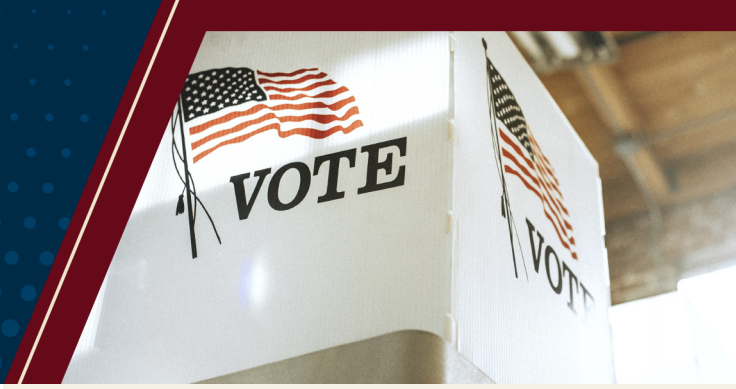
PHYSICAL SECURITY CHECKLIST FOR ELECTION OFFICES



INTRODUCTION

Ensuring a secure and resilient election process is a vital national interest and one of the highest priorities for the Cybersecurity and Infrastructure Security Agency (CISA). CISA is committed to working collaboratively with election officials and election technology and service providers to manage risks to the nation's election infrastructure. As part of the comprehensive suite of resources available to election officials, this checklist is a tool to quickly review existing practices and take steps to enhance physical security and operational resilience in preparation for election day.

HOW TO USE THIS RESOURCE

This checklist provides a series of questions designed to help election officials identify areas to enhance physical security at election infrastructure facilities and take action to implement low- or no-cost options in the short term.

SECURITY CHECKLIST

Plan and Prepare

YES / NO **Have you established a Facility Security Plan for your office that addresses key tasks for maintaining office security?**

- Implement policies for securing exterior doors and windows, securing sensitive areas within the facility, utilization of a facility alarm system (if installed), and observation of parking areas for unattended vehicles or suspicious activity.
- Institute procedures to monitor the parking area and policies to act on unauthorized vehicles.
- Implement a "If You See Something, Say Something ®" public awareness campaign. This can be as simple as posting signs with contact information for the public to report incidents to.
- Institute access control policies/procedures for personnel, volunteers, and the public to permit only authorized access to sensitive locations. Establish a strong key control accountability system and restrict key duplication.
- Practice your incident response and continuity of operations plans to familiarize personnel with their responsibilities. This can also help identify gaps in the plans so they can be addressed before an incident occurs.

YES / NO **Have you developed other plans to support secure and resilient election operations?**

- Establish an **Incident Response Plan** that identifies security responsibilities, emergency contacts, and response procedures. Your Incident Response Plan should also include an **Incident Response Communications Playbook** that helps navigate how to communicate clearly and transparently with voters and the public if an incident occurs, and what steps have been taken to ensure a safe and secure elections process.

- Establish a **Continuity of Operations Plan** to ensure that essential election functions can continue if disruptions to operations occur. This could include planning for backup power solutions for polling locations or election offices or identifying alternative sites to continue operations if a facility is inaccessible or unusable.

YES / NO **Have you established procedures for handling suspicious mail/packages, to include potential bomb threats?**

- Prepare an area for safe mail handling with direct access to the outside of the building or in a location with doors that can be closed.
- Have personal protective equipment available for staff handling mail and easy access to water.
- For additional information check-out the joint CISA, Federal Bureau of Investigation, U.S. Election Assistance Commission, and U.S. Postal Inspection Service Election Mail Handling Procedures to Protect Against Hazardous Materials and CISA's Bomb Threat Guide and the Bomb Threat Checklist.

YES / NO **Have you coordinated with emergency responders in your jurisdiction?**

- Talk through your Facility Security and Incident Response Plans with emergency responders ahead of time so they can understand your organization's posture before they arrive on scene during an incident.
- Provide emergency responders with a list and/or map of election infrastructure locations, to include temporary voting locations. Review facility floorplans and evacuation routes.
- Work with emergency responders to see if they have emergency radios for use during election operations and times of increased threat.

YES / NO **Have you worked with emergency responders to mitigate potential risks from hoax incidents like swatting or fake bomb threats targeting election facilities during voting period?**

- Ensure your local public safety 9-1-1 computer dispatch system has election locations, including temporary locations, identified so the system alerts emergency responders that the incident location may be a target for hoax calls to disrupt election operations.

YES / NO **Do you have mechanisms in place to facilitate receiving and sharing threat information?**

- Join threat information sharing platforms like the Election Infrastructure-Information Sharing and Analysis Center.
- Engage and share information with the Fusion Centers that cover your jurisdiction.
- Work with your neighbors (owners/operators of neighboring offices or buildings) to share knowledge of threats and security concerns and encourage them to report security incidents to appropriate authorities. If possible, consider sharing security camera feeds/footage with each other.

Implement

YES / NO **Do you conduct spot-checks both during and after business hours to make sure security procedures are being implemented as intended?**

YES / NO **Are points of entry and sensitive locations or assets monitored by security cameras and/or intrusion detection systems?**

- Consider implementing video security monitoring and alert systems that cover, at a minimum, points of entry and storage locations for sensitive assets such as ballots and election equipment.
- If professional-grade commercial security solutions exceed available resources, consider lower cost, commercially available options such as home security solutions that include video cameras with motion detection capability, email/text alert functions, and intrusion detection sensors for doors and windows.

YES / NO **Are fixed and/or portable "panic buttons" in use?**

- Many professional grade security systems include options for fixed and portable duress alarms or "panic buttons" that integrate into a facility's broader security system.
- If professional-grade commercial security solutions exceed available resources, there are low-cost commercially available portable "panic buttons" that can be programmed to contact local law enforcement and come in form factors like key fobs.

YES / NO

Are procedures in place to control visitor entry?

- Ensure the Facility Security Plan enacts procedures for full accountability of visitors (ex., implementing sign-in/sign-out procedures).
- Prevent visitors from entering through unauthorized entry points (ex., make sure all other doors are locked other than the public entrance).
- Implement mechanisms to inform other employees of the presence of visitors inside the facility. For offices where continued monitoring of visitor entry locations is challenging, consider hanging a bell on the door or installing some form of motion or business doorbell sensor that alerts when a door opens.

YES / NO

Do ground floor windows and large glass entry doors have privacy measures installed?

- Install contact or privacy film on ground floor glass doors and windows if they do not have other features to obscure outside visibility. Contact or privacy film can be purchased from your local hardware store and some types can provide some shatter resistance.
- If altering building windows is not possible, then apply window treatments or curtains that can be easily adjusted to obscure visual observation into the office.
- If allowable, consider prohibiting parking next to the election office building during election operations and times of increased threat.

YES / NO

Are physical barriers present in front of entrances to mitigate high-speed avenues of approach or unimpeded straight-line paths for vehicles?

- Install security bollards (typically made from metal or cement) in front of facility locations to help protect pedestrians and prevent accidental or deliberate vehicular damage.
- If permanent solutions like bollards exceed resourcing, contact your transportation department for possible temporary barriers that may be available. Another alternative could be filling extra-large exterior planters to use as a barrier.

YES / NO

Are fire extinguishers pre-positioned in sensitive locations?

- Install a fire extinguisher in each room where ballots, election equipment, and election supplies are stored.
- Ensure there is a fire extinguisher in each polling place.

YES / NO

Are ballot drop boxes located in well lit, continuously monitored areas?

- Place drop boxes in locations that provide good lighting, allow for continuous video surveillance, and are observable by facility staff.

Report

Know how to report cyber or physical security incidents to relevant state and local authorities, CISA, and other federal partners.

- Take advantage of CISA's Last Mile initiative to document reporting guidance
- Print out CISA's 2024 General Election Cycle: Voluntary Incident Reporting Guidance for Election Infrastructure Stakeholders

RESOURCES

#Protect2024 | CISA
cisa.gov/topics/election-security/protect2024

Critical resources for state and local election officials serving on the front lines.

2024 General Election Cycle: Voluntary Incident Reporting Guidance for Election Infrastructure Stakeholders | CISA
cisa.gov/resources-tools/resources/2024-general-election-cycle-voluntary-incident-reporting-guidance-election-infrastructure

Election infrastructure stakeholders are encouraged to share information related to cyber and physical security incidents with each other, state fusion centers, local law enforcement and federal partners.

Physical Security of Voting Locations and Election Facilities | CISA
cisa.gov/resources-tools/resources/physical-security-voting-locations-and-election-facilities

This general guide provides resources and actionable steps to connect, plan, train, and report that election officials should consider to improve their physical security posture and enhance resilience of election operations in their jurisdiction.

What to Do: Bomb Threats | CISA
cisa.gov/resources-tools/resources/what-do-bomb-threats

This guidance document provides an overview of bomb threats and some recommended practices to mitigate the impacts associated with these threats.

Suspicious Mail | USPIS
uspis.gov/tips-prevention/suspicious-mail

Follow and share these tips to protect yourself and others against suspicious mail.

Election Mail Handling Procedures to Protect Against Hazardous Materials | CISA
cisa.gov/resources-tools/resources/election-mail-handling-procedures-protect-against-hazardous-materials

This guide provides an overview for election officials on preparing to handle mail safely, identifying potentially suspicious mail, and responding to potential hazardous materials exposure from handling mail.

Last Mile Products | CISA
cisa.gov/resources-tools/services/last-mile-products

The CISA Last Mile initiative provides election administrators and their partners a range of customizable resources based on security best practices and industry standards to help secure election infrastructure nationwide.