretary of State) or among a large group (like multiple counties' operations centers sharing real-time trends). These paths will account for all of the necessary communication paths to enable local (“Down-and-In”) and external (“Up-and-Out”) communication.

While we’re focused on *who* here, think through *why these specific teams need to be connected*: to share lessons learned and important information that could impact other locations, and to update the group on concerns reported in the incident tracker.



Get Prepped: Based on your staff task organization and your mapped elections ecosystem, identify your “down-and-in” and “up-and-out” communication paths. Plan for these in advance by creating standard report formats, distributing necessary equipment, providing contact rosters, and coordinating with external entities for scheduled information sharing events.

Group Type	Purpose	Communications Path Diagram
<p>WHAT: Voting Location Support Chat Group</p> <p>WHO: Rovers with their respective Poll Chiefs</p>	Allows those in the field to have real-time operational communication and support while enabling rapid information sharing among proximal polling sites.	
<p>WHAT: Field Support Chat Group</p> <p>WHO: All Rovers and Battle Staff Field Support Team</p>	Allows for fast and consistent information communication and situational awareness across the county from the Battle Staff to the Rovers who then relay to voting locations.	

Group Type	Purpose	Communications Path Diagram
<p>WHAT: Battle Staff Internal Chat Group</p> <p>WHO: All Battle Staff members</p>	<p>Ensures timely cross-leveling of information. Outside of the periodic updates, getting every Battle Staffer's attention at the same time will be nearly impossible; this chat group allows team members to check chat history when able, ensuring they do not miss anything.</p>	
<p>WHAT: Individual County-to-State Chat Groups</p> <p>WHO: County and State Offices</p>	<p>Point-to-point vertical comms between county offices and the state level counterpart to inform and discuss issues that it may need assistance with resolving to include deployment of state level resources the county may not be aware of. Provides an opportunity for the state and county to respond cohesively to issues that may affect one another.</p>	
<p>WHAT: Statewide Ops Center Chat Group</p> <p>WHO: State and All County Ops Centers</p>	<p>Provides all jurisdictions with visibility of incidents occurring across the state. Allows the state to analyze trends and commonalities in order to identify incidents impacting beyond single jurisdictions.</p>	
<p>WHAT: Election Day Cyber Situational Awareness Room (National)</p> <p>WHO: Operated EI-ISAC open to all states and local jurisdictions</p>	<p>Provides a centralized information-sharing platform for the elections community and federal partners regarding cybersecurity threats to election infrastructure across the nation.</p>	

Step 2. Determine How to Communicate

Your primary method of communication should always be the most time efficient and reliable. The best way to achieve this will depend on the type and purpose of the information being conveyed. For instance, the primary method for precincts to report polls open would not be well served by having individual locations calling in. A more efficient approach, such as chief election workers responding to an automated message sent to their phones (or responding to a “polls open” message on their laptop), would allow an automated system to log responses without the need for manual checks. This method frees up key staff capacity and phone lines to focus on problems at hand.

On the other hand, automated messaging and response is not an appropriate method when the chief election workers need assistance resolving issues. In that situation, they could leverage their Voting Location Support Chat Group to elevate issues to the attention of rovers or elections support liaisons. Likewise, rovers can address multiple issues at a time while promoting cross-learning among voting locations.



Pro tip: Some jurisdictions have chat capability built into existing systems, such as office software tools or election technology (i.e., an election management system or electronic poll book chat room). Additional resources include:

- Openly available software for dedicated chat rooms, such as Microsoft Teams, Skype, Google Hangouts Chat, Slack, GoToMeeting, and WebEx Chat.
- Text groups using end-to-end encrypted applications, like Signal and Wickr.¹

Remember to train on any new tools before implementation.

A Note on Regulatory Requirements: As with emails, it is possible to keep a chat history and a backup log to maintain election related communications. Be sure that you confirm and test the appropriate settings prior to the voting period to ensure options such as “disappearing messages” are turned off and chat backup is turned on.



Get Prepped: Identify what options exist for different communication paths and decide which method best meets your requirements. Equipment purchasing or software downloads/updates may be required and should be integrated into your election operations overall preparation.

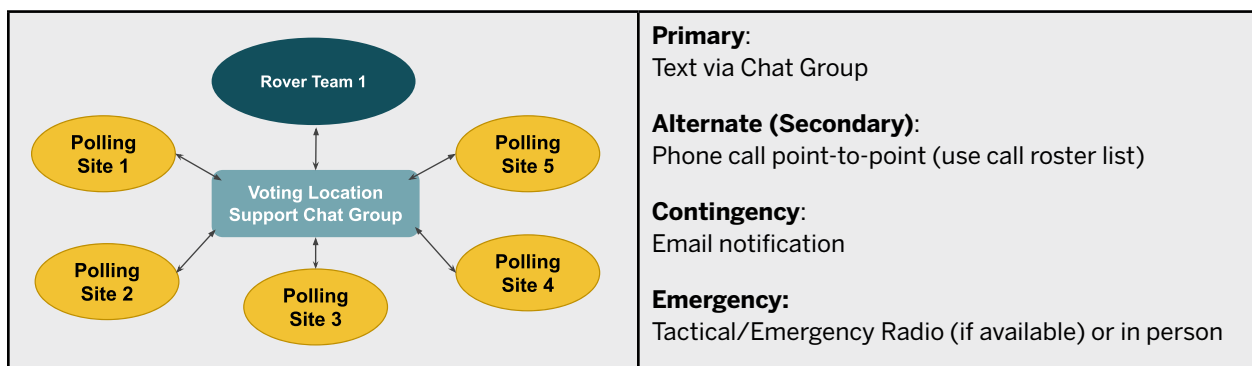
¹ This is not intended to be an exhaustive or endorsed list, but rather, to offer suggestions on readily available tools that can be adapted. Encryption, data retention/logs, legal requirements, accessibility, compatibility, cost, and organization are among the many factors that should go into this decision.

Step 3. Determine Backup Communications Plans

Election operations' success requires reliable communication at scale, with little room for snags or downtime. The military uses **PACE** (Primary, Alternate/Secondary, Contingency, and Emergency) plans to ensure that operations remain uninterrupted even if communication systems fail. To establish a PACE plan, identify four reliable communication methods, and then prioritize them by effectiveness. If one fails, your team should be prepared to move to the next in line to keep communications flowing and maintain situational awareness.

Establish your teams' PACE Plans:

- For each communication path, identify if it will be used between individuals or groups as well as its purpose.
- Identify available communication methods, including web-, phone-, radio-based and in-person (the Battle Staff in the operations center should have a list of all available methods of communication).
- Decide which are most effective and reliable based on the path's purpose.
- Choosing the four best methods, create a PACE Plan for each Critical Communication Path. Here's an example:





Get Prepped: Implementing a good communication plan is one of the most difficult organizational tasks. Help your team succeed by developing these critical game-day tools in advance:

- Develop a contact roster. It should contain contact information required for the PACE Plans you developed (email, phone numbers, usernames for chat platforms).
- Share the contact roster across the network. Schedule when you'll make updates (e.g., to replace or add team members) and ensure that teams have the up-to-date version. Add a **version number** and **date of last update** to your contact roster.
- Test your PACE Plan: Schedule a rehearsal PACE Plan Test for each communication path. Make changes to the PACE plans when needed and ensure that everyone knows about the change to the SOP. Also confirm that everyone on the team knows how to use your communication tools and that all tools are working properly (e.g., items are charged/have batteries, you've tested for technical problems).

Step 4. When to Communicate—Scheduled and Unscheduled Information Sharing

You've identified how team members will communicate, now capture basic rules for *when* you'll communicate within each path. Begin by dividing what will be communicated into two groups: **Scheduled Information**—the things you know you'll communicate, and **Unscheduled Information**—the unpredictable events that will arise and need to be shared.

Scheduled Information Sharing

Brainstorm the group's routine information and scheduled reports, like voter turnout updates or whether precincts reporting polls are open. Develop a simple format to communicate these reports; your format should cover what information is shared and when it's reported (it may be time- or event-based). Capture these formats in your SOP. These reports should become part of your operations Battle Rhythm outlined in Section 4. Adhering to scheduled information sharing during election operations will ensure that the staff has an up-to-date operating picture, empowering it to be proactive and prepared rather than just reactive.

Putting It Into Practice. Consolidate scheduled information sharing via planned information briefs: an Initial Guidance Brief, Periodic Internal Update Briefs, and an External Stakeholders Brief.

Initial Guidance Brief. Open the day with a 10-minute brief from the director to the Battle Staff, other elections staff and rovers; invite others, including chief election workers, if available. The brief provides guidance on: task delegation, roles and responsibilities, restating Critical Information Requirement (CIR) thresholds and notification requirements, and known major events for the day. *(Note: CIRs will be addressed below in Section 3)*

Periodic Internal Update Briefs (“Down-and-In”). Provide a 10-15 minute update led by the Ops Center. Facilitate maximum participation, regardless of location. Briefers relay information succinctly; they hit the most important points to ensure everyone is tracking critical changes since the last update.

Agenda Event	Briefer
Roll Call	Deputy
ANALYST UPDATES	
1. Weather and Environmental Considerations (1 minute)	Emergency Ops Center/ Law Enforcement Liaison
2. Emerging Issues, Disruptions, or Trends Overview (1 minute)	Incident Tracking Team
CIR Update (1 minute)	Director or Deputy
1. Any Level 1 or Level 2 Incidents Observed?	
2. Outstanding Incidents Requiring Attention in the Next [2] hrs	
TEAM UPDATES	
1. National Level Update (As Applicable) (1 minute)	Deputy
2. Field Updates (2 minutes)	Field Support Team
3. Projected Events Next [2] hours (1 minute)	Deputy
Liaison (LNO) Update (2 minutes)	LNOs
Closing Summary (1 minute)	Director or Deputy

Preset External Stakeholder Briefs (“Up-and-Out”). The director (or appropriate communications officer/ liaison) provides similar updates to key external stakeholders. Briefs cover relevant information in a consolidated format and are scheduled in advance to support proactive— rather than reactive—communication. Stakeholder briefings include:

- Periodic media update briefs
- Interstate election team updates
- Inter-jurisdiction election team updates

For more information, visit D3P’s **Election Cyber Incident Communications Plan Template**. This communications plan includes guidelines and template materials to help election officials respond quickly and in a coordinated fashion to a cyber-related elections incident.

Unscheduled Information Sharing

Determine how your group wants to communicate unscheduled information across the different methods before game day. One simple, tried and true method is the 5Ws format:

1. *Who was affected by the event?*
2. *What happened?*
3. *When did it happen?*
4. *Where did it happen?*
5. *Why is it important: does it answer a Critical Information Requirement (CIR) or require additional action from someone?*

Example Report

1. Precinct 4
2. Poll worker told about tweet accusing County X of voter discrimination
3. Reported at 9:20 am; Tweet post at 9:00 am
4. Online: Twitter
5. CIR #7



Get Prepped: Develop standardized reporting formats in advance and distribute them to your staff. These should be incorporated into your SOPs.

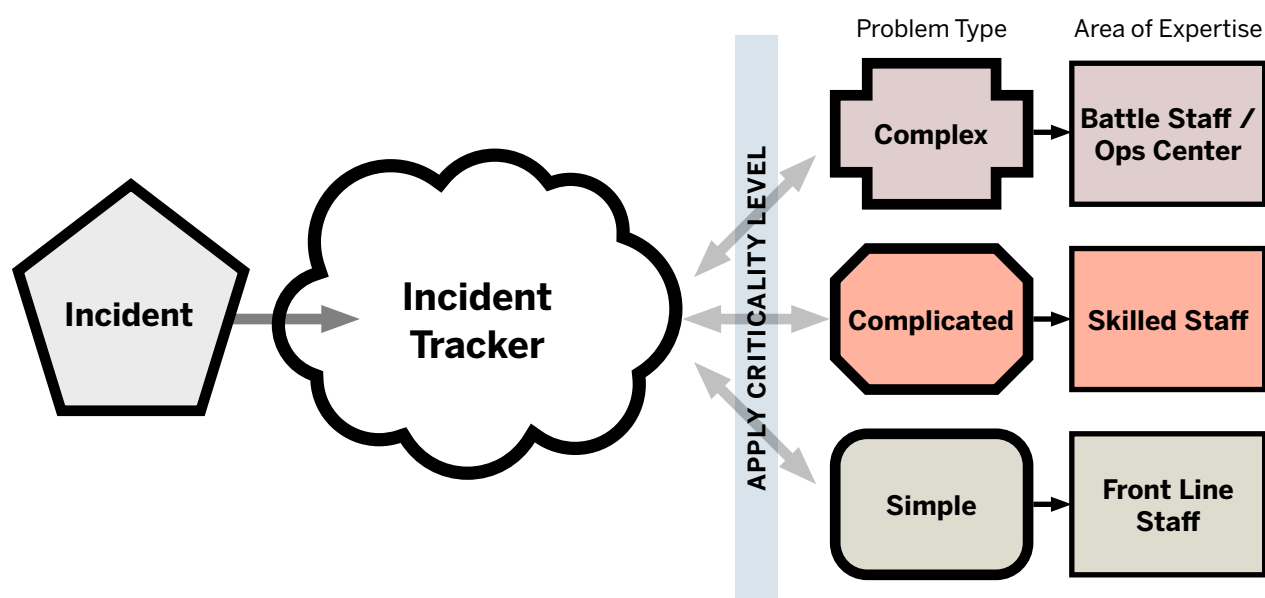
3. Taking Action: Election Incident Tracking, Analysis, and Response

Incident management processes serve as the connective tissue for seamless integration of people, resources, and information. Not only does the process enable detection and identification of issues but it also empowers streamlined responses that prevent escalation and allow operations to recover faster. Establishing an organized and easily analyzed incident tracking system ensures that insights, decisions, and issue resolution are derived from the right context and information. Incident tracking allows leaders to remain informed about conditions on the ground and provides visibility of their teams' responses to issues being faced in the field. In addition to the real-time benefits to empower informed decision-making, these systems also help improve future operational performance by using the information to identify areas that need more attention before the next voting period.



Pro tip: Conduct After Action Reviews (AARs) following operational events to identify what worked well and what can be improved upon. For things that can be improved upon, identify an action officer who has lead for making the changes.

To set the stage: it is important to understand the components of your incident management process and how they all come together. The flowchart below shows how incoming incidents can be recorded, prioritized, and triaged based on criticality. Then, based on the criticality category and issue type, the incident is matched with the appropriate staff element to resolve it.



Systems that enable sharing and aggregation of information across localities, states, and the country can help to identify trends. Often, incidents are not isolated to a single state or locality. This is important because without bigger picture data analysis, you may overlook critical issues that, in isolation, seem minor or insignificant.

When developing an incident tracking system, keep in mind three questions in deciding what information to capture:

1. *What information do I need in order to make decisions?*
2. *How will information be input, collected, and analyzed?*
3. *How will the system enable and empower everyone involved to have the most accurate information at a given point in time?*

The following steps walk you through setting up and implementing your own system.



Case in Point: Getting Stronger Together through “Up and Out” Collaboration

Given the interconnectedness of the financial services, no company can operate in a silo when it comes to incident prevention and response. A breach within a bank, for example, can very quickly expand to ATM networks, payment providers, clearing and settlement entities, and third-party services.

This has prompted competitors to collaborate for the good of the financial services industry. In October 2018, for example, the companies of an industry working group, called the P20 Cyber Working Group and Board, visited the IBM X-Force Command Cyber Range in Cambridge, Massachusetts, to test incident response communications, decision-making effectiveness and stakeholder notification during an incident. This resulted in strengths, weaknesses, and opportunities being identified. A SWOT (strengths, weaknesses, opportunities and threats) analysis was performed and shared between and among companies. The exercise was a first step in establishing inter-organizational coordination among leadership and cross-functional teams during an incident.²

2 Gary B. Meshell, “How the Financial Services Industry is Preparing to Avoid and Respond to Systemic Cyberattacks,” SecurityIntelligence (Cambridge, MA: IBM, 2019), <https://securityintelligence.com/how-the-financial-services-industry-is-preparing-to-avoid-and-respond-to-systemic-cyberattacks>.

Step 1. Identify Critical Information Requirements (CIRs)

Elections teams will be faced with hundreds—if not thousands—of pieces of data. While it is important to log as much as is operationally feasible, you also want to ensure that your Battle Staff and leaders are focusing on those issues that are most important. In the military, information determined necessary to report is often defined by Critical Information Requirements, or CIRs. Applying the concept to elections operations, CIRs are ultimately approved by the team's senior official (e.g., election director) and help the elections team understand time-sensitive issues that could result in mission failure. These requirements are then further broken down into criticality levels based on their severity.

CIRs need to address the full scope of issues that impact election operations or election integrity. CIRs also need to be actionable and identifiable to everyone on the elections team. Good CIRs are questions that will provide important answers requiring action.

Weak CIR: Is voting at precincts going well?

This question is both **vague and subjective** – making it **harder to answer** as a matter of fact and less likely that issues will be consistently raised by all team members, regardless of their level of training.

Strong CIR: Are there any locations where voters are waiting longer than 30 minutes to cast their vote?

This question is **clearly interpreted** by any team member, regardless of training, and it establishes a **clear objective** standard.

Teams at all levels—from precincts to states—should have CIRs. Begin with CIRs from one level up: if you're a local jurisdiction, start your development with the state's CIRs. Then look internally to your own operations and develop local CIRs.



Pro tip: Your CIRs should be a dynamic list that allows for real-time flexibility as you uncover new indicators or identify issues of emerging relevance.

Incident criticality levels are a structured method of prioritizing CIRs based on the incident's impact to critical operational systems and the overall operating environment. The following chart identifies the criticality levels for elections based on the incident's impact on the integrity of elections and scope of resourcing needed for resolution.

Criticality Level	Impact Description	Area of Expertise	Problem Type
1	<p>Very High: Broad election impact. Can affect the integrity of the election. Any incident that will likely result in media coverage. Requires senior-level engagement and external coordination to resolve. Must be reported up and out.</p> <p>When numerous Level 2 events exceed normal quantities (compared to previous voting baselines).</p>	Battle Staff/ Ops Center	Complex
2	<p>High: Resolution requires expertise and critical thinking. Coordination and external reporting may be required, but does not affect the integrity of the election.</p> <p>When numerous Level 3 events exceed normal quantities (compared to previous voting baselines).</p>	Battle Staff/ Ops Center	Complex
3	<p>Medium: Cannot be addressed by Firstline. Incident escalated for resolution by staff with subject matter expertise.</p> <p>When numerous Level 4 events exceed normal quantities (compared to previous voting baselines).</p>	Skilled (potential coordination with Ops Center)	Complicated
4	<p>Low: Resolution can be handled by following SOPs. It does not need to be escalated, but needs to be documented.</p>	Firstline	Simple

For people to prioritize CIRs and pass information, they need to know what the CIRs are. Local jurisdictions should provide each voting location with its specific CIR list to enhance consistency in reporting and reduce human subjectivity when determining whether someone at a higher level needs to know—CIRs make that clear. The chart below shows a CIR list organized by criticality level:

CIRs	Criticality Level
<p>Has the integrity of the voter registration database been compromised?</p> <p>Has the accuracy of results been compromised?</p> <p>Has the integrity of ballots or ballot definition files been compromised? (i.e., Are contests listed multiple times or left off of ballots entirely? Do ballots have candidates missing or in the wrong contest?)</p> <p>Has the election-night reporting website been defaced with misleading information?</p>	1
<p>Is an incident going to force the voting location to open late?</p> <p>Is voting equipment error impacting overall voting location operations, resulting in voter inability to cast ballots?</p> <p>Will the voting location need to be relocated?</p> <p>Is an incident or circumstance requiring voting hours to be extended?</p> <p>Is an incident going to significantly delay reporting of results? (i.e., a jurisdiction having issues connecting to the statewide election-night reporting system at or after the close of polls?)</p>	2

<p>Is voting equipment error impacting overall polling site operations but not affecting voters' ability to cast ballots?</p> <p>Is the voting location low on ballots?</p> <p>Is a group electioneering at multiple voting locations?</p> <p>Is there a problem with the voter look-up tool?</p> <p>Are there materials that need to be sent out to the voting location?</p>	3
<p>Is the voter looking for a voting location?</p> <p>Is the voter just verifying registration status?</p> <p>Is the voter informed that she/he can vote a provisional ballot, and how to verify whether or not it is counted?</p>	4



Get Prepped: Identify your CIRs and criticality thresholds. Create small reference cards that serve as CIR quicksheets and distribute them across your staff. From election workers and call centers to your Battle Staff, these quicksheets will enable your team to always know what they should focus on and report.

Step 2. Capturing Critical Incident Data

Next, you need to find a way to capture critical information reporting at scale. Think about the source(s) of the data and how the data will be integrated into the system and used by the team—what information is useful for your team to be successful and responsive? The greatest barrier to use for any information reporting system is time—there is rarely enough of it when you are running operations, so anything that takes too much time to input information will be a burden. The user interface should make inputting incidents as quick and easy as possible. An overly onerous capture process is more likely to be a deterrent than a useful tool.

If you do not capture data, it cannot be tracked and managed effectively. The best source to input data is the one closest to the problem. However, we know that is often the chief election worker and that may not always be possible. To ensure that incidents are captured completely, every election staff member must have access to enter data they are receiving. Staff must also be assigned to monitor and input issues they identify from the internal IT networks, social and traditional media, and other external dependencies. Ideally, all these incidents should be collected and tracked through a unified incident tracking system.

The Incident Response Team and Deputy Director provide oversight of the incident listings to ensure that they are adequately reflecting the appropriate criticality level. Initial reporting levels should be pre-determined by incident type with the option to adjust as needed. Here's an example, an initial incident is reported by a poll chief to their assigned rover. The rover identifies the issue requires greater technical knowledge, and calls the Battle Staff field support team staff. The field support team staff does not have resident expertise to provide immediate resolution, but confirms incident data on the incident tracker, then assigns to County IT staff for technical assistance. The Incident Tracking team oversees task delegation—making sure IT is tracking it and that it gets resolved.

There are different types of tools to capture and display data (Step 3 will get into critical information displays). Some examples observed during D3P field visits that are already being utilized by elections offices include: county-level subscriptions to emergency management tracking tools such as WebEOC; general collaborative work management programs like SmartSheets; and election specific programs like Asked. If you do not have the resources to implement a software program, any data sheet that can be shared with multiple users in real time can achieve some of the most important functions. The D3P team put together an example incident management tracker leveraging Google Sheets.³ For more information on this example contact D3P at connect@d3p.org.



Pro tip: You can pre-program your incident tracker to auto populate certain data fields based on the user information (i.e., some data is automatically captured or pre-registered, such as the voting location and timestamp). This will save time and increase ease of use, especially at the voting location level.



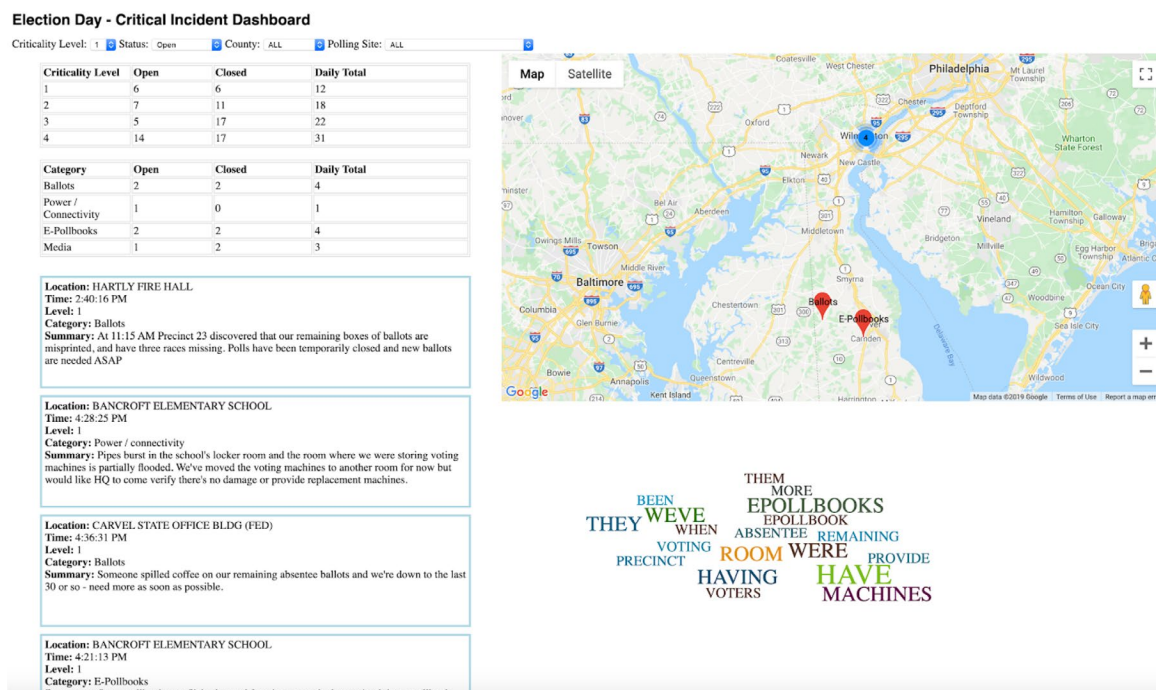
Get Prepared: Identify what systems you already have available to leverage for incident tracking and if they meet your requirements. Bring the team together to discuss best methods of implementation and potential obstacles to use. Create SOPs that make incident tracking efficient and effective so it benefits all levels of operation, from the voting location to the Election Director.

3 This is not intended to be an exhaustive or endorsed list, but rather, to offer suggestions on readily available tools that can be adapted. Encryption, data retention/logs, legal requirements, accessibility, compatibility, cost, and organization are among the many factors that should go into this decision.

Step 3. Feeding Critical Incident Data into Dashboards

Once information is captured, it is fed into dashboards (tools to visualize important data and signals) in the Operations Center and for analysis beyond the Ops Center. You can set up different types of dashboards depending on which information is most important in maintaining the Battle Staff team's situational awareness and oversight of operations. Predefined dashboards that provide views of the data ranging from a detailed to summary level will help you and your teams stay focused and prioritize tasks.

In the Operations Center, having a display of the current top issues is critical. In an ideal situation, as discussed below, this will include visualization components that help members of the Battle Staff quickly identify which high criticality incidents are active throughout the election jurisdiction and what is being done to address them. In the most minimal case, this could be as simple as a filtered view of a spreadsheet that only shows the highest-priority and most complex issues. Regardless of the approach, it is essential to keep this dashboard at a strategic level (executive summary).



D3P's example Incident Dashboard includes three separate fields:

1. Incident Criticality and Type Overview: provides a summary overview of what is going on by criticality level and incident type. In the top left, the tables show the total number of incidents and how many are open or closed (resolved). This allows the staff to know which issues to focus on or if an unexpected trend is emerging (i.e., there's a higher number of VRDb issues than normal during a period of time). This data is most effective when it can be compared to a baseline created from previous voting period data. On the bottom right is a word cloud based on the description inputs of incidents, which helps visualize commonalities that may be otherwise missed.
2. Top Individual Incident Summaries: provides a snapshot of the most critical issues that are still open and need resolution. This should be limited to a handful of the most important issues, based on CIR levels.
3. Map: highlights issue areas in the jurisdiction. In general, the incidents and counts that display on the map should align with the filters most relevant to the viewer. For the Battle Staff in the Ops Center, for instance, only high-priority incidents are displayed, or areas with a density of lower-priority incidents at a high volume. This helps the Battle Staff identify their hot zones and plan more efficiently in resourcing support and incident management.



Pro tip: In addition to the Ops Center Dashboard, you can also maintain a dashboard on your personal computer that displays fields most relevant for your key tasks. For instance, if you are responsible for monitoring media, then you may want to prioritize or include a dashboard table that focuses on media-related incidents. This will save time and increase ease of use, especially at the voting location level.

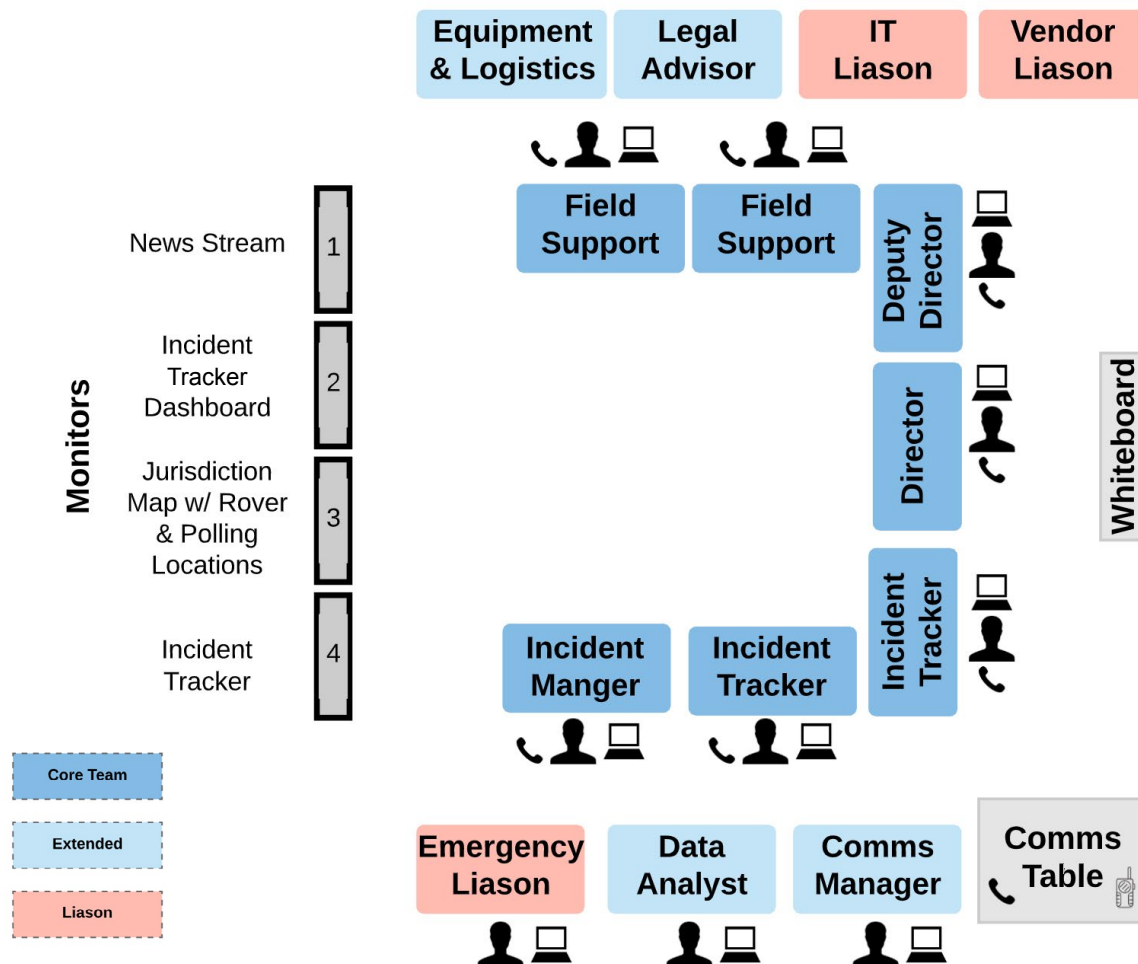


Get Prepped: See what types of dashboards your incident tracking system is capable of displaying and what critical fields it cannot. For those it cannot, find another way to track that information (i.e., there is no mapping tool to put precinct locations and rover jurisdictions/locations on, so use large, laminated paper map instead that you can physically update with incidents throughout the day).

4. Bringing it All Together: The Operations Center

The Operations Center is the centralized location where a leader and key staff come together to command, control, and coordinate all operational activities. Through sustained situational awareness, the Ops Center manages ongoing operations, mitigates preventable issues, solves complex problems, and disseminates key communications and information. An Operations Center is *not* where everyone on staff hangs out, and it is not open to the media, political parties, and external entities (except for demonstration purposes to highlight the capability to these and other stakeholders).

Here is an example of an Ops Center physical setup at the most basic level:



[Appendix B includes some Department of Defense examples designed for larger Ops Centers.]



Pro tip: An Ops Center can be located in any size space, on any budget. While there are always preferred conditions, you can make anything work. The most important thing to remember is that you want to have the right people with the right information and the processes to enable and support them. Don't forget to have a plan for where to relocate your Ops Center in case an emergency forces you to move.

Regardless of the layout, the room should maximize leaders' access to information. As a first option, place display screens on the biggest wall and the leadership in the middle with their key staff surrounding them. Position other team members so that the data flows most critical to them are also easily visible. This will provide the greatest situational awareness while also enabling ease of communication among team members. The following are examples of communication methods to share real-time information and ensure broader group situational awareness in the Ops Center:

- Chat group with polling chiefs and rovers.
- Internal Battle Staff chat group.
- Election Day Cyber Situational Awareness Room operated by EI-ISAC. The room provides a centralized information sharing platform for the [election's](#) community and federal partners regarding cybersecurity threats to election infrastructure.

Operations Center Information Displays

Information displays, specifically the incident tracker dashboard, are huge force multipliers in the Operations Center; these resources improve your situational awareness and help to prioritize (and periodically reprioritize) where the Battle Staff is focusing time and energy. Continuously displaying critical information provides everyone with a common operating picture and ensures the entire team's situational awareness. With good information flow, the team can see signs of problems and stop them before they start, effectively assessing problems in the context of their scope and scale.

Screens should at a minimum display the following:

1. *Local News.* Provides real-time traditional media reporting on the jurisdiction for situational awareness and beyond for contextual awareness.
2. *Incident Dashboard.* As discussed in the previous section, this tool provides a strategic-level overview of the elections operating environment and issues being faced in the field.

3. *Jurisdiction Map with Voting and Rover Locations.* Elections happen in the physical world; it's important to reflect that in your Ops Center and see how the operating environment comes together in terms of resourcing, people, and other externalities. Being able to see jurisdiction boundary lines and voting locations can help with understanding an incident or series of incidents. The setup can be as simple as printed copies on the wall or as sophisticated as integrated mapping programs that incorporate overlays such as traffic, road closures, and GPS tracking of the rovers.



Pro tip: For jurisdictions that provide cell phones to their rovers and election workers, enabling a GPS location tracker on the phone can provide critical information for real-time decision-making. For instance, if there are three locations in a rover's region that are having issues, other available rovers can be reallocated to assist based on their proximity.

Most smart phones offer native integrated location sharing services, which can be a free option. A wide variety of software is available as well for personnel/fleet management applications that can display digital map overlays. Other agencies in your jurisdiction, such as emergency services or road management services, may have such software already available that you can use. Be careful when selecting applications to make sure they are trusted and that you understand all the embedded features.

Getting the Operations Center into a Battle Rhythm

While elections are fluid and have lots of unknowns, it is critical to provide structure to ensure proper sharing of information. An easy way to capture these important events is by developing an Operations Center battle rhythm: a deliberate schedule that captures a cycle of activities, specifically scheduled information sharing, in order to synchronize current and future events. An effective battle rhythm will enable a team to create shared understanding and set conditions for mission success through a predictable coordinated schedule.

Battle Rhythm Example

0600	Battle Staff and Rovers Initial Guidance Brief
0700	Voting Locations Report Prepared to Open
1100	Midday Issue Update Brief (Battle Staff and Rovers)
1300	Scheduled Midday Media Update
1600	Mid-Afternoon Issue Update Brief (Battle Staff and Rovers)
1900	Polls Close

Standardizing Operations Beyond the Battle Staff

You can't see everything that's coming, but you know certain issues will inevitably emerge. A clear response plan for the "knowns" will leave space to think about and react to the "unknowns." Identify anticipated incidents based on past election experiences. Develop and implement SOPs for methodical logging, troubleshooting, resolution, and communication of common, recurring incidents. Practice using these SOPs in any simulations or dry runs so that they become second nature. Also, capitalize on opportunities during early voting periods to identify patterns and issues getting commonly escalated, as well as test the effectiveness of SOPs.

Here are a few ideas of election SOPs that will increase a team's effectiveness:

- **Call Center FAQs:** step-by-step process on how to answer the most common public questions (where is my voting location, when does it open, etc.).
- **Call Center Voter Registration:** step-by-step process for how to do voter registration lookups to confirm voter registration status and voting location.
- **Voting Location Equipment:** a printout guide for resolving the top 10 technical issues with your voting equipment; what they are and a step-by-step guide on how to troubleshoot each one.
- **Voting Location Common Operational Irregularities:** step-by-step process for dealing with the typical voting irregularities and processes that election workers must manage. This can include provisional voting, a voter who received a vote by mail ballot but shows up at the voting location, or electioneering.



Get Prepped: Do practice runs as a Battle Staff in the Ops Center and with the broader election staff. Test your SOPs and PACE plans.

Next Steps: Making It All Happen

You now know the building blocks to establish an effective Elections Battle Staff and Operations Center. It's your time to begin preparing, and the clock starts *now*.

First, review the **Top 10 Takeaways for Building Your Battle Staff** from this Playbook and look over the **Get Prepped Checklist** to guide your high-level planning. Refer to the **Pro Tips** for additional guidance.

Next, practice. Remember: when things get rough, people don't always rise to the occasion—but often fall back on what they know. That's why the military spends so much time training and rehearsing. That's also why private sector companies invest in war games and tabletop exercises. And that's why professional sports teams spend so much time out on the field between games. We play like we practice. So practice being a cohesive Battle Staff, iron out wrinkles during early voting periods, and the repetition will make sure your team is ready.

The challenges to elections keep evolving and so must we. The decentralized, vulnerable nature of our election system makes it complex to defend. Therefore, we must be stronger, better, and faster with the resources we have. The Battle Staff model, along with its practices and processes, will help any elections team improve efficiencies and increase effectiveness.

Appendix A: Get Prepped Checklist

Preparation requires setting up systems in advance, teaching people the purpose and intent of what they are doing and allowing them to practice in order to better understand their roles and those of others. This checklist consolidates these key actions from throughout the playbook.

People and Purpose

- ☐ Map out your election ecosystem. Identify what entities the elections office has operational control over or a coordinating relationship. In coordinating relationships, identify where liaisons already exist and where new ones are needed to fill gaps.
- ☐ Identify your entire election staff: frontline, staff, and battle staff. Organize your staff so that each element has a clearly defined task and purpose. For those on the frontline, use develop and implement SOPs to assist with managing known issues in a consistent and efficient way. Develop an SOP for incident reporting that will inform the task and purpose of different staff members.
- ☐ Identify who will be filling each staff role in advance, including liaisons from external entities. In some jurisdictions, one individual may have multiple roles. In others, many people might be required per role. Have a staff roster published and distributed in advance so people know who the appropriate touch points are.

Shared Situational Awareness through Communication

- ☐ Based on your staff task organization and your mapped elections ecosystem, identify your “down-and-in” and “up-and-out” communication paths. Plan for these in advance by creating standard report formats, distributing necessary equipment, providing contact rosters, and coordinating with external entities for scheduled information sharing events.
- ☐ Identify what options exist for different communication paths and decide which method best meets your requirements. Equipment purchasing or software downloads/updates may be required and should be integrated into your election operations overall preparation.

- ☐ Develop a contact roster. It should contain contact information required for the PACE Plans you developed (email, phone numbers, usernames for chat platforms).
- ☐ Share the contact roster across the network. Schedule when you'll make updates (e.g., to replace or add team members) and ensure that teams have the up-to-date version. Add a **version number** and **date of last update** to your contact roster.
- ☐ Test your PACE Plan: Schedule a rehearsal PACE Plan Test for each communication path. Make changes to the PACE plans when needed and ensure that everyone knows about the change to the SOP. Also confirm that everyone on the team knows how to use your communication tools and that all tools are working properly (e.g., items are charged/have batteries, you've tested for technical problems).
- ☐ For Scheduled and Unscheduled Information, develop standardized reporting formats in advance and distribute them to your staff. These should be incorporated into your SOPs.

Bringing it All Together—Your Election Operations Center

- ☐ Do practice runs as a Battle Staff in the Ops Center and with the broader election staff. Test your SOPs and PACE plans. Here are a few example areas where SOPs could improve efficiency and effectiveness in issue resolution.
 - ☐ **Call Center FAQs:** step-by-step process on how to answer the most common public questions (where is my voting location, when does it open, etc.).
 - ☐ **Call Center Voter Registration:** step-by-step process for how to do voter registration lookups to confirm voter registration status and voting location.
 - ☐ **Voting Location Equipment:** a printout guide for resolving the top 10 technical issues with your voting equipment; what they are and a step-by-step guide on how to troubleshoot each one.
 - ☐ **Voting Location Common Operational Irregularities:** step-by-step process for dealing with the typical voting irregularities and processes that election workers must manage. This can include provisional voting, a voter who received a vote by mail ballot but shows up at the voting location, or electioneering.

Appendix B: Operations Center Physical Layout Models

Below, we outline four common operations center layouts favored by the Department of Defense. These can be adapted for varying sizes of offices from the local municipality to large county or state level. The “clustered positions” layout allows for personnel to work in teams or groups; the “rows facing displays” layout allows all personnel to be focused on a common area for information; the “V positions facing display” layout allows personnel to work in groups while facing displays; and the “conference arrangement” is best used with smaller groups and works well when personnel need to focus on a common discussion. These options are not mutually exclusive, and depending on the needs of the state or locality, a hybrid of these options may be most suitable.

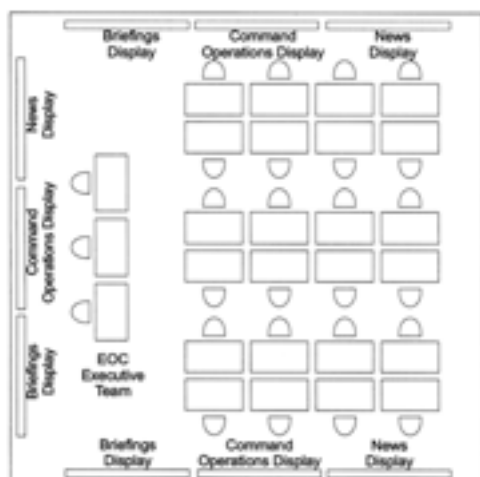


Figure 1: Clustered Positions

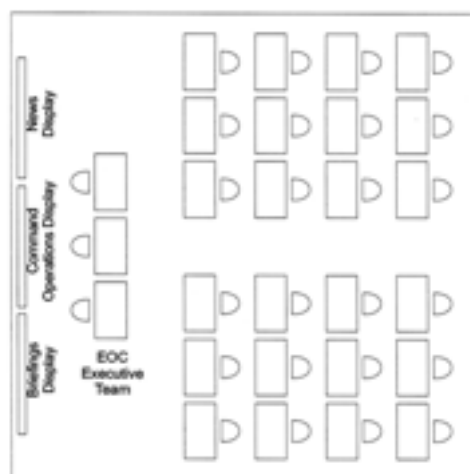


Figure 2: Rows Facing Display



Figure 3: “V” Positions Facing Display

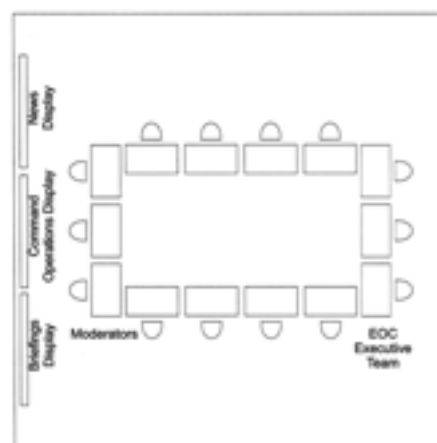


Figure 4: Conference Arrangement

Appendix C: Leadership and Teamwork in Action

This Playbook is based on three leadership philosophies used by high-performing organizations—from military task forces to public- and private-sector incident response teams. We believe the key to leadership is harnessing the power of people to address simple problems and focus energy on the complex. These concepts are critical in making that a reality.

Mission Command

The U.S. Army's Mission Command philosophy focuses on how commanders, supported by their staffs, combine the art of command and the science of control to understand situations, make decisions, direct action, and accomplish missions. Leaders plan, prepare, and execute, all while continuously assessing the operation to ensure mission success.

Mission Command is guided by principles of cohesive teamwork, shared understanding, clear guidance, and empowered, disciplined initiative. These principles increase efficiencies, cross-level information, and allow leaders to make the most informed decisions possible.⁴

Swarm Leadership

Proponents of Swarm Leadership believe that when leaders across the organization all base their decisions on the same guiding principles, the organization is able to accomplish more than any single leader alone. This philosophy requires properly organizing staff and defining clear roles, so that problem ownership can be delegated to the appropriate level. Staff at every level of the organization are applying the same guiding principles with a clear focus on the same goal: *"How can I help make the election a success?"*

The Swarm Leadership philosophy is based on five guiding principles. As you build your structure, communication channels, and decision-making protocols, ask yourself if they are consistent with these principles.⁵

4 Army Doctrine Publication, "FM 5-0 The Operations Process," in Field Manual No. 5-0 (Washington, D.C., Department of the Army, 2010), <https://armypubs.us.army.mil/doctrine/index.html>.

5 Lenny Marcus, "Five Leadership Principles We Learned from the Boston Marathon Bombing," National Geographic Blogs (Washington, D.C.: National Geographic Partners, LLC, n.d.), quoted in Eric McNulty, "Five Principles for Leading the 'Swarm,'" Cambridge Meta-Leadership (Brookline, MA: Cambridge Meta-Leadership, 2017), <https://cambridgemetaleadership.com/five-principles-for-leading-the-swarm/>.

Swarm Leadership Principle	Election Application
Unity of Mission	<p>Why we are here and what we are trying to achieve:</p> <p>1) Protecting free and fair elections</p> <p>2) Preserving the public's trust and confidence in the democratic process</p>
Generosity of Spirit and Action	<p>One team, one fight. We may all be responsible for different areas across the country, but at the end of the day, we can help each other achieve our shared mission. We do our best work together. Helping one another is critical to achieving our mission.</p>
Stay in Lanes/Help Others Succeed	<p>We share ownership by delegating responsibility and ensuring all key tasks are covered. We fulfill our assigned tasks. We help out and step up when the situation calls for it.</p>
No Ego, No Blame	<p>This is not about us as individuals. This is about us as a team—one American team. Mistakes will happen; we all make them. Vulnerabilities exist; we all have them. Sharing and getting stronger is what matters.</p>
A Foundation of Relationships	<p>Trust and confidence in one another leads to success.</p>

Meta-Leadership

Meta-Leadership focuses on developing a shared course of action across organizational lines. Effective meta-leadership produces a seamless integration of people, resources, and information that allows the organization to “catch (detect and report), respond (control and contain), and return to pre-event normal (recover)” from any incident.⁶ Just as with successful communication, this approach requires leadership across multiple levels of operation—up, down, and across. Meta-leaders understand that to effectively guide complex operations, they need to do the following: see how small things are part of a larger picture; engage and involve other stakeholders; anticipate and integrate change; and in taking all of these steps, wield influence and deliver impact beyond their own immediate authority.⁷

Meta-leadership also highlights the importance of training leaders and team members to thrive in high-stress, complex environments. Humans exhibit a biological reaction to stress. The brain’s amygdala overtakes rational thinking and turns to the basic survival instincts of freeze, flight, or fight. Meta-leadership calls this “going to the basement.” A complex environment—like an election—requires more than a simple freeze/ flight/ fight response. Team members “in the basement” are not able to react sustainably or effectively to the problem at hand. A meta-leader gets them “out of the basement.” Training and preparedness allow us to do this by teaching us patterns and skills that we can fall back on during a crisis. Having these skills as second nature allows us to move past the basic survival instincts, out of “the basement,” and up to the “workroom” to develop necessary responses to the challenge. With advanced training, leaders can also develop the ability to move themselves beyond the workroom to the “laboratory,” where they can develop creative solutions and new patterns, even in moments of stress.



6 Kristopher W. Shrader, Designing an Effective Emergency Operations Center for the City of Martinsville, Virginia (Martinsville, Virginia: Martinsville Fire & EMS Department, n.d.), <https://www.hsd1.org/?view&did=719492> [Accessed November 25, 2019].

7 National Preparedness Leadership Initiative, “Meta-Leadership,” (Cambridge, MA: Harvard T.H. Chan School of Public Health, n.d.), (Cambridge, MA: Harvard T.H. Chan School of Public Health, n.d.), <https://npli.sph.harvard.edu/meta-leadership-2> [Accessed November 25, 2019].

Do you see a way to make this Playbook better?

We can continue to improve this resource as the digital environment changes.

We want your feedback.

Please share your ideas, stories, and comments on Twitter [@d3p](#) using the hashtag [#BattleStaffplaybook](#) 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