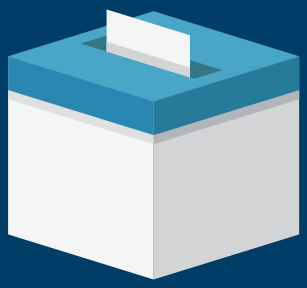
Security Resources
for the Election Infrastructure Subsector



The **Cybersecurity and Infrastructure Security Agency** (CISA) and the **Federal Bureau of Investigation** (FBI) have developed a summary of some of the resources available across the federal government for state, local, territorial, and tribal (SLTT) election officials and their private sector partners to assist in responding to threats to personnel and guidance on assessing and mitigating risks to their physical assets.

While many of these resources are not explicitly election security focused, the Election Infrastructure Subsector may find them useful in the course of their work. Since the lines between physical security and cybersecurity are increasingly blurred, select cybersecurity-focused resources have also been included in this document. All of the resources cited here are available at no-cost to the user and can be found on the websites listed below.

Threats to Election Officials and Infrastructure

In response to increased threats of violence against election workers following the 2020 U.S. election cycle, the FBI and CISA prioritized efforts to address these threats. The FBI and CISA take all threats of violence seriously, including those targeting election workers for their critical role in safeguarding the electoral process for all voters. The Department of Justice (DOJ) established the Threat to Election Workers Task Force to vigorously investigate and prosecute these threats. If you are the victim of a threat as an election worker, please take the following steps:

- If there is imminent threat to life, call 911
- To report threats, contact the **Election Crimes Coordinator** at your local FBI office (www.fbi.gov/contact-us/field-offices); submit a tip online at 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
- Finally, contact your CISA regional office for physical security risk guidance tailored to your jurisdiction and facilities. CISA Protective Security Advisors (PSA) can perform assessments, such as the Security Assessment and First Entry (SAFE) tool, that highlight vulnerabilities with your physical election infrastructure, including election offices, ballot processing locations, storage areas, voting centers, and other election facilities. Find your local PSA here: www.cisa.gov/cisa-regions

Protecting Physical Security: Guidance Documents and Other Resources

- **CISA Physical Security Preparedness at Voting Locations and Election Facilities** provides actionable steps for election officials to improve the physical security posture and enhance resilience of election operations in their jurisdiction: www.cisa.gov/sites/default/files/publications/physical-security-of-voting-location-election-facilities_v2_508.pdf
- **CISA Last Mile products** are customizable tools that election officials can use to improve their infrastructure security. Examples of these products include Election Security Planning Snapshot, Election Emergency Response Guides, Election Safeguards, and other templates. For more information and to request a customized Last Mile product, please contact: electionsecurity@hq.dhs.gov
- **CISA Soft Targets and Crowded Places Security Plan Overview and Resource Guide** provides public and private sector partners with relevant information to enhance their preparedness and security: www.cisa.gov/sites/default/files/publications/DHS-Soft-Target-Crowded-Place-Security-Plan-Overview-052018-508_0.pdf www.cisa.gov/sites/default/files/publications/19_0424_cisa_soft-targets-and-crowded-places-resource-guide.pdf
- **CISA Protecting Infrastructure During Public Demonstrations** offers security recommendations for businesses that may be the target of unlawful acts during public demonstrations: www.cisa.gov/sites/default/files/publications/protecting_infrastructure_during_public_demonstrations_508.pdf
- **CISA Mitigating the Impacts of Doxing on Critical Infrastructure** defines and provides examples of doxing, explains the potential impact of doxing to critical infrastructure, and offers protective and preventative measures, mitigation options, and additional resources for individuals and organizations: www.cisa.gov/sites/default/files/publications/cisa_insights_mitigating_the_impacts_of_doxing_508.pdf
- **Office of the Director of National Intelligence (ODNI) Counterterrorism Guide for Public Safety Personnel** assists first responders in recognizing and reporting suspicious activity, spotting indicators of mobilization to violence, and responding to and mitigating terrorist attacks: www.dni.gov/nctc/jcat/index.html

Key Website/Contact Information

- **CISA Election Security** webpage contains all of CISA's election security tools and resources, including all of the federal government's resources listed in this document: www.cisa.gov/election-security
- **CISA Hometown Security** program website provides tools and resources to support community security and resilience: www.cisa.gov/hometown-security
- **CISA Interagency Security Committee** addresses continuing government-wide security for federal facilities and has created numerous standards, policies, and best practices documents that are available for individuals and organizations to review at: www.cisa.gov/isc
- **CISA Office for Bombing Prevention** provides a variety of resources, trainings, tools and products to help state and local authorities, private partners and others understand and mitigate the threat of improvised explosive devices and protect critical infrastructure: www.cisa.gov/obp
- **CISA Central** is CISA's hub for critical infrastructure partners and stakeholders to request assistance and services. CISA Central operates 24/7: Central@cisa.gov or 888-282-0870
- **FBI Tip Line** is FBI's hub for reporting election and non-election threats and crimes: https://tips.fbi.gov or 1-800-CALL-FBI (225-5324)
- **FBI Election Crimes and Security** webpage provides information on understanding and reporting election crimes: www.fbi.gov/elections
- **FBI Protected Voices** initiative provides tools and resources to political campaigns, companies, and individuals to protect against online foreign influence operations and cybersecurity threats: www.fbi.gov/protectedvoices
- **ODNI National Counterterrorism Center (NCTC) First Responder Toolbox** provides information to aid in preparedness, coordination, response, safety, security, and investigations among counterterrorism stakeholders: www.dni.gov/index.php/nctc-how-we-work/joint-ct-assessment-team/first-responder-toolbox
- **US Election Assistance Commission (EAC)** serves as a national clearinghouse of information on election administration, and has additional election security related resources, which can be found here: www.eac.gov/election-officials/election-security

Trainings and Exercises

- **CISA Election Security Trainings** provide additional guidance to election stakeholders in managing risk and strengthening election infrastructure resilience. To schedule or to learn more about these trainings, email: electionsecurity@hq.dhs.gov
- **CISA's Interagency Security Committee** (ISC), which focuses on security for all federal facilities, provides online and interactive training courses that may be useful to securing your physical infrastructure: www.cisa.gov/interagency-security-committee-training
- **CISA's Office For Bombing Prevention (OBP)** provides in-person, virtual and web-based independent study trainings. These courses assist public and private stakeholders with awareness and response to improvised explosive device (IED) threats: tripwire.dhs.gov/training-education/counter-ied-training-0
- **CISA Exercises**, including tabletop exercises, provide scenario-based training to help identify areas for improvement, share best practices, and enhance preparedness against threats to election infrastructure and personnel: www.cisa.gov/critical-infrastructure-exercises

Alerts and Public Service Announcements

- The **Elections Infrastructure Information Sharing and Analysis Center** (EI-ISAC) offers a suite of election security resources, including threat intelligence products, threat and vulnerability monitoring, incidence response and remediation, and other products and services: www.cisecurity.org/ei-isac/
- **FBI Internet Crime Complaint Center** (IC3) accepts online complaints from victims of internet crime and publishes both industry and consumer alerts on internet crime-related issues: www.ic3.gov
- **CISA National Cyber Awareness System** (NCAS) is a repository of CISA alerts pertaining to current security issues, vulnerabilities, and exploits: www.cisa.gov/uscert/ncas/alerts