States United DEMOCRACY CENTER

Keeping Statewide Elected Officials Safe: Office and Staff Security Considerations

The security of statewide elected leaders is essential to maintaining peace, order, and trust in American democracy. This document addresses suggestions for safeguarding such officials' office and making their staff a security resource. Other documents in the series include: Reviewing Security Resources and Deploying the Security Team, Protecting Loved Ones and Hardening Home Security, Preparing for Events, Protecting Personal Identifiable Information, and Securing Online Activity.

Designate points of contact between office staff and the relevant security professionals.

They should communicate with each other regularly and implement systems to share concerns from members of their respective teams. These same individuals should also receive law enforcement briefings concerning threats and other security risks.

Determine a notification system for threats.

The official and their chief deputy should be made aware immediately of any potential threats to the official, their staff, or loved ones, regardless of the perceived seriousness of the threat. Agree on what specific communications platform will be used for these notifications (e.g., text, calls, Slack, etc.).

Screen visitors in advance of their arrival to the office.

At the least, basic internet searches based on an individual's name, phone number, address, and email should be completed before new individuals meet with the elected official. Questions to elicit this information can be incorporated into an online form or a phone script.

Obtain background checks of new hires.

Law enforcement counterparts may be able to help.

Review and drill emergency procedures with the security team (e.g., active shooter drills, fire drills, bomb threats, etc.).

These procedures should be up to date for the current office location, layout, and staff. Make sure emergency roles are not assigned to former staff. Update all new employees as they onboard about these procedures.

Set clear security policy and expectations, and train and run drills with office staff.

Law enforcement or security professionals can train staff in how to enhance security, including what to look out for at events, how to screen individuals seeking appointments with the office, steps to properly document and alert others to threats, and what phishing emails look like. Similarly, policy and training in how to avoid security pitfalls, especially with social media, are key. Consider running drills to reinforce training.

Assess and strengthen as needed the office's physical security.

Security professionals should assess the office for security vulnerabilities and offer suggestions. Physical barriers should separate the lobby from the staff, and ideally additional barriers should block access to the elected official's office. Security cameras should be installed and should store video and be monitored regularly. Periodically audit the list of individuals who have access to the office, parking, and other sensitive areas. Consider installing a panic button or silent alarm.

Determine whether and when to have security professionals provide physical monitoring of the office.

Under some conditions, such as an active threat to the official, periodic physical monitoring of the office may be warranted by security professionals or by law enforcement.

Updated March 2023
