THE LAST MILE
Election Security Toolkit

Thousands of local jurisdictions make up the U.S. elections stakeholder community and together represent the "Last Mile" in reducing risk to election infrastructure. The CISA Last Mile initiative provides election administrators and their partners a range of customizable resources based on good practices and industry standards to help secure election infrastructure nationwide.

State and Local Election Administrators

Election Security Snapshot: Highlights the measures jurisdictions take to strengthen the security of their election systems and identifies key state and federal points of contact, as well no-cost CISA services available to jurisdictions. Jurisdictions may include priority security initiatives they plan to take in a template that tracks their progress. The Snapshot can be displayed in election offices or polling places, bolstering confidence among voters.

Election Emergency Response Guide: Assists election personnel in determining incident response steps and appropriate emergency contacts for a variety of risks that may disrupt election processes, including severe weather, violence, and fire. The Guide includes red flags for recognizing potential cyber incidents and both state and federal law enforcement and intelligence partners for reporting incidents.

Election Safeguards Guide: Communicates the specific, comprehensive security measures that election administrators have enacted to protect various components of election security. The development process may help administrators identify additional measures to implement, and the final product can build trust among voters and election workers in the integrity and security of their elections.

Election Personnel Threat Reporting Guide: Overviews state-specific definitions and laws for various types of physical threats and provides guidance for documenting and reporting threats against election personnel. It includes key federal contacts and links to additional threat reporting resources.

Cyber Incident Detection and Notification Planning Guide: Provides planning guidance to help jurisdictions recognize potential cyber incidents and develop a basic response plan. It includes key stakeholders and contact information worksheets, incident notification plans, and an incident indicators system to determine the appropriate response plan.

Vendors

EI-SCC Election Security Vendor Guide: Supports election infrastructure partners in communicating their security measures to their customers and third-party providers and recommends mitigation steps for customers. The Guide also provides CISA-approved steps for incident handling, reporting, and response planning.

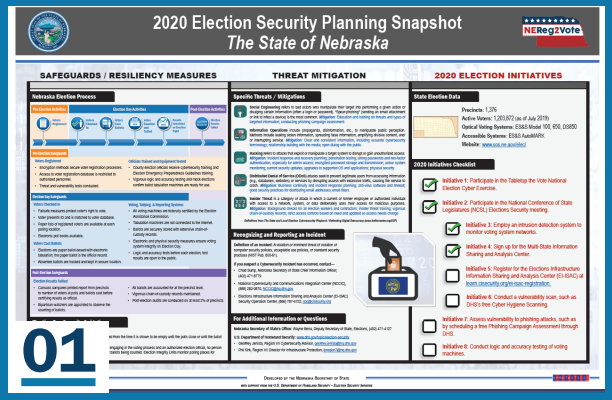
Political Outreach

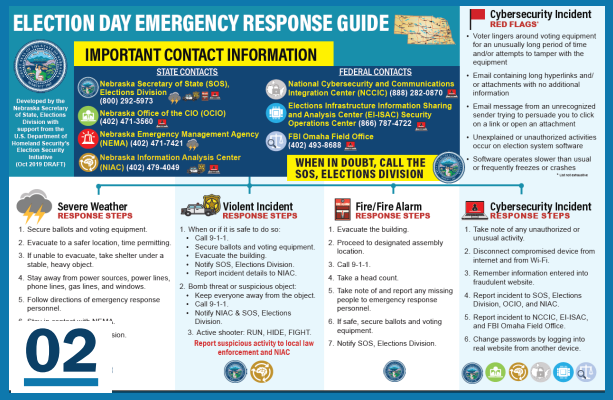
Political Party and Campaign Snapshot: Assists members of political parties and campaigns to recognize and respond to potential cybersecurity incidents. The nonpartisan Snapshot includes contact information and key election dates customized to the state.

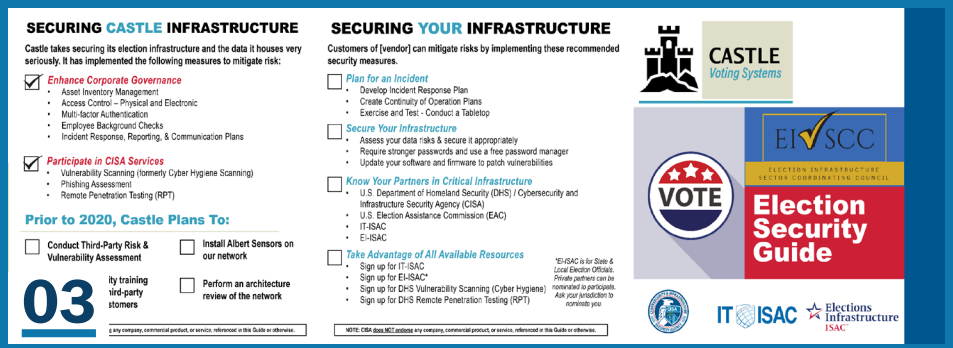
Refer to the next page for example products. Contact electionsecurity@cisa.dhs.gov to coordinate product development.

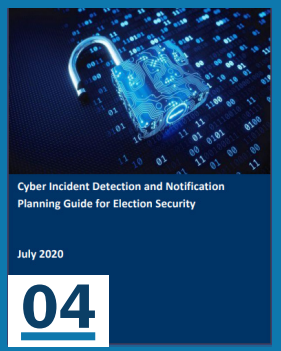
THE LAST MILE
Election Security Toolkit

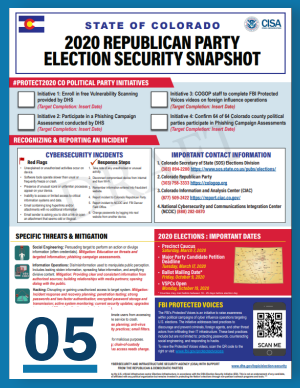
Last Mile products can be tailored to meet the unique needs of state and local election administrators, the private-sector partners that support them, and political organizations. Final products are the result of active collaboration between CISA and the customer to address dynamic or conditional cyber and infrastructure risks. **Contact electionsecurity@cisa.dhs.gov to coordinate product development.**

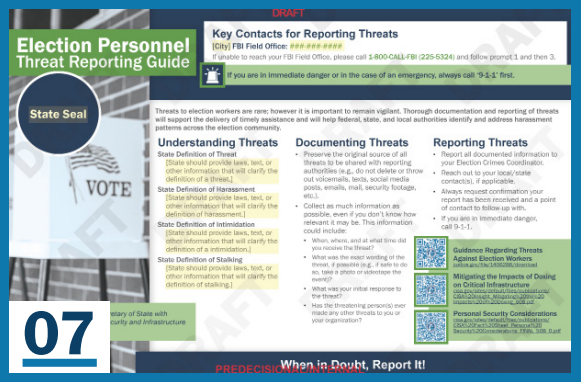












**Products shown are samples. CISA works with customers to customize templates and content.*

01 CISA introduced the **Election Security Snapshot** to provide election administrators a tool for training election workers and communicating security to stakeholders.

02 CISA created the **Election Emergency Response Guide** (EERG) in response to requests from election administrators to leverage the incident response section of the Snapshot and dive deeper into emergency response steps.

03 As vendors are a critical component of election infrastructure, CISA expanded support to provide a Snapshot of the election security measures adopted by private-sector partners through the **EI-SCC Vendor Guide**.

04 The **Cyber Incident Detection and Notification Planning Guide** further expanded upon the EERG and developed additional Last Mile incident response resources by supporting election administrators in developing their own incident response plans.

05 CISA adapted the Snapshot into the **Political Party and Campaigns Guide** to support partisan organizations in improving their cybersecurity posture.

06 Based on 2020 lessons learned from election administrators, CISA elaborated on the safeguards section of the Snapshot by creating multiple **Election Safeguards Guides** to identify and to communicate the election security measures enacted.

07 In response to an increase in threats facing election workers, CISA created the **Election Personnel Threat Reporting Guide** to support them in understanding, documenting, and reporting threats.