

Keeping Statewide Elected Officials Safe: Reviewing Security Resources and Deploying the Security Team

The security of statewide elected leaders is essential to maintaining peace, order, and trust in American democracy. This document addresses suggestions for reviewing such officials' security resources and assessing their security team. Other documents in the series include: Protecting Loved Ones and the Home, Office and Staff Security Considerations, Preparing for Events, Protecting Your Personal Identifying Information, and Securing Online Activity.

Maintain routine and regular communication with the head of the agency in charge of protection.

The elected official and key staff should have periodic meetings and identify specific communication practices with the relevant agency head to communicate about evolving security needs, resources, and plans. The official and staff can learn what types of additional, emergency, or as-needed resources can be provided, the process for making and approving such requests. The agency head should also help ensure that the official receives regular threat assessments, and should advise on security resources for travel or events.

Ensure that local law enforcement has relevant contact information.

The staff and agency head should ensure that 911 stores the official's office, home, and cell phone numbers and addresses such that a call for service from these numbers and addresses instantly alerts emergency services that an elected official needs help. Staff may also need to use this service.

Review security practices regularly and consider a periodic outside audit.

Changes in staff or office location, technology developments, the threat landscape, the proximity of an election, and other factors may all affect security needs, including the number of security professionals working to protect the official and the practices they use. Updating security practices regularly is key to address change and identify blind spots. A periodic third-party review can help.

Make security personnel decisions that maximize the official's comfort with and trust in the security professionals.

The level of control over security personnel varies widely by office. The official may wish to designate personnel for different functions or locations, such as for home or travel. It is commonplace to change a security team's practices and roster to address an official's comfort. If vetting and picking the whole team is an option, make sure priorities (e.g., dealbreaker prior disciplinary issues) are known in the screening process and consider having the official participate in the selection process.

Set clear confidentiality expectations and know what technology the security professionals use.

Given the access that security professionals have, clear expectations of confidentiality are key. The general counsel for the office can help ensure that confidentiality expectations address any recording or transmitting devices that the security team uses. For any law enforcement agency that provides help, it is important to understand what technology they use and have a shared understanding of confidentiality needs and limitations.

Communicate with the security team.

Officials or their staff should regularly and freely communicate security needs and preferences. Good security teams try to accommodate hobbies, family life, and the official's style of constituent engagement. Implement processes for officials, their loved ones, and staff to report security issues, like threats, to the security team.

Updated March 2023

The States United Democracy Center is a nonpartisan organization advancing free, fair, and secure elections. We focus on connecting state officials, law enforcement leaders, and pro-democracy partners across America with the tools and expertise they need to safeguard our democracy. For more information, visit www.statesuniteddemocracy.org or follow us at @statesunited.