

Drones in Election Settings

A LAW ENFORCEMENT BRIEFING



This guide is part of the CSSE Briefings for LEOs series, aimed at helping law enforcement understand what makes election settings unique—and how those differences should shape your response.

Standard drone incident response protocols should apply in election settings. What follows is how the nature of the election might prompt you to prepare, and to refine incident response plans.

Five Steps to Safer Elections

CSSE's "Five Steps" is a framework for election and law enforcement agencies working together, with five simple principles:

— **Meet, Share, Agree, Plan, Practice** —

We suggest planning for drone incidents as part of a "Five Steps" process with your local election office.

1 MEET WITH YOUR ELECTION OFFICIAL

Drones should be one topic addressed when you meet with your local election official to discuss security. Consult CSSE's *Five Steps to Safer Elections* for guidance on that first meeting, where you'll exchange numbers, set communications protocols (and liaisons, if needed), and schedule additional meetings as needed.

- **Use the meeting to build a relationship** to ensure you can verify information quickly in a crisis and coordinate an effective response.
- **Ask for a list of election sites**, usually including the main office and the warehouse (which may double as a mail ballot counting site), early voting sites and election day polling places, and the most critical, vulnerable dates and times for each site.

2 SHARE DETAILS OF YOUR OPERATING ENVIRONMENTS

What's Different About Election Settings

One issue that may arise at a voting location which can prompt a police response is **violation of the statutorily protected perimeter**. The size and the restricted activities within this zone vary under state law. Multiple states prohibit campaigning in this area.

- A drone carrying political signage flying inside the protected space while voters are present was recently reported.
- Video of the incident shows an election official attempting to explain relevant state law restrictions to the drone operator.
- Multiple challenges, including identifying the drone operator, may delay and complicate the response from election staff and LEOs in these situations.

More aggressive use of drones, such as for **harassment of voters or election officials**, may be difficult to distinguish from permissible campaign activities.

- Within or beyond the perimeter, aggressive use of drones could be disruptive to voters.
 - Even a drone flying beyond the restricted perimeter (for instance, above a voting site parking lot or a busy sidewalk) may make some voters feel unsafe and trigger complaints.
- In some states, most in-person voting occurs on one day. Disruption by a drone could disenfranchise voters.

- Some threat actors aim to disrupt voting (see CSSE's *Bomb Threats for LEOs* guide). Drones could enable them to target certain voters or voting sites.

Voter intimidation/election interference is a crime under federal and state law.

- Federal law prohibits intimidation that interferes with the right to vote (18 US 594).
- State laws that restrict activity within the protected perimeter vary. States may also have laws on voter intimidation.
- Election officials and law enforcement need to know the relevant statutes and work with local government counsel to clearly understand what activity is prohibited and permitted under state law.

Information You Should Share With Election Officials

Local drone usage: Provide known settings where hobbyists fly (particularly near election sites) and local incidents, if any, such as harassment or corporate espionage.

Regulatory landscape: Election officials are unlikely to be aware of Federal Aviation Administration (FAA) rules, restricted areas, and rules for identifying drones and their operators.

- **Review drone law and protocols.** Law enforcement should approach the election setting with an understanding of statutes

2 SHARE (CONT.)

directly addressing drones (review *Additional Resources* below) as well as state law and any drone protocol adopted by their agency.

- **Consult legal counsel.** The regulation of drones in an election context will vary based on state laws that, for example, prohibit voter intimidation and election interference or protect voter privacy. Work with local counsel to understand the appropriate legal framework.
- **Consider local code.** Cities or counties may have authority to clarify permitted

and prohibited drone usage within their jurisdictions. For instance, a city that experiences voter complaints about close calls with drones might consider the [ordinance adopted by the city of Calabasas, CA](#), which adds prohibitions on flight "closer than 25 feet to any individual."

Your Incident Response Plan: If you have a plan, explain how you respond to drone complaints. This forms the basis for an election incident response protocol.

3 AGREE ON KEY STRATEGIES & PROCEDURES

Election officials are responsible for administering elections. They will be the first to hear reports of misconduct at voting sites, which may include allegations of drone activity that violates state law. Law enforcement is responsible for public safety.

Both agencies have important but distinct roles. Coordinating ahead of an election to reach an agreed understanding of strategy and response steps will improve crisis response.

Incident Command: Command in a drone incident should follow the protocol you establish in an election security plan.

Incident Response: Drone incident response plans may include:

- Incident reporting (who contacts who, and what information is helpful)
- Assessment of airspace and restrictions
- A classification plan for drone activity:
 - **Benign: restricted** (ie, flying in airspace restricted by FAA rules or electioneering law); **harassing** (for instance, flying near individuals); or **dangerous** (dropping items or appearing to carry a payload)
- Identification of and communication with the drone operator
- Tactics if infractions or aggressive/dangerous behavior continues

4 PLAN FOR DRONE INCIDENTS AS PART OF A BROAD ELECTION SECURITY PLAN

Incorporate agreed strategies and tactics into a written incident response plan as discussed in the *Five Steps*.

- **Know the airspace.** Determine whether any election sites are located in controlled airspace, near airports, or in areas with FAA restrictions.
- **Discuss distinctions between election sites.** A drone at a polling place may be engaged in electioneering. At a ballot counting facility, it could be tracking employees to their homes or gathering site security details.
- **Drone law is complex, and drone usage is rapidly evolving.** Consider contacting the FAA's local Flight Standards District Office to understand new developments and any advice or alerts they may provide about election day drone activity.
 - Speak with your attorney about the intersection of federal and state authority over airspace.

OTHER RESOURCES

CSSE | [Five Steps to Safer Elections](#)

Federal Aviation Administration | [Unmanned Aircraft Systems & Public Safety Agencies](#)

Federal Aviation Administration | [Public Safety Small Drone Playbook](#)

5 PRACTICE YOUR RESPONSE TO DRONE INCIDENTS

Once you have a drone incident response plan, work with election officials to practice a coordinated response.

For example, add a drone scenario to an existing tabletop exercise (TTX) or training being conducted for election security. Ideally, the TTX will bring together dispatch, responding officers, and the election office liaison in the same room with election officials to practice coordinated response.

