

# A Guide to Election Security Resources

## ELECTION PROTECTION HUB

This guide provides a brief introduction to key resources and strategies for election officials concerned about physical and cyber security. The Public Rights Project team is happy to help you navigate these resources. For more information, reach out to [sophie@publicrightsproject.org](mailto:sophie@publicrightsproject.org) and [join our Election Protection Hub](#).

### 1 Building an inter-agency task force to anticipate and respond to threats before, during, and after an election

Establishing an inter-agency election security task force can help to ensure a cohesive and effective response to threats to the electoral process. Task force members can share information, coordinate responses to potential threats, and develop comprehensive plans to maintain the integrity and security of elections.

#### Potential task force members

- Election administration
- Local police and sheriff's departments
- County, city, and district attorneys
- Other participants might include state troopers or constables, the FBI, or other state, county, or local officials involved in election administration

#### During early voting and on Election Day

- Report, record, and resolve incidents according to task force protocols

#### Post-election phase

- Ensure that task force members are prepared to coordinate responses for recounts, litigation, and other post-election activities as needed
- Produce a post-election report documenting incidents, responses, and lessons learned

#### Pre-election phase

- Form a task force well in advance of an election to allow sufficient time for planning, bolster public confidence in election security, and deter threats
- Develop clear communication protocols covering inter-agency communication, media interactions, and escalation procedures to authorities like the state or FBI
- Create comprehensive guidance and training materials for poll workers and staff to handle threats or irregularities
- Collaborate with law enforcement to review and enhance the security of polling places and other election infrastructure, including physical security assessments and contingency planning
- Share essential information, such as polling place locations, with law enforcement in advance
- Set up a system for real-time communication during the election

## 2 Reporting a threat

The [Cybersecurity & Infrastructure Security Agency \(CISA\)](#) lays out the steps to take in response to a threat to election officials or infrastructure.

- If there is imminent threat to life, call 911
- To report a threat, contact the Election Crimes Coordinator at your local FBI office ([fbi.gov/contact-us/field-offices](https://www.fbi.gov/contact-us/field-offices)); submit a tip online at [tips.fbi.gov](https://tips.fbi.gov); or call 1-800-CALL-FBI (225-5324), Prompt 1, then Prompt 3. Contacting the Election Crimes Coordinator at your local FBI office is the best way to report election threats
  - Should you have any trouble identifying or contacting your ECC, you also may call the Public Integrity Section (PIN) of the U.S. Department of Justice via its main line at 202-514-1412. Please ask for John D. Keller, PIN's Principal Deputy Chief, or Sean F. Mulryne, Deputy Director of PIN's Election Crimes Branch
  - To report anomalous cyber activity and/or cyber incidents 24/7, email [report@cisa.gov](mailto:report@cisa.gov), or call (888) 282-0870
- [Contact your CISA regional office](#) for physical security risk guidance tailored to your jurisdiction and facilities. Find your local PSA here: [cisa.gov/cisa-regions](https://www.cisa.gov/cisa-regions)
- Contact your County IT services, if applicable, to support your immediate facility and local infrastructure protection.

## 3 Locating additional resources for funding and implementing election security measures

Below you'll find additional resources for election officials security, cybersecurity support, and information on funding.

### Security resources for election officials

- [Security Resources for the Election Infrastructure Subsector](#) (CISA)
- [Personal security checklist for election officials](#) (Election Assistance Commission)
- [Security Resources for Election Officials](#) (Election Assistance Commission)
- [Election Security in a Time of Disturbance](#) (The Elections Group)
- [Sample Memorandum of Understanding between election office and partnering agencies for security services](#) (Committee for Safe and Secure Elections)
- [Combating swatting attempts](#) (Committee for Safe and Secure Elections)

### Cybersecurity support

- Free cybersecurity support is available for election officials through the [Elections Infrastructure Information Sharing and Analysis Center \(EI-ISAC\)](#) and for other state, local, tribal, and territorial government officials through the [Multi-State Information Sharing and Analysis Center \(MS-ISAC\)](#). Members have access to a Security Operations Center open 24/7, 365 days a year, staffed by experts experienced in threat analysis, digital forensics, and incident response, as well as other no-cost tools and trainings.
- [Removing personal identifying information from a Google search](#)

### Funding

- [How States are Spending Election Security Grant Funds](#) (National Association of Secretaries of State)