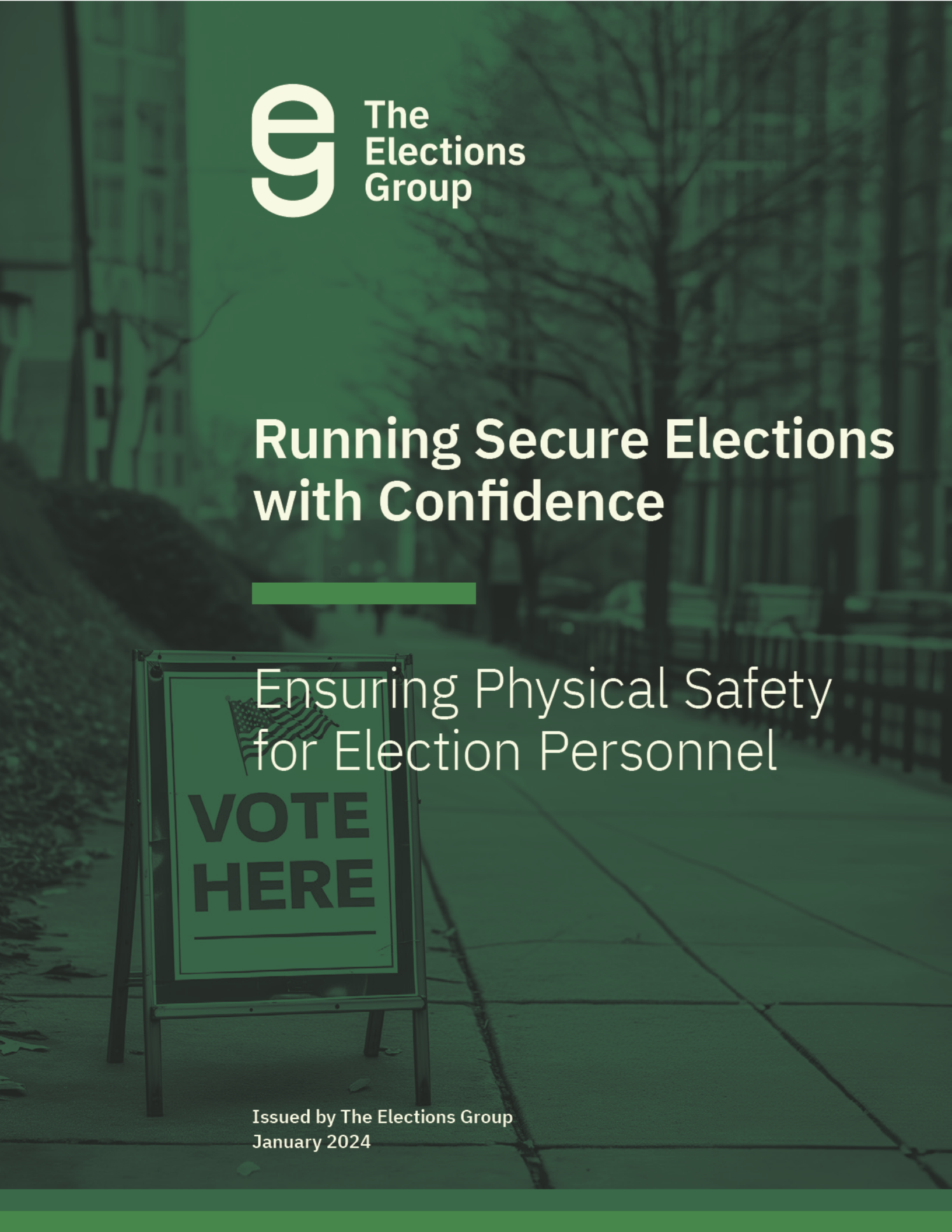
The Elections Group

Running Secure Elections with Confidence

Ensuring Physical Safety for Election Personnel



Issued by The Elections Group
January 2024

Table of Contents

A note from the authors

The authors would like to preface this discussion with some reassurance. The topic of personal security for election officials became part of public discourse due to threatening activities. Such threats take an agonizing toll on a target's sense of safety even if they never result in action. At the time of publication, we are not aware of physical violence carried out against an official for their role in an election in the United States. In the event our country again sees such threats, comprehensive plans exist to provide officials with protection and ensure resilience.

Introduction

So much focus in the past several years has been on security in elections. The potential of cybersecurity attacks shutting down sectors of government helped to stimulate the elections community to closely scrutinize the routines, procedures and equipment utilized by election officials. Election officials have since participated in a wide array of trainings and exercises on these topics to help prevent and respond to physical threats and cyberattacks. Rising to the challenge of "even more to do," election officials steadfastly implemented new policies, new priorities and new equipment to ensure secure elections.

Starting in 2016, election officials became acutely aware of the threats posed by cyberattacks against their offices and elections infrastructure. They responded quickly with structured training and security exercises, enhanced communications and new security protocols. Fortunately, the workforce we depend upon to run and administer elections is a resilient one. This resiliency is evident now, as the elections workforce stands against a new type of election threat: violence against election officials.

The response to this new threat to election officials has been mixed. The roles and important contributions of election officials were recognized not only by bad actors, but also by politicians and policy advocates, working to protect elections and the election workforce.

Bad actors targeted election officials regardless of whether they were elected or appointed, represented swing districts, or were affiliated with a particular political party.

In light of this new threatening activity, legislation was introduced to penalize those who threaten election officials and to provide increased funding and protections to election officials. [1]

[1] According to NCSL, since 2020 11 states passed legislation protecting election officials and poll workers. https://www.ncsl.org/elections-and-campaigns/state-laws-providing-protection-for-election-officials-and-staff

For more than four years, election officials across the country have experienced these threats. The impact is real. A significant percentage of election officials resigned in the wake of these threats, taking with them years and often decades of institutional knowledge.

The reality ahead is that election officials will continue to face threats and violence. Today's election officials, while extremely resilient, face unparalleled exposure to a range of threatening activity. Online threats expose election officials to a greater degree than ever before. Our previous paper, Defending Democracy: Protecting Election Officials From Online Threats, details how digital threats develop, how social media can increase their impact, how threats can have a devastating impact on your sense of security and how you can protect yourself online.

Threats against members of the election workforce and their families are real. Election officials and everyone involved in administering elections, from office staff to poll workers, are open to threats and attacks.

This paper addresses the need for election officials to develop a plan to protect themselves and their staff. From what has been observed on a national level, there is no clear pattern for targeting members of the election workforce, and it is possible that targeting could be done at random. In contrast, online threat behavior follows a set pattern:

1. Misinformation breeds online discontent.
2. Amplifiers recruit an online mob.
3. Threats target real people.
4. Harassment extends to family and friends.
5. Social media delivers attacks.
6. Online attacks move to offline threats.

The seemingly random targeting requires a security plan that is broad enough in scope to protect a wide range of officials and workers. Given that online threat behavior follows a set pattern, security plans can be ready-made quickly implemented if a threatening situation emerges. Attacks on election workers are no longer unthinkable. Election workers can counter them with preparation, quick action, coordinated support from security partners.

There are three aspects of physical security that must be addressed in the plan:

- Building Cooperation with Law Enforcement,
- Heightened Office and Worktime Security, and
- Improving Personal Physical Security.

Building Cooperation with Law Enforcement

Intimidation and violence are crimes for law enforcement to prevent and address. This section suggests strategies to build a relationship with law enforcement so that you can call on them for support when needed.

The Initial Approach: Seek Broad Participation

The first step in engaging law enforcement is meeting with relevant agencies. Consider inviting a range of police agencies, including state and local law enforcement, your local CISA support, your regional FBI field officer and U.S. Marshals. Broad perspectives will improve the discussion, and you might find varying interest in further collaboration. Most large agencies will have a protective services unit (though names vary) responsible for providing security or security advice to judges and the court system, elected officials and others. Representatives from these units will have constructive advice and may be involved in future incident response.

It may not make sense for state and federal agencies to meet with every jurisdiction separately. Consider working with your state association to schedule a statewide meeting or coordinate a regional meeting with surrounding jurisdictions. CISA's protective security adviser can help coordinate since each state has at least one law enforcement "fusion center" designed specifically to ensure information sharing across law enforcement agencies. These federal resources are prepared to support a statewide or regional effort.

Well-defined objectives will lead to a more productive meeting, and a strong agenda will help set the tone. Some of the desired outcomes of the initial meeting may be to achieve:

1. A better understanding of how agencies will share information when threats to physical safety are reported.
2. An understanding of the expected level of service from different agencies involved, including the bar for law enforcement response.
3. An overview of what details or evidence will make it more likely to get enhanced support or protection.
4. An understanding of tools that may already exist to help provide protection and security for election workers, including poll workers.

Build Consensus About Election-Related Violence

You may need to build the case with law enforcement that election threats are unique in their impact to the local and even national community, in their prevalence and that requirements for transparency pose specific security risks You are the best person to contextualize this for your law enforcement partners.

Law enforcement may not be aware of the scale of threatening behavior aimed at election officials. They may not recognize why threats against election officials deserve their heightened attention. You may need to build that case with law enforcement.

The intimidation of election officials impacts not only individuals and their families, but also the foundational institutions they manage. Law enforcement may not be aware that the Department of Homeland Security designates the election facilities and technology managed by local officials as part of our nation's critical infrastructure. Threats made against election officials have a "debilitating effect" on our security and safety at a fundamental level. Because our entire community and nation share the consequences, law enforcement must understand threats in this context and ensure election officials can perform their role without fear of unprotected retaliation.

If officials cannot rely on law enforcement protection, they may be less willing to admit and correct mistakes or explain election results. They may also be less likely to speak on behalf of a colleague. The entire

election community will share the consequences. Because an attack on one may affect the ability of others to do their job, threats against election officials are more impactful to our society than other threats. They require a strong law enforcement response. In recognition of this special status, some state legislatures have introduced and passed laws that apply stiffer penalties for harassment or intimidation when the victim is an election official. As of this writing, 11 state legislatures have passed laws to enhance the protection of election officials.

Law enforcement agencies may be unaware of the seriousness of threats directed at election offices. A quick internet search will reveal the prevalence of such incidents in recent years and demonstrate that threats against election officials are not isolated, rhetorical or harmless ways to let off steam. They are part of a continuum of behavior that has culminated in physical confrontation and violence. Discussing real-word examples will help shape law enforcement perspectives on the risks you face and needed protection.

You must also establish how your workspace is different from others in need of personal or private security. A private office may be able to close its doors to the public, but election work requires openness and transparency. To varying degrees, the public may be permitted to enter your workspace to observe election events. Indeed, groups likely to be dissatisfied and angry at the vote count in your jurisdiction are the very demographics with whom you need to establish legitimacy by offering ample, genuine opportunity to observe all phases of election work. Describing the balance between election security and election transparency is an item to place on the agenda when you meet with law enforcement.

Your goal is to establish a shared understanding that the threat to election workers is real, that significant protective resources may be needed at some point and that it warrants a planning effort in keeping with the principles of transparency that are essential to fair elections.

Ultimately, law enforcement and security staff may be needed to deter violence, and possibly to address threatening individuals and intimidating groups. At the same time, a pervasive law enforcement presence can feel overbearing to some voters. Law enforcement election activity must balance competing demands in very different settings, such as voting locations, mail ballot drop box locations, offices and central count facilities.

Communicate with Law Enforcement

Communicating effectively with law enforcement partners involves recognizing how the perspectives and information needs of elections and law enforcement are different. We recommend identifying a consistent liaison from law enforcement and channeling most communication through them. Ideally, they will visit the election office, meet staff and observe operations. You need to keep law enforcement apprised of the changing threat level. Telling the liaison about online chatter or anger directed at the office will create a deeper awareness of context if the situation deteriorates and a response is necessary.

During a meeting, ask law enforcement to provide some basic security guidance. This information, coming directly from law enforcement, may help to cement principles already provided in other training settings. Allow law enforcement to review the incident response tracker used to document any security events. **Creating an incident response form can help ensure you capture all necessary details.**

If an incident requires a law enforcement response, it may proceed along two lines: investigative and protective. Law enforcement will set the terms for the investigative response. Ask your partner agency about what information they will need you to document if you receive threats or observe suspicious activity.

If and when a security situation develops, the election office must take the lead, making detailed requests to law enforcement for protective services, in line with the terms of engagement established ahead of time. The goal is to avoid surprises. An overly energetic response may intimidate voters. An insufficient response may leave election personnel feeling unsafe.

As the election official, you can best gauge how a response may be perceived, and the law enforcement agency knows what it can and cannot accomplish. Be prepared to make detailed requests for personal security. If particular staff members are threatened, ask directly what can be done for them. Make specific requests, look for specific responses and inform all election personnel about what to expect.

Finally, remember that the goals of law enforcement engagement are primarily to deter potential assailants and reassure the public that no one can disrupt the election. Both goals depend on

public awareness of law enforcement's involvement. Work out a strategy in advance that addresses when it will be appropriate to issue a joint statement to the press, mention law enforcement support on social media or even stand at the same podium.

Incident Response Planning

Your coordination with law enforcement includes **establishing rules of engagement**. This step is critical and includes defining communication protocols around what information is reported and how. If law enforcement doesn't understand why certain things get reported it may be difficult to get them to react appropriately. In the cyber security context, the Government Coordinating Council (GCC) and Sector Coordinating Council (SCC) built similar communication protocols. It may be worth creating a similar framework, for example an Incident Escalation Reporting Policy, for jurisdictions to adopt so the entire community can speak with one voice.

Develop your own framework with your law enforcement partner, documenting the circumstances that would prompt you to request increased security presence and the actions they would take. Here are steps to consider:

- Centralize reporting through a liaison with authority to send assistance immediately or to change deployment patterns.
- Have ongoing engagement with the liaison to build familiarity with election personnel, election customs and security vulnerabilities.
    - Observation during candidate filing, petition verification or other pre-election moments with a larger public presence at the office.
- Consult on office security (cameras, facility design, etc.)
- Provide staff with security training.
    - Protecting email, social media and other accounts, training to prevent cyber bullying and threats and how to be safe about the information shared
    - See something/say something training on observing visitors to the office
    - Personal security advice and training (de-escalation, active shooter training, etc.)

- Introduce partners to a broad group of election personnel.
    - In a crisis, targeted personnel will feel safer if they already know the person responsible for security assistance.
    - You cannot introduce every poll worker to law enforcement, but even second degree recommendations help—for instance, a staffer coordinating poll worker assignments can instill confidence by saying, “We’ve worked with them, and we know they’ll take care of you.”
- Stronger presence at the central election facility, potentially including parking facilities at main times of arrival/departure.
- More frequent patrols past drop boxes, polling places and other remote sites.
- A plan detailing how law enforcement support will increase as threat levels rise.
    - Patrolling or deployment at private homes in the event election personnel are threatened.
- A joint communication plan to ensure the public and any potential perpetrators are aware of law enforcement support for election personnel.
    - Ensure the plan addresses how to communicate about ongoing investigations, balancing the deterrent effect of public awareness with legal and policy needs for investigative reticence.

After developing a shared assessment of the threats to election officials and a security agreement on the assistance law enforcement can provide, it may be useful to participate in a “tabletop exercise,” a simulated emergency in which election staff and law enforcement act out their roles. This can call attention to and help reconcile the differing perspectives of diverse agencies and staff that may otherwise remain implicit and create friction. It will build ‘muscle memory’ so that procedures aren’t forgotten in a real crisis.

Security Planning Resources

The Cyber Infrastructure Security Agency (CISA) published a Tabletop in a Box exercise template that you can modify with different scenarios to achieve desired learning and practice objectives.

CISA has also published an outline, or template, for building your incident response plan in the cyber context titled Cyber Incident Detection and Notification Planning Guide for Election Security. Pay particular attention to Appendix A: Key Stakeholders and Contact Information Worksheets. Many of these will overlap, and if not, they provide a logical parallel to build from.

Heightened Office and Worktime Security

Election offices will benefit from a physical security audit. Protective service units of law enforcement agencies, notably CISA, routinely conduct such reviews for officers of the court or other elected officials and may be willing to do a walk-through and make recommendations.

Discuss how activity and observation in your office changes on major dates in the election and post-election calendar and how to adjust security procedures without compromising election principles that require ample observation.

Other important elements of office security are presented in our paper Election Security in a Time of Disturbance, which focuses on the threat of disturbances or attacks at a central election facility and offers steps to improve security there. Here, **we focus on how offices can provide security for election personnel themselves, particularly as they leave central facilities to visit outlying sites or to return home**.

During a crisis, speaking with all relevant election personnel is an immediate priority. Explain the nature of the concern, whether it is a direct threat or angry controversy that could lead to an incident. If an election procedure or decision is under fire, explain the situation in detail. They are most likely to understand and project your message through their own networks.

Reassure them of their own safety. Provide some detail on the steps you are taking. Offer staff advice on what they can do themselves. Many tips for staff are outlined below in the sections on personal safety.

If the situation requires heightened law enforcement presence around election facilities, brief your staff. Different employees may have had different experiences and maintain varying sensibilities

about police. Offer staff the opportunity to speak privately with you or other senior staff (such as a human resources director) about their concerns. To the degree possible, introduce security and election personnel to one another. The law enforcement presence is intended to protect staff. Even those who are wary of law enforcement are likely to appreciate protection in this context. Approaching the situation carefully and acknowledging concerns will help avoid difficulties.

Train election personnel to be vigilant, watch for unusual behavior or people who loiter near election sites without a known role, and report suspicions. Staff at one county in 2020 noticed a lurker who was writing down license plate numbers in the election warehouse parking lot. Staff should watch for these indicators (adapted from the CISA "Personal Security Considerations" factsheet.):

- Loitering without a reasonable explanation
- Picture taking or other unusual focus on election facilities or personnel, especially if there are attempts to hide the behavior
- Attempts to avoid security staff, check-ins or video cameras
- Threats of violence - direct or implied
- Leaving a backpack or other package behind

Reporting incidents like thes can trigger law enforcement observation or even an interview with the person involved. This can be an effective deterrent.

Deploy security video surveillance at central facilities as well as at outlying sites like early voting site entrances and drop boxes. Security footage helped authorities immediately identify and arrest the man behind a ballot drop box fire in Boston in 2020. Many election sites, like town halls and school buildings, already have security cameras. Enter agreements or, at a minimum, discuss with those agencies your interest in accessing or preserving that footage.

Routinely confirm that all cameras are functioning as expected. This includes ensuring the storage device for the system has sufficient memory to retain the recordings, confirming the ablity to retrieve videos from a specific point in time, and verifying that the angle or view of the camera is adjusted to capture the appropriate areas. If using motion detection, test your settings by entering the space and verifying the camera activated.

As a best practice, ensure that the entrance to the location is captured, being mindful to not aim the cameras in ways that affect voting privacy. Where practical, consider purchasing security cameras for sites without them. Consult with a local vendor to see what options best fit your needs and budget. If suspicious activity is reported, video provides an opportunity to review the behavior, which could be benign. Video footage can also show if a suspicious person has been present at other times. **Note:** Grants may be available to fund such purchases.

Providing a secure entrance and exit will help provide peace of mind and reassure your staff. If your office is under threat, advise staff to approach parking areas or transit stops in groups. Provide an escort if needed. Ask law enforcement to provide security of the parking area by escorting staff and monitoring for suspicious individuals.

Using two-person teams to transport ballots and other secure materials is always the best practice. In incidents where election workers moving materials have been pursued, they were working in pairs. This allowed the passenger to call law enforcement and navigate to a secure destination. In certain circumstances, some states mandate that teams be bipartisan. Even when not mandated, bipartisan teams provide greater transparency and strengthen credibility if your operations are under attack.

Ask law enforcement to provide some level of patrol at all election sites, scalable when threat levels change. A periodic presence at ballot drop boxes and early voting parking lots will show potential bad actors that law enforcement supports the election authority.

Regardless of threat outcomes, remember that anyone in a targeted office may feel afraid or threatened. It is **critically important to take action on behalf of staff**—listening and acknowledging their concerns, explaining threats and providing emotional support will help maintain morale and mitigate trauma.

Consider providing specific assistance to individual staff members who face a more direct threat. One county whose parking lots were surveilled by agitators, worked with the state department of motor vehicles to provide temporary license plates to re-anonymize staff vehicles. Covering the cost of cab fare, temporary installation of home security cameras and even relocation to a hotel are accommodations to consider to ensure staff safety where specific threats exist. Purchasing a

home security camera system ahead of time and having IT staff learn how to install and use it will allow rapid deployment in an emergency. **Do not skimp on serious measures when someone's physical safety is at risk**.

Improving Personal Physical Security

This section outlines strategies to protect election personnel, their families and their homes, and to prevent violence and threats to them in their public role. There are preparatory steps to take today, steps to take as threats emerge and steps that must be taken to protect those named or singled out by online agitators.

Safeguarding Your Online Presence

One of the most effective things individuals can do is **lock down their online presence and make it more difficult to find their personal information**. The first step is determining how easily someone can find your personal information. Second is working to get the information removed. Your goal is to make it difficult for bad actors to learn where you live or to find names, photos and information about those close to you. Depending on your role and your level of concern, it may be sufficient to eliminate some sources of information and keep a list of social media accounts that you will turn private if tension levels rise. Our companion report, Defending Democracy: Protecting Election Workers from Online Threats, gives in-depth instructions on this and other aspects of personal cybersecurity.

Maintaining Personal Safety Measures

Other basic aspects of personal security are easy to overlook. Below are some helpful tools:

- If controversy arises, be vigilant about locking your doors and your vehicle, using your garage if you have one, pulling your blinds or shades at night.
- Consider asking trusted neighbors to keep an eye out for people lingering near your house.

Educate Those Around You

- Talk to friends and family about the election. Give them an overview of your rigorous election procedures. Convey your conviction that the procedures are fair and results are accurate. They can be allies in protecting you from gossip or anger in the wider community. You may also inform them of any known attempts to malign your reputation.

De-escalate Situations

Learning de-escalation techniques can be helpful in confrontations.

- Speak in a calm voice. Your tone and posture should assure observers that you believe they will be satisfied once you explain how procedures ensure the integrity of the vote.
- Conduct yourself with firm but polite professionalism to help defuse disruptive situations.
- Remember that even angry, misguided observers are usually acting in good faith. This may help you understand and successfully address their concerns.
- Listen and talk in a manner that demonstrates you take the concern seriously, such as "I want to make sure we know exactly what happened here, so everyone is satisfied we're handling it correctly."
- Be specific when explaining law, local practice and procedures so that voters and observers know the rules and their boundaries.

If you are with a colleague when a situation develops, one of you should take responsibility for communication, using tone and gesture to slow the situation down and explain that whatever is upsetting the instigator can be addressed. The second person can observe and decide whether to call a supervisor, an election attorney or law enforcement. Handing off communication to an attorney can be very valuable in de-escalating a situation or redirecting anger towards someone on the phone rather than you. Role-play these techniques ahead of time to make them automatic.

Remember to enter, share and update phone numbers for law enforcement and other key people in your cellphone on a routine basis. If you key a police station address into your contacts, you can map a route there at a touch if you believe you're being followed.

Discussing the steps we mention next can be unsettling, but remember that you are planning for contingencies, however unlikely. Planning will help ensure your safety if individuals who are angry, suspicious or acting unreasonably attempt to act on their threats.

Have an evacuation plan and identify a place where you and your family could stay if you feel unsafe at home. This could be a hotel or the home of friends or family. If the threat is real, it may be appropriate for an election office to pay for temporary accommodations. If the atmosphere is tense, pack a bag in preparation. Election workers with young children should review school or daycare pick-up arrangements and consider discussing a more supervised pick-up structure with administrators.

When out in public, avoid poorly lit areas, be alert to your surroundings, and keep texting, phone conversations and other distractions to a minimum.

If you receive threats or ugly communications, save and document them:

- Print them out.
- Keep emails in a special folder.
- Screenshot text messages.
- Write down the time and content of any phone call.
- Report the threat immediately to the office and/or law enforcement.

Election officials are public servants. If they are threatened, government security is fully justified. That could mean asking police to patrol your street and neighborhood more often or station a patrol car there, if you're comfortable with police presence. Consider whether you want a security camera at your house. In a crisis, it might be appropriate to ask the election office to install one for you temporarily.

In summary, election offices have provided cab fare, rented vehicles and even obtained temporary license plates so election personnel could not be tracked by their vehicles or identified by their plates. A variety of measures small and large should be considered to support election personnel and give them the confidence and peace of mind to do their jobs.

Deterring Violence Through Preparedness

Incidents of intimidation and aggression toward election officials are a reality, and we must prepare for the possibility that they may occur again. By taking the proper steps now to build relationships with law enforcement, to strengthen the digital and physical defenses of our offices, and to provide for the personal security of election personnel, we can ensure that attempts to intimidate the election community will fail, and election outcomes will not be undermined.

In-Crisis Checklist

Communications

- ☐ With staff and workers
    - ☐ See something / Say something
    - ☐ Upgrading personal security to meet the threat level
    - ☐ Upgrading digital/social media security
- ☐ With law enforcement
- ☐ With neighboring offices
- ☐ With potential public relations allies
- ☐ With public

Law enforcement implementation

- ☐ Discuss the incident or situation and agree on the threat level
- ☐ Request general protective service for the office, such as added patrols or posting of officers
- ☐ Request security for individuals who have been threatened.

Hardening the central facility

- ☐ Ensure cameras are working
- ☐ Brief all security staff
- ☐ Change office entry policy
- ☐ *****Balance any restrictions with the need for transparency and observation and the requirements of voter services.

Parking and outlying facilities & sites

- ☐ Hardening private homes (independently if desired, but also with official assistance after specific threats)
- ☐ Providing temporary license plates

Support for individual staff

- ☐ Pairs/teams for external assignments
- ☐ Cab fare

Support for targeted staff

- ☐ Upgrading home security
- ☐ Requesting temporary police protection
- ☐ Rental vehicle or plate change
- ☐ Temporary housing