THE
ELECTIONS
GROUP

Running Elections Without Fear

Ensuring Physical Safety
for Election Personnel

Issued by The Elections Group

Table of Contents

A note from the authors

The authors would like to preface this discussion with some reassurance. We will list threats and threatening activity from 2020 that forced the issue of personal security for election officials into the realm of public discussion. Such threats take an agonizing toll on a target's sense of safety even if the perpetrators never move into action. Still, it's worth stressing that we are not aware of physical violence targeting an official for their role in an election in the United States in 2020. One important purpose of this document is to let election officials know that in the event our country again sees such threats, comprehensive plans exist to provide them with protection.

Introduction

The 2020 election forced Americans to recognize a new challenge to our democracy. Online forums of partisans, spurred by foreign adversaries and even politicians, used the innocent actions of election workers and a few honest, correctable errors to create **a viral outbreak of threats against election officials** and workers, intended to intimidate them into changing procedures, decisions and even outcomes. These threats culminated **in incidents of actual physical confrontation.**

It's tempting to believe your office is immune because you're not in a swing state. This paper is for anyone who has had a network crash, a worker who forgets a step in a complex process, or an outcome that took the losing candidate by surprise. In a time of toxic distrust, even minor mistakes may be used to fan anger, which can lead to threats, confrontation or violence.

Our previous paper, Defending Democracy: Protecting Election Officials From Online Threats, details how digital threats develop, how they can ramify through social media to impact you and others around you, their devastating impact on your sense of security and how to protect yourself digitally.

This paper addresses the potential for real-world incidents to burst out of those online forums. We suggest what you can do now to prepare for such incidents and outline how to adjust your physical security posture if online anger is directed at your office or actual threats develop.

We discuss how to build a relationship with law enforcement today. Creating information-sharing networks, **using the response to cyber-attacks in the 2016 election as a model,** can foster understanding of threats in the election community and help law enforcement agencies begin to understand the urgency and the uniqueness of the election security situation.

2020: Escalating Incidents with Ominous Potential

The general outline of political unrest in 2020 is well known—distrust of covid-related changes to election administration provided kindling, fanned into flames online by those unhappy with the election outcome, building to the eruption of January 6th. Some see an antecedent in the Michigan militia plot to kidnap Gov. Whitmer and try her in a spurious "court". Others draw parallels with some summer protests, almost always orderly, but sputtering in a few places, like Portland, into aggressive confrontation led by small numbers who challenged the legitimacy of the elected government.

Less well recognized but more relevant to election officials were incidents through the fall and early winter where ballots and election staff themselves were targeted—not digitally, but in person. (See Table: Confrontation Targeting Elections, a Timeline). The election's legitimacy was questioned, and its mechanisms and personnel became targets for escalating physical confrontation. These incidents were important precursors to the riot to disrupt election certification in Washington D. C. on January 6, 2021. And January 6th warns us that many angry voters respect no legal restraint and may use violence to try to change an election's outcome.

Confrontation Targeting Elections: A Timeline	
October 19, 2020	**Van forced off the road in Harris Co., TX over misconceived fraud theory** Van bumped; tradesman with no election connection detained by private investigator pursuing bizarre and imaginary mail ballot plot.
October 20	**Arson at Los Angeles, CA mail ballot drop box** Several hundred ballots damaged; perpetrator unknown.
October 22	**Armed men near a St. Petersburg, FL, early voting site** Armed, uniformed security guards gathered in a pop-up canopy across the street from the site. Sponsor and purpose unclear.
November 5	**Armed protestors massed at Arizona mail ballot counting site** They demanded counting continue; their presence prompted shutdown instead.
November (Uncertain Date)	**Intruders in the yard of a Georgia election official** **Noose left at door of Georgia election vendor employee**
December 1	**Gwinnett Co., GA elections staff pursued by a vehicle** IT staff ultimately called 911 and waited at a county facility parking lot.
December 6	**Armed protesters outside Michigan Secretary of State's home**
January 2, 2021	**Fulton Co., GA staff confronted while retrieving ballot drop box contents**

Confrontations were overwhelmingly launched by the political right in 2020. Yet, we caution that perpetrators who act to delegitimize elections could change with different outcomes.

All election offices should plan for security. In October 2020 we published, Election Security in a Time of Disturbance: Standing Up to Intimidation, Preventing Overt Attack, to help election officials prepare for activities that were on the horizon. At the time, we envisioned the potential for overt disruption at central election facilities and suggested ways to minimize it. Much unrest in 2020 did focus on central facilities, and administrators and law enforcement recognized and responded to that threat, hardening defenses there.

As it happened, some of the most alarming behavior happened at remote locations - at drop boxes, on roads where workers and volunteers were pursued, and even at private homes**. This paper provides added policy and coordination advice about the physical security of election personnel.**

Erratic Linkage Between Cyber-Mobs and Real-World Incidents

In 2020, many threats to election officials originated online, when cyber-mobs targeted jurisdictions whose results they distrusted. They sifted through videos and other information for routine practices they might deem suspicious. Online partisans doxed election officials and workers (that is, published their addresses and other personal information), leading to threats both online and in person.

In our companion paper, Protecting Election Officials from Digital Threats, we go into more detail on the origins of such attacks, and suggest how election officials and workers can protect themselves by limiting the amount of their personal information that is online.

What is clear from the timeline of physical confrontations is their inconsistent relationship with online activity. Doxing led to trespassing at the Georgia Secretary of State's home, and a noose left on a contractor's doorstep. But **many incidents did not follow threats or doxing.** Instead, they occurred when people steeped in the paranoia of online discussion decided to visit election sites, convinced that the election and all involved with it were illegitimate.

Elections workers in a Dec. 1st stalking incident had not been named or targeted. Instead, it unfolded after an angry partisan who believed in a conspiracy involving "Chinese servers" showed up to surveille an election facility. When he saw workers loading (phone) equipment into a vehicle, he decided those were the fateful servers. He followed them, live-streamed his pursuit, and tried to confront the IT staffers. They called 911 and pulled over in a camera-covered parking area to wait for police.

Likewise, a ballot drop box where partisans confronted election workers on Jan. 2 was not a particular subject of internet chatter. It was just another drop box that conspiracy-mongers had identified. Partisans, primed to see cheating where none existed, showed up and pursued the staff charged with collecting ballots from the drop box and taking them to the central count facility, where law enforcement intervened.

If there is a pattern, it's a focus on activities that are somewhat less well understood or transparent. We do believe that leaning more heavily on bipartisan teams of poll workers, even in roles that can legally be completed by election staff, can insulate election offices from some criticism. Still, those who begin with an unjustified assumption of malfeasance are likely to simply find something else to question.

The unpredictability, **the somewhat random targeting once a jurisdiction is subject to suspicion, means that a security plan must be broad in scope.** It should afford protection to a wide range of officials and workers who could become targets. And it must be 'shovel-ready,' to quickly implement if and when the cyber-mob's gaze turns to your jurisdiction. Attacks on election personnel are no longer unthinkable, so security partners must upgrade their ability to respond today. Once the threat finds a target, however unlikely or undeserved, it may be too late.

If the capricious finger of an online mob turns towards your office, there are three aspects of physical security that must be addressed:

- 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 election sector should construct the same type of response to threats of violence that was mounted after Russian interference efforts in the 2016 election. In the last four years, the Cybersecurity & Infrastructure Security Agency (CISA), the Justice Department through the FBI, state and national election associations, and the work of individual offices and election officials, created new strategies of cyber-protection and resilience that broadly and successfully changed the habits and practices of our industry.

Between now and the next federal election, every election office should participate in a meeting or briefing on physical safety issues with local law enforcement, an effort that could be aided by their local CISA protective security advisor (PSA).

The Initial Approach: Seeking Broad Participation

The first step in engaging law enforcement is meeting with relevant agencies. Consider inviting a range of police agencies, including the local CISA support, FBI, US Marshals, state and local police. 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 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 should be prepared to support a statewide or regional effort. Additionally, the Election Assistance Commission (EAC) could assist by convening nationwide conference calls similar to those convened by CISA with the CDC, USPS and others during last year's pandemic.

Well-defined objectives will lead to a more productive meeting. Desired outcomes might include a better understanding of how agencies will share information when threats to physical safety are reported, what service level to expect from different agencies, what details or evidence will make it more likely to get enhanced support or protection.

Building Consensus About Election-Related Violence

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 more attention than other threats in the daily police blotter. You may need to **build that case with law enforcement.**

The **intimidation of election officials should be viewed as a special category of crime, more like a terroristic threat against the judiciary** than the many other types of threatening behavior reported to police. Election officials, like judges, manage a foundational institution, and should be able to 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 whole 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 dangerous to our society than normal threats. They require a strong law enforcement response.** In recognition of this special status, some state legislatures are considering stiffer penalties for harassment or intimidation when the victim is an election official.

This guide can help develop talking points to succinctly convince law enforcement their involvement is necessary. Use it to build a shared understanding of the problem's scope and the strategies required to respond.

For example, law enforcement agencies may be unaware of the seriousness of threats directed at election offices. **The incidents listed in the previous section provide tangible evidence 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 these incidents should help shape law enforcement perspectives on the risks you face and what protective efforts are called for.

You also need to establish how election work is different from other fields needing personal or private security. A private office may be able to close its doors to the public, but election work requires transparency. In fact, 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 should be 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 itself feel overbearing to some voters. Law enforcement election activity must balance competing demands in very different settings such as voting sites, offices and central count facilities.

Communication 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 should 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.

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. **Creating an incident response form can help ensure you capture all necessary details**.

If and when a security situation develops, the election office should take the lead, making detailed requests to law enforcement for protective services, pursuant to terms of engagement established ahead of time. The goal is to avoid surprises—either an overly energetic response that may intimidate voters, or an insufficient response that leaves election personnel feeling unsafe.

The election authority 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 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 should include **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 in concert.

You should **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. Some steps that should be considered:

- Centralizing reporting through a liaison with authority to send assistance immediately or to change deployment patterns.
- 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.
- Consultation on office security (cameras, facility design, etc.)
- Providing staff security training
    - See something/say something training on observing visitors to the office
    - Personal security advice and training (de-escalation, active shooter training, etc.)

- Introductions to a broad list 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-level recommendations help—for instance, a staffer coordinating poll worker assignments 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.
    - This plan should address 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 vision 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 help to surface and 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 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 go home.**

During a crisis, speaking with all relevant election personnel should be an immediate priority. Explain the nature of the concern, whether direct threats 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.

You should reassure them of their own safety. Provide some detail on the steps you are taking. Offer staff advice on what they can do themselves (i.e., many of the things 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 an HR 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 recognizing their concerns will avoid difficulties.

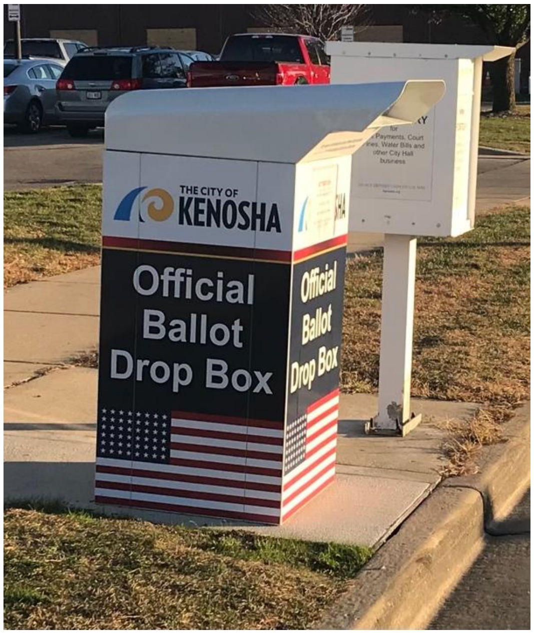
Election personnel should be trained to be vigilant, watching for unusual behavior or people who loiter near election sites without a known role, and to report suspicions. Staff at one county in 2020 noticed a lurker who was writing down license plate numbers in the election warehouse parking lot. Staff 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 this can trigger law enforcement observation or even an interview with the person involved. This can be an effective deterrent.

We suggest security camera coverage 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.

Confirm that all cameras are working, have sufficient memory to retain recordings, that video can be retrieved, and that they are focused on the appropriate area. Cover the entrance! But camera placements should **never** show how anyone is voting. Where practical, consider purchasing security cameras for sites without any. If suspicious activity is reported, video gives the opportunity to review the behavior, which could be benign. It also can show whether a suspicious person has been present at other times.



Arrival and departure of staff was shown to be a vulnerability by the December 1 incident in Georgia, where IT staff departing an election warehouse were pursued. In a crisis, secure entry and exit will reassure staff. If your office is under threat, advise staff to approach parking areas or transit stops in groups. Provide an escort if needed. Request security oversight such as a deputy to monitor the parking lot for anyone who seems suspicious.

When staff move election materials, working in pairs is safer. In each incident where election workers were pursued, they were working in teams. In a team, the passenger is better able to call law enforcement and to navigate to a secure destination. There is ‘safety in numbers,’ and the flip side—fear is sharper if someone is threatened and alone. Of course, using 2-person teams to transport ballots and other secure materials is always the best practice. In certain circumstances, some states even 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 troublemakers that law enforcement supports the election authority. This can deter them. If threats intensify, patrols should be more frequent.

Because cyber-mob activity is capricious, and those inspired to act in the real world are volatile and unpredictable, everyone in a targeted office may feel threatened. In the next section, we will detail how to improve personal physical security. **But first we want to emphasize the absolute importance of taking action on behalf of staff**—explaining threats, listening and acknowledging their concerns, and providing emotional support will help maintain morale and mitigate a traumatic experience.

Offices should also **consider providing specific assistance to individual staff who face a more direct threat.** One county whose parking lots were surveilled by agitators worked with the state DMV 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 should be considered 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 discusses strategies to protect election personnel, and to prevent violence and threats to them in their public role from compromising their home and family. There are 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.

The origin of attacks targeting individuals in 2020 was almost always “doxing,” meaning online trolls tracked down their contact information and addresses to threaten them. In some cases agitators even showed up at private homes. This happened to high-ranking officials, office staff, and even vendor staff singled out by online trolls.

One of the most effective things that individuals can do today is to **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 cyber-mobs 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 cyber-security.

Other basic aspects of personal security are easy to overlook. 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.

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.

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 habitual. **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.

Even discussing the steps we mention next can be scary, but remember that you are planning for contingencies, however unlikely. Planning will help ensure your safety if angry and misguided people try to act on their suspicions. **Have an evacuation plan and identify a place where you and your family could stay if you feel unsafe at home**. This might be the home of friends or family, or a hotel. 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. Review pick-up arrangements at your children's school or daycare and consider discussing a more supervised pick-up structure with their administration.

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

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

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

Because election officials are public servants, if they are threatened, government security is fully justified. That can mean asking police to patrol your street and neighborhood more often, or even to station a patrol car there temporarily if you're comfortable with police presence. Consider today 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.

Offices in 2020 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

We may hope that the incidents of intimidation and aggression towards election officials before and after the 2020 Presidential Election were an aberration, but we must prepare for the possibility they were not. By taking steps now, building relationships with law enforcement, strengthening the digital and physical defenses of offices, and providing 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 by mobs or violent individuals.

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 PR 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 normal 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