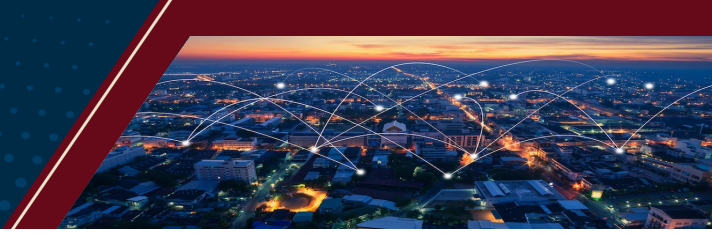
2024 GENERAL ELECTION CYCLE: VOLUNTARY INCIDENT REPORTING GUIDANCE FOR ELECTION INFRASTRUCTURE STAKEHOLDERS



OVERVIEW

Election infrastructure stakeholders are encouraged to share information related to cyber and physical security incidents in accordance with their incident response plans. Information sharing partners will likely include state and local election offices, state fusion centers, state and local law enforcement, and federal partners. Voluntarily sharing incident information facilitates faster access to incident response resources, greater understanding of threat actor tactics, and alerts to other election stakeholders about current threats and actions to help them protect their infrastructure.

VOLUNTARY FEDERAL GOVERNMENT PARTNER INCIDENT REPORTING: WHO TO CONTACT

CYBER INCIDENTS

To maximize situational awareness and support for the 2024 election cycle, report actual or suspected cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC).

1. **Report suspected cyber incidents to CISA. Email report@cisa.dhs.gov, call 1-844-Say-CISA (1-844-729-2472) or submit online at https://www.cisa.gov/report.** CISA can help with incident response and recovery for suspected cyber incidents. CISA shares relevant cyber threat and incident information to the EI-ISAC for dissemination to the broader election community.

2. **Report suspected cyber incidents to the FBI. Contact your local FBI Field Office: https://www.fbi.gov/contact-us/field-offices. You can also contact the FBI Internet Crime Complaint Center at www.ic3.gov, FBI's National Tip Line at 1-800-225-5324 or submit a tip online: https://tips.fbi.gov/home.** FBI is the principal investigative arm of the U.S. Department of Justice and leads the U.S. Government's investigations of criminal activity related to elections. FBI has the responsibility to investigate malicious cyber activity and potential election crimes, including the use of disinformation related to the time, place, or manner of voting.

3. **Report suspected cyber incidents to the EI-ISAC. Email soc@cisecurity.org or call 866-787-4722.** The EI-ISAC is the election community's largest cyber threat and incident information sharing mechanism. EI-ISAC is partially funded through cooperative agreement by CISA to function as a 24 x 7 x 365 analysis and information sharing hub for cyber threats and incidents and provide no-cost cybersecurity and incident response services.

PHYSICAL SECURITY INCIDENTS

1. **If there is an imminent physical threat call 911 immediately. Report physical security threats and incidents to state/local law enforcement,** in accordance with your incident response plans and identified points of contact.

2. **Report physical security threats and incidents, including suspected threats or acts of violence against election workers, to the FBI.** Contact your Election Crimes Coordinator or find your FBI Field Office: https://www.fbi.gov/contact-us/field-offices. You can also contact the FBI Internet Crime Complaint Center at www.ic3.gov, FBI's National Tip Line at 1-800-225-5324 or submit a tip online: https://tips.fbi.gov/home

3. **Report mail-related incidents and suspicious mail to the United States Postal Inspection Service (USPIS). Call USPIS at 877-876-2455 or report a mail crime online: uspis.gov/report.** USPIS is the federal law enforcement and security arm of the United States Postal Service (USPS) and protects the mail, including Election Mail sent to and from voters domestically and internationally.

4. **Share information about physical incidents that impact the security or operation of election infrastructure—power outages, loss of communication services, or other threats or hazards—with CISA. Email report@cisa.dhs.gov or 1-844-Say-CISA (1-844-729-2472) or submit online at https://www.cisa.gov/report.** Instances of criminal activity or active threats should first be reported to the appropriate local, state, or federal law enforcement entity for appropriate response. For physical incidents impacting election infrastructure, reporting to CISA enables broader stakeholder notifications of national threat trends and informs physical security risk analysis and mitigation guidance for emerging risks.

EXAMPLES

The below list provides some examples of incidents election infrastructure stakeholders are encouraged to report.

Potential Cyber Incident Examples	Potential Physical Incident Examples
• Denial-of-service incident on official websites • Compromise of account passwords or network infrastructure security keys • Successful phishing attack • Malware or ransomware incident • Suspicious network traffic or activity • Unauthorized access to data • Unauthorized network access • Website defacement or impersonation	• Intimidation, harassment, or assault of election workers • Suspicious packages or mail • Threats of violence to personnel or facilities • Unauthorized access to facilities or equipment • Vandalism of election facilities or equipment • Violence at voting locations or election facilities • Utility disruptions impacting election facilities or operations • Natural disasters impacting election facilities or operations