# Preparing for Election Day Disruptions



Election Day disruptions pose significant risks to the integrity and stability of the electoral process. The primary aim of preparing for such disruptions is to ensure the safety and security of voters and election workers, maintain public confidence in the election process, and guarantee the continuity of election administration operations. Effective preparation involves establishing a robust preparedness and training baseline, developing comprehensive crisis communication strategies, and fostering coordination with local, state, and federal agencies. By proactively addressing potential threats and disruptions, election offices can mitigate risks, manage crises efficiently, and ensure that elections proceed with minimal interruptions.

Effective partnerships with local and state law enforcement are crucial for preparing and responding to Election Day disruptions. These partnerships ensure that election officials have access to the expertise, resources, and support needed to address security threats and maintain public safety. Collaborative efforts include joint training exercises, sharing critical information, and establishing clear communication protocols. By working closely with your local first responder community, election offices can develop comprehensive security plans, conduct risk assessments, and coordinate responses to potential threats effectively.

Similar to establishing partnerships with local and state law enforcement and emergency management officials, it is crucial to establish relationships with all relevant media outlets in your jurisdiction, including print, digital, and T.V. In a crisis involving voting and public safety, transparency and communication are key. Identify points of contact for media outlets and cultivate these relationships to ensure your ability to provide the general public timely and relevant information during a crisis.

## Have Collaborative Discussions

Effective collaboration between election officials and law enforcement is essential for creating a resilient relationship where both sides understand and support the other's mission. Law enforcement must recognize the critical importance of maintaining election operations continuity despite potential disruptions. Concurrently, election officials should understand that law enforcement views election disruptions through the lens of public safety and criminality. By establishing predefined roles and fostering mutual understanding, both parties can efficiently support each other's core mission objectives and ensure the electoral process's integrity while maintaining public safety.

Download and tailor CIS's `Guide for Collaborative Discussions on Election Disruption Preparedness` to help facilitate these discussions.

## Examples of Election Day Disruptions

**Bomb Threats**

Bomb threats involve communications about the presence or intent to detonate explosives, causing disruptions, panic, and resource strain in election administration. These threats aim to disrupt or extort. Managing these threats requires assessing the threat, establishing communication protocols, and coordinating responses with law enforcement to ensure the safety of voters and election workers. While the use of "empty" bomb threats as a tactic of disruption has increased over the past several years, the use of actual bombs as a form of terrorism is still very real. All threats should be taken seriously validating the importance of coordinating with local law enforcement officials and other first responders.

**Swatting**

Swatting involves providing false information to law enforcement to trigger a tactical response by law enforcement, endangering election and law enforcement officials while also diverting resources from actual emergencies. While swatting has traditionally focused on individual targets, election-related disruptions may include the targeting of precinct locations, ballot counting facilities, and drop box locations. This both disrupts operations and poses significant safety risks. Preventing and mitigating swatting requires collaboration and information sharing with law enforcement.

**White Powder Hazards**

White powder incidents aim to cause fear and disrupt election administration operations. White powder hazards are most commonly sent via mail; however, the scattering of white powder at a polling location or dispersing it into or around a ballot drop box could disrupt voting and create fear among the electorate and election support staff. Preparation includes training staff to handle suspicious packages, maintaining communication channels, and having protocols for safe handling of mail to minimize disruptions and ensure voter and staff safety. White powder hazards can overwhelm the response capacity of local officials, particularly in smaller jurisdictions, making it essential to discuss this potential threat with your jurisdiction's first responders.

**Other Election Day Disruptions**

Election Day disruptions can include but are not limited to protests and counter-protests, active shooters, threats of violence, and other activities that, directly or indirectly, may interfere with the electoral process. These disruptions pose safety hazards, deter voter participation, and undermine the election's integrity. The risk of multiple simultaneous disruptions, such as a bomb threat coinciding with a protest outside the office, can complicate evacuation plans. Preparedness requires close coordination with law enforcement, fire, and emergency management officials; robust security measures at all election sites; and clear communication strategies. Having backup plans and effective communication with first responders is crucial to manage complex scenarios and ensuring the safety of voters and election workers.

## Goals

1. Prepare your office for potential disruptions (Level 1 maturity)
2. Establish partnerships with local first responders and the community (Level 1 maturity)
3. Prepare and execute on your communications approach (Level 1 maturity)

## Actions

For Preparing for Election Day Disruptions, the necessary actions are the same for all maturity levels.

### Prepare your office

1. **Assign and Coordinate Roles**: Ensure clarity in duties for all staff during any potential disruptions.
2. **Appoint a Point of Contact (POC)**: Make someone in your office accountable for coordinating emergency contacts and responses.
3. **Budget Assessment**: Allocated resources to implement security and COOP plans.
4. **Develop a Detailed Security Plan**: Include protocols for managing various disruptions and consider using CISA's Protective Security Advisors program for no-cost support.
5. **Brief Election Staff**: Provide all election staff with the knowledge and tools needed to respond effectively.
6. **Ensure COOP Readiness**: Develop, maintain, practice, and make a Continuity of Operations Plan (COOP) readily available. Consider the EAC Continuity of Operations Plan Template.

### Prepare your partners and community

1. **Establish Initial Meetings**: Engage local law enforcement and security agencies to discuss collaboration and establish communication channels.
2. **Define External Partnership Scope**: Outline the scope and guidelines for a partnership with your local law enforcement counterparts. Consider creating a memorandum of agreement, ensuring a clear framework for cooperation.
3. **Conduct Joint Training and Exercises**: These can include simulations of various disruption scenarios, such as bomb threats or active shooter situations, ensuring that all parties understand their roles and responsibilities during a crisis.
4. **Share Information**: The locations of polling places and contact information for key personnel helps law enforcement plan and respond more effectively to incidents.
5. **Establish Communication Protocols**: Ensure swift and appropriate responses by designating points of contact and using secure communication channels.

### Prepare your communications approach

1. **Internal Communication**: Cross-train staff for multiple roles and establish protocols for different disruptions using email, phone, text, or in-person communication to keep staff informed in real-time.
2. **External Communication**: Establish a communications point of contact (POC) and ensure law enforcement counterparts have POCs. Develop joint communication protocols with law enforcement for coordinated responses and to avoid conflicting statements.
3. **Establish Relationships with Media Outlets**: Ensure local media know who they will hear from for authentic information. Include print, radio, television—anywhere your constituents' get information.
4. **Enhance Online Presence**: Establish accounts as official to so the media and public know where to get factual information.
5. **Leveraging Multiple Channels**: In a crisis, communicate through ever means available to you.
6. **Pre-approve Messaging**: While every emergency is unique, have approve template for potential crises to shorten your response time and get ahead of rumors and falsehoods.
7. **Engage the Community**: Build trust and cooperation between election officials, law enforcement, and the public to enhance overall preparedness and ensure a more coordinated response to disruptions.
8. **Post-Election Review**: Review, discuss, and update plans after every election. Consider using The Elections Group Crisis communications toolkit.

## Cost-Effective Tools

- CIS's `Guide for Collaborative Discussions on Election Disruption Preparedness`.
- CISA's Bomb Threat Guide.
- CISA's Swatting Prevention and Response Guidance.
- CISA's best practices for mail screening.
- EAC's Continuity of Operations Plan Template.
- CISA's Training Video Series.
- CISA's Last Mile Tool Kit.
- CISA's Enhancing Election Security Through Public Communications.
- The Committee for Safe and Secure Elections Resources for Election and Law enforcement Officials.
- The Elections Group de-escalation resources.
- The Elections Group Strategies for Increasing Dropbox Security.

## Mapping to CIS Controls and Safeguards

- There are no relevant CIS Controls

## Mapping to CIS Handbook Best Practices

- There are no relevant Handbook best practices.