SEPTEMBER 2026

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

2026 ELECTION INFRASTRUCTURE SECURITY PLAN

SECURING THE NEXT 250

This Page is Intentionally Left Blank.

EXECUTIVE SUMMARY

Election infrastructure requires steadfast security and resilience. It is a vital national interest and one of the Department of Homeland Security's highest priorities to support the greater national security landscape. The American people's confidence that their vote will be counted as cast is essential, and securing election infrastructure requires year-round diligence and close coordination between state, local, and federal partners.

In January 2017, election infrastructure was designated as a critical infrastructure subsector, within the Government Services and Facilities Sector. Over the last two years, CISA has recommitted to its statutory mission and remains resolute in strengthening the security of election infrastructure, as with all critical infrastructure sectors. DHS has consistently supported CISA's delivery of cybersecurity and physical security services to election officials.

In July of this year, Secretary Mullin tasked CISA with developing the Election Infrastructure Security Plan, which had been developed to help partners defend against cyber and physical threats to election infrastructure. It describes the critical technologies and processes that support election infrastructure, details potential threats to physical, technological, and human components, and outlines the no-cost products and services provided by CISA to support election infrastructure partners and stakeholders.

National-level coordination, grounded in candid, transparent acknowledgment of threats to election infrastructure, will help partners defend against risks that could materialize during an election cycle. Coordination between the federal government, election officials, and other election infrastructure stakeholders plays an important role in sharing threat information, developing security measures and mitigation strategies, and reducing election infrastructure risks.

At the request of state and local government officials, including election officials and vendors, CISA provides no-cost, voluntary cyber and physical security services, including technical expertise, vulnerability scanning and training, as well as exercises. CISA's regional teams assist partners across the country by assessing risks, helping entities bolster defenses, improving resilience, and responding promptly to threats.

Under President Trump's and Secretary Mullin's leadership and direction, CISA's goal is to ensure the American people can trust voting systems and know that physical safety measures will be in place when they go to their assigned polling locations to cast their votes. CISA is well-prepared to support the states for any election—whether local, regional, or federal. Election security is not a partisan issue. Election security is national security.

ELECTION INFRASTRUCTURE OVERVIEW

The Election Infrastructure Subsector encompasses both physical assets such as storage facilities, polling places, and centralized vote tabulation locations used to support the election process, and the information and communications technology – including voter registration databases, voting machines, and systems to manage the election process and report results – operated on by state and local governments. Over 10,000 local election jurisdictions manage the day-to-day administration of elections, often selecting and purchasing voting systems from options certified at the state and federal level.[1] State and local election officials have the primary responsibility for protecting election infrastructure. The federal government, including CISA, provides information, tools, and resources to help these state and local officials secure their elections.

Election Infrastructure Components, Systems, and Networks

Election infrastructure encompasses physical, technological, and human elements necessary to conduct elections. As described in the Election Infrastructure Subsector-Specific Plan, the following is a list of Subsector components and assets:[2]

PHYSICAL COMPONENTS: Equipment and materials, facilities, and records that support or provide protection for the Subsector.

- **Voting Locations** – Facilities used by election officials to enable voters to cast ballots in person. Continuity of the voting process is dependent on the availability of voting locations and their ability to provide security and any other systems required to operate the voting process.
- **Technical Facilities** – Facilities used to house servers and network equipment, which can be a mix of onsite, offsite, or co-located facilities. Also, there may be separate facilities used to generate ballot files and tabulate votes.
- **Storage Facilities** – Includes warehouses or other similar facilities used to house equipment when not in use.
- **Processing Facilities** – Facilities used to print ballots, ballot envelopes, or polling place supplies. These facilities are either onsite or at a contractor's facility and must have adequate security and protection from the elements to ensure voting processes continue.
- **Administrative Facilities** – State, local, and tribal election offices where election officials carry out their election administration duties.
- **Voting Hardware** – Ballots, poll books, machines, and records, as well as the physical equipment that supports digital systems that must be stored securely and protected.

TECHNOLOGICAL COMPONENTS: Hardware and software components critical to supporting the election security mission, including computers, servers, databases, and other IT systems and assets used in Subsector activities to fulfill one of the following functions:

- **State and Local Networks** – Systems to conduct daily government functions, which may indirectly impact or connect with election system components, including email networks and other state and local-level systems, such as the Department of Motor Vehicles (DMV) systems.

[1] Who is in charge of elections in my state? | U.S. Election Assistance Commission

[2] Election Infrastructure Subsector-Specific Plan: An Annex to the NIPP 2013 (2020): Election Infrastructure Subsector-Specific Plan

- **Voter Registration Systems** – Systems used to collect personal voter information, including residency address, age, and other information required to determine voter eligibility and prevent duplicate registrations. These systems are maintained at the local jurisdiction, the state level, or a combination of both.
- **Election Systems** – Systems used to manage the entire voting process, which can include addresses, precincts, political and taxing districts, poll workers, voters, candidates, ballot layout, and the casting of votes.
- **Election Management Systems** – Sets of processing functions and voting system databases that define, develop, and maintain election databases; perform election definitions and setup functions; format ballots; and maintain ballot images, cast vote records and audit trails.
- **Tabulation Systems** – Systems used to record votes, then accumulate and present them. Votes may be recorded on paper, directly onto voting machines, or both, including through Direct Recording Electronic (DRE) machines, or optical scanners used to cast paper ballots marked by hand or with a Touch Screen Ballot Marking Device (BMD).
- **Results Reporting** – Election-night reporting systems that generate and display unofficial results. These systems can be online systems, locally hosted systems, or a combination of both. These systems operate by uploading count data to the application, which then displays the totals in relationship to the overall population of a given jurisdiction.
- **Public Information Systems** – Systems that provide the public with general information about the election process, upcoming elections, and election results. These systems can also offer individual-level information regarding registration status, provisional ballot status, mail ballot status, or voting location, or support blank ballot delivery.
- **Electronic Poll Books** – Systems used by workers at polling places or voting centers to determine the eligibility of voters and their correct ballot style. Some electronic poll books allow jurisdictions to update voter records or register voters for the first time. Electronic poll books used to update voters' addresses or register new voters will be connected to the internet, and should be secured accordingly, including multi-factor authentication for administrative functions.
- **Internal Production Software and Servers** – Various software platforms and servers that support the election infrastructure environment. This includes, but is not limited to, geographic information systems (GIS), which support the creation and assignment of eligible voters into various political and election-specific subdivisions.

KEY STAFFING ROLES: Personnel with specialized training, certification, knowledge, skills, authorities, or roles whose absence could cause undesirable consequences or inhibit the election security mission.

- **Strategic and Operational Positions** – Elected and appointed officials at the state and local level, such as local election officials, state election directors, State Chief Election Officials, Secretaries of State, and others who make up the leadership of the Subsector. These individuals operate election systems and have an in-depth understanding of their functionality. Their subject matter expertise ensures the operability of the election system. This includes operators of voting systems and related technology.
- **Temporary/Seasonal Support Positions** – Individuals selected on a short-term basis to carry out specific tasks essential to the conduct of elections, including temporary office staff, poll workers, and individuals outside the direct supervision of election officials.

ELECTION INFRASTRUCTURE THREAT LANDSCAPE

Federal, state, local, and private sector partners work closely together to secure election infrastructure from a range of cyber and physical threats. This section highlights cyber vulnerabilities, voter-registration database security challenges, insider threats, and other physical security issues that may impact the security of election infrastructure.

Cyber Vulnerabilities

Election-related software, like all complex software, contains vulnerabilities that require timely remediation. However, structural constraints within the certification ecosystem can significantly limit vendors' ability to release patches and prevent system owners from applying them quickly. Additionally, CISA's assessments show that state, local, tribal, and territorial (SLTT) election offices frequently struggle with basic cybersecurity hygiene and vulnerability remediation.

Election infrastructure is often accessible from general enterprise networks, which create opportunities for lateral movement by adversaries who compromise email systems, user workstations, or other IT assets. CISA assesses that the overall security of U.S. elections is shaped by the interaction of three major factors:

- Software vulnerability management is limited by outdated certification regimes.
- Inconsistent transparency from election system vendors regarding vulnerabilities and patch status.
- The cybersecurity immaturity of many SLTT networks responsible for hosting election systems.[3]

Across all critical infrastructure sectors, threat actors consistently rely on basic, reliable techniques that function across diverse products and environments. Instead of relying on novel exploits, they repeatedly target the same categories of weaknesses that resurface in software. These adversaries often succeed, because many preventable software flaws remain unresolved. Addressing these fundamental issues would eliminate a significant portion of today's most common compromises.

CISA recommends election officials and stakeholders to consider the following mitigation measures:

- Harmonize patch management and certification requirements for voting systems and associated IT infrastructure to allow cybersecurity updates in real-time without affecting system certification. Follow CISA's Best Practices for Securing Election Systems, at https://www.cisa.gov/news-events/news/best-practices-securing-election-systems.
- Use paper ballots that can be easily reviewed to ensure transparency, auditability, and resilience against software failures or manipulation.
- Conduct post-election manual audits of paper ballots to verify that voting systems function properly and to identify errors *before* certifying the final results.
- Encourage election software providers to:
  - Assign Common Vulnerabilities and Exposure (CVE) numbers to vulnerabilities discovered in their software;
  - Notify customers promptly if elections software source code is leaked or stolen;
  - Report cybersecurity incidents to appropriate authorities; and
  - Provide a software bill of materials (SBOM) with all delivered products.
- Ensure all security incidents and remediations activities are documented clearly, consistently, and transparently.

[3] CISA Election Report (2026) | Cybersecurity and Infrastructure Security Agency

Voter Registration Databases

Reports from the last decade reveal that Statewide Voter Registration Databases (VRDB) are attractive targets for foreign adversaries. Hackers have attempted to breach voter registration systems in all 50 states, with confirmed success in at least 20 states.[4] State and local election officials must prioritize system security and implement safeguards to prevent the exploitation of data that may already have been exposed. Priority safeguards for voter registration databases include:

- Multi-factor authentication for all administrative and remote access to the VRDB and connected systems, using phishing-resistant methods for privileged accounts where feasible.
- Network monitoring and anomaly detection, including intrusion detection sensors and a documented network baseline to identify unauthorized access attempts, unusual traffic, and any large or irregular data transfers.
- Role-based, least privileged access, with each user limited to the data required for their duties and access reviewed regularly.
- Comprehensive logging and audit trails recording who changed what, when, and under what authority, with critical logs retained for at least one year and the ability to detect and reverse unauthorized modifications.
- Architectural separation of public-facing services from the master database, so that online registration and look-up functions never interact directly with the system of recording.[5]

Insider Threats

Elections are administered at the state and local levels of government. Given the wide range of operational and short-term roles required to administer and support responsibilities during an election cycle, it is important to understand how insider threats—both intentional and unintentional—can introduce risks to conducting secure elections. An insider threat is the potential for an insider to use their authorized access or special knowledge of an organization to cause harm, whether maliciously or unintentionally.

This risk is a growing concern for election infrastructure stakeholders, including permanent staff, temporary or seasonal workers, volunteer poll workers, contractors, and vendors. Because seasonal and volunteer personnel may not undergo the same vetting as permanent staff, the election infrastructure subsector's reliance on a large temporary workforce makes insider risk a structural feature of election administration rather than an occasional exception. There are a growing number of foreign adversaries that have continued to monitor election networks and attempted to influence or interfere in U.S. elections. One way a foreign derived threat could manifest is via attempts to exploit insider access to interfere with election infrastructure or processes. Foreign adversaries, as well as other malicious actors such as criminal networks, could attempt to gain insider access through a variety of methods.

Insider Threats can take place in several ways:

- Malicious insiders who engage in sabotage, theft, espionage, or fraud — for example, making unauthorized changes to voter registration databases, ballot definitions, tabulation configurations, or results-reporting processes.
- Negligent or unintentional insiders whose mistakes introduce vulnerabilities — such as mishandling equipment, falling for phishing, or inserting unauthorized removable media into election systems.
- Third party insiders, including contractors and vendors, whose access to systems or sensitive data extends the trust boundary beyond the election office.

[4] Vulnerabilities in Electronic Voting and Ballot-Counting Systems (2026) | Cybersecurity and Infrastructure Security Agency
[5] Id.

CISA coordinates closely with federal partners, including the Federal Bureau of Investigation (FBI), to mitigate insider-threat risks to election infrastructure. Many longstanding election practices—such as handling ballots in bipartisan teams of two, allowing observers to be present during ballot counting, and maintaining chain-of-custody procedures—were specifically designed to reduce the likelihood and impact of insider threats. Election officials are encouraged to follow their state laws on these procedures. Election offices benefit from formalizing these established practices into a documented insider-threat program.

Threats to the Physical Security of Election Infrastructure

Over the past two decades, U.S. government offices and employees—including election offices and officials—have been the targets of multiple physical security incidents, such as receiving letters containing suspicious materials and bomb threats. In 2024, more than a dozen election offices across several U.S. states received letters, some containing white powder and threats. Although the powder was later determined to be non-hazardous, the intent appeared to be intimidation.[6] CISA recommends that election offices maintain procedures for handling mail and responding to potential hazardous materials exposure, and ensure all personnel are trained in these procedures.

Additionally, CISA tracked 107 election-related incidents reported via open source through its Technical Resource for Incident Prevention (TRIPwire) system between January 1, 2022, to the present. Of these incidents, 96 were bomb threats; five involved suspected explosive devices that functioned; five were suspicious packages; and one involved bomb-making materials found onsite.

From 2022 through August 2026, CISA supported 58 exercises, provided 53 Counter-Improvised Explosive Device (C-IED) trainings and technical assistance events, and conducted more than 2,100 physical security assessments, each addressing the most significant threats identified for the specific localities involved. Trends in findings from CISA's exercises revealed the importance of:

- Building and maintaining strong relationships among state and local election officials and federal partners—including CISA, the FBI, the United States Postal Inspection Service (USPIS), state and local law enforcement, emergency managers, private-sector partners, fusion centers, and Information Sharing and Analysis Centers (ISACs)—as well as other cross-sector stakeholders (e.g., communications, energy, IT) that support election operations within their jurisdiction.
- Developing and maintaining an Incident Response Plan and Continuity of Operations Plan (COOP) that addresses a range of physical security threats. These plans should be reviewed for updates at least annually, and personnel must be familiar with the plans and trained accordingly.
- Promoting trust in state and local election offices as the authoritative source for election information by prioritizing transparency and proactively sharing accurate information about election processes—including security measures, verification practices, and contingency planning activities.

[6] Election officials sent suspicious packages in at least five states

CISA NO-COST PRODUCTS AND SERVICES FOR ELECTION INFRASTRUCTURE SECURITY

CISA provides a comprehensive suite of no-cost, voluntary services to election officials and private-sector election infrastructure partners, offering support that strengthens cybersecurity, enhances physical security, and improves the overall resilience of election infrastructure.

Key Services

- End-to-end exercise planning and conduct services: Upon request and subject to available resources, CISA collaborates with state and local election officials and their security partners to design and deliver exercises tailored to the requesting organization's objectives. Each exercise concludes with an after-action report identifying strengths, areas for improvement, and recommended resources to support future planning. These exercises may take the form of seminars, workshops, or tabletop exercises, depending on needs and objectives. Seminars help orient participants to new or updated plans, procedures, or guidelines; workshops support the development of new processes; and tabletop exercises validate plans and procedures, rehearse incident response and recovery concepts, and identify gaps and opportunities for improvement.
- CISA Tabletop Exercise Packages (**CTEPs**): CISA has an extensive library of ready-to-use customizable tabletop exercise packages available on CISA.gov. Each package includes template objectives, scenarios, discussion questions, and supporting references and resources. CTEPs cover a broad range of cybersecurity and physical security topics, including several tailored for election-infrastructure stakeholders. CISA also offers workshops to help jurisdictions maximize the value of CTEP materials.
- Counter-IED and Risk Mitigation Training: CISA offers nationally accredited training and resources to help stakeholders build the capability to prevent, respond to, and mitigate bombing threats. These trainings are delivered through the Office for Bombing Prevention (OBP) and focus on practical skills, awareness, and preparedness. To learn more visit: Office for Bombing Prevention (OBP) Training Program | CISA
- Active Shooter Preparedness Webinar: This 2-hour webinar enhances awareness of active-shooters threats and teaches methods to reduce the impact of an incident. It reviews behavioral indicators, response options, and actions that increase survivability. Contact: ASWorkshop@cisa.dhs.gov.
- Conflict Prevention Webinar: This 1-hour training assists participants in recognizing warning signs of escalating behavior, assessing situations involving persons of concern, and applying practical de-escalation strategies using non-threatening actions. Contact: ConflictPrevention@cisa.dhs.gov.
- Insider Threat Mitigation Workshop & Briefing: This 2-hour briefing supports the improvement and development of insider-threat mitigation capabilities, by emphasizing a multidisciplinary, holistic approach to identifying and reducing insider threats. Contact: SecurityPlanning@cisa.dhs.gov.
- **Canaries and Canary Tokens:** CISA deploys decoy systems and digital tokens across participating organizations' networks to help detect unauthorized access and lateral movement. This early-warning capability—jointly monitored by CISA and participating organizations—enhances threat detection and strengthens incident-response readiness for prioritized organizations.
- **Cloud Security & Assurance Service:** A voluntary offering that helps organizations strengthen their cloud-security posture, reduce systemic risks, and prepare for emerging threats. The service delivers deep visibility, risk-driven insights, and actionable recommendations to strengthen cloud environments.
- **CISA Attack Surface Testing (CAST):** CAST delivers continuous penetration testing for critical infrastructure organizations. The service evaluates network accessibility and reviews web

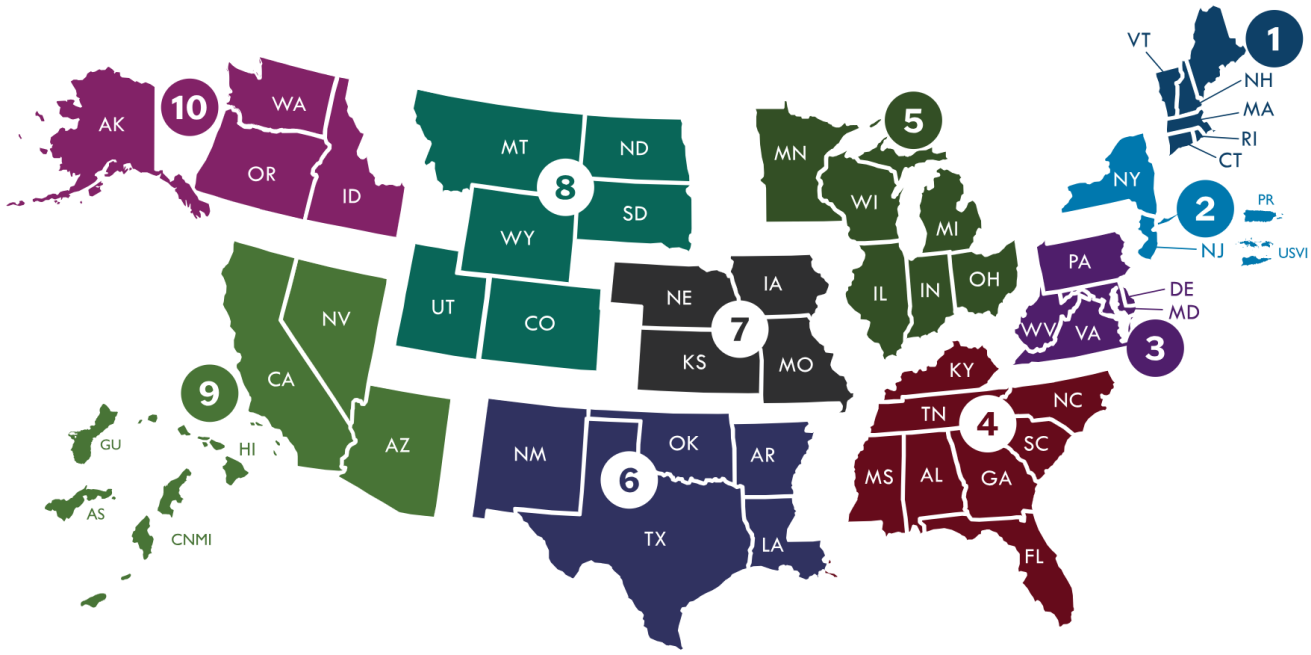
applications for exploitable weaknesses, enabling organizations to proactively manage their attack surface and verify the effectiveness of remediation efforts.

- .gov Domain Program: CISA sponsors the .gov top-level domain and offers it at no cost to U.S.-based government organizations and publicly controlled entities, helping improve authenticity, trust, and security for official digital services.
- **Vulnerability Scanning:** This service continuously monitors internet-accessible network assets (public, static IPv4 addresses) for vulnerabilities and risky configurations. Participants receive weekly reports detailing all findings, along with ad-hoc alerts for urgent issues such as unsafe services and known exploited vulnerabilities. For more information and sign-up: Cyber Hygiene Services | CISA.
- **Web Application Scanning (WAS):** This service conducts in-depth assessments of publicly accessible web applications to identify vulnerabilities and misconfigurations that attackers could exploit. WAS evaluates issues including—but not limited to—items in the Open Web Application Security Project (OWASP) Top Ten, which covers the most critical web-application security risks. Participants receive monthly detailed reports and may request on-demand assessments to help maintain continuous web-application security. For more information and sign-up: Cyber Hygiene Services | CISA.
- **Risk & Vulnerability Assessments (RVAs):** CISA provides full RVAs—including on-site penetration tests—for mature critical infrastructure organizations. RVAs provide a comprehensive evaluation of an entity's security posture, covering internal and external systems, authentication weaknesses, network architecture, and exploitable pathways. Each RVA results in a detailed, actionable report outlining risks and mitigation steps. For more information and sign-up: Risk and Vulnerability Assessments | CISA.
- **Cybersecurity Performance Goals (CPGs) Assessment 2.0:** The CPGs 2.0 represent voluntary, high-impact security practices that form a prioritized baseline for organizations of all sizes. Developed from CISA's operational data and collaboration across government and industry, the CPGs help critical infrastructure owners reduce cyber risk by focusing on action most correlated with preventing or mitigating attacks. For CPGs: Cybersecurity Performance Goals 2.0 (CPG 2.0) | CISA. For assessment training: Cybersecurity Performance Goals (CPGs) Assessment Training | CISA.
- **CISA's Known Exploited Vulnerabilities (KEV) Catalog:** To support the cybersecurity community and network defenders—and to help organizations better manage vulnerabilities and keep pace with active threat activity—CISA maintains the authoritative public catalog of vulnerabilities known to be exploited in the wild. Organizations should incorporate the KEV catalog into their vulnerability-management prioritization processes to ensure that the most critical and high-risk vulnerabilities are addressed first. Learn more about how to use the KEV catalog in your organization.
- **CISA Learning:** CISA offers no-cost online cybersecurity training on topics including cloud security, ethical hacking, risk management, malware analysis, and more. CISA Learning replaces the Federal Virtual Training Environment (FedVTE) and is available to federal, state, local, tribal, and territorial government staff and contractors, Veterans and military personnel, and U.S. residents. For questions or access visit CISA Learning | NICCS.

CISA's Regional Security Advisors

CISA's cadre of critical infrastructure security experts, located around the country, provides tailored support to election infrastructure stakeholders. CISA's 10 Regional Directors serve as Election Security Advisors (ESAs) for their respective regions, building trusted relationships with election officials and overseeing the delivery of CISA's cyber and physical security services. Cybersecurity Advisors (CSAs) offer onsite cyber assessments and provide targeted cybersecurity guidance based on an organization's specific security posture. Protective Security Advisors (PSAs) can assess physical infrastructure security risks and provide options for consideration to reduce vulnerability to physical threats.

Regional advisors play a critical role in ensuring SLTT partners receive timely, expert support aligned with national cybersecurity risk-reduction priorities.



To connect with your regional advisors or schedule services, you can reach out to your local CISA regional office—contact details are available at cisa.gov/about/regions. This aligns directly with CISA's broader election security support model, which emphasizes voluntary, no-cost assistance delivered through regional teams.

Enterprise data confirms that CISA's regional personnel, including CSAs and PSAs, provide localized cyber and physical security support, vulnerability scanning, incident-response assistance, and election infrastructure security services to SLTT partners. These regional teams work closely with election officials to assess risk, strengthen defenses, and coordinate timely support during any heightened threat conditions. For current information and to request services, visit the CISA Election Security Services Page,[7] which provides up-to-date resources, offerings, and points of contact for election infrastructure stakeholders.

[7] All information drawn directly from official CISA resources on election security services (as of July 2026). Services remain voluntary and available upon request. For more information, see the U.S. Cybersecurity and Infrastructure Security Agency's Election Security Services: https://www.cisa.gov/topics/election-security/election-security-services

Information Sharing for Election Infrastructure Stakeholders

Timely, accurate threat information is essential to securing election infrastructure. State and regional fusion centers serve as a key channel for sharing threat intelligence and risk-assessment data, strengthening the security and resilience of election operations. As state-owned and operated entities, fusion centers integrate state, local, and federal partners to address both cyber and physical risks to election infrastructure. They serve as a channel for threat reporting, analysis, and information sharing. Applied to elections, this model lets officials receive briefings and indicators relevant to election systems, report detected or suspected threats and incidents and obtain analytic and situational-awareness support during election periods.

Fusion centers offer several advantages:

- Fusion centers already coordinate on physical security threats to election operations, such as bomb threats, suspicious mailings, and disruption of election facilities, alongside cyber threats, giving election officials a single channel for the full range of risks.
- Fusions centers are owned and operated by the states; an election information sharing model built on Fusion Centers keeps the function under state control and aligned with the constitutional role of states in administering elections.

To learn more about Fusion Centers and to locate the one closest to you, please visit Fusion Center Locations and Contact Information | Homeland Security.

Additionally, CISA communicates with state and local partners regularly and provides them with timely threat intelligence, expertise, no-cost tools and resources these partners need to defend against risks. This includes working with various private information sharing and analysis centers to share cybersecurity information and guidance. State and local governments seeking assistance are encouraged to contact our CISA regional teams who can help assess risk, strengthen defenses, enhance resilience, and respond immediately to incidents.

For the 2026 election cycle, CISA is supporting an information-sharing platform to exchange intelligence and situational updates in a familiar, low-barrier environment. All Fusion Centers, State and Local election officials will have access to this information sharing tool at no cost. The platform supports near real-time communications, and gives officials a single, accessible space to receive indicators, ask questions and coordinate with peers and federal partners. Federal partners, Fusions Centers, Federal Agencies and CISA Central will be actively engaged on the platform for day-to-day communication with state and local election officials. This model was successfully deployed and utilized during FIFA World Cup 2026. It is easy to use, modernizes election information sharing and enhances state and federal collaboration.

CISA is also working to build improved access to timely and actionable intelligence through unclassified and classified threat briefings and indicators for election infrastructure partners and stakeholders. CISA partners with DHS's Office of Intelligence and Analysis (I&A) and the FBI to support the flow of federal threat reporting to state and regional fusion centers and, through them, to the state and local officials who need it.

Security Operations Center (SOC) Call: The SLTT SOC call is a technical exchange discussing key cybersecurity issues affecting SLTT entities and the cyber community. Please work with your CISA Regional Office to get connected by going to CISA Regions | CISA.

Critical Infrastructure Intelligence Initiative (CI3): In partnership with DHS I&A and the Office of the Director of National Intelligence (ODNI), CISA leads the Critical Infrastructure Intelligence Initiative (CI3), a regularly scheduled monthly classified threat briefing during which the Intelligence Community (IC) briefs cleared critical infrastructure stakeholders at the state and local levels. The threat briefing,

which spans cyberattacks, foreign adversaries, emerging threats, and critical infrastructure owner and operator concerns, is broadcast to over 70 secure locations nationwide, including state and regional fusion centers, FBI Field Offices, and National Guard Locations. In addition to delivering classified information to cleared partners, CI3 pairs each briefing with monthly Unclassified//For Official Use Only notes and mitigation recommendations to ensure that the threat intelligence presented is accompanied by actionable measures that can be shared with state and local security professionals and government officials to enhance critical infrastructure security and resilience, including elections systems. Beyond providing a common baseline understanding of risks and threats, the CI3 program ensures stakeholders have the relationships, contacts, and access points necessary to obtain immediate access to sensitive information during emergencies.

State, Local, Tribal, and Private Sector Clearance Program: CISA also provides access to classified threat intelligence through its State, Local, Tribal, and Private Sector Clearance Program (SLTPS), which provides clearances to owners, operators, and decision-makers for critical systems, such as election infrastructure. Stakeholders leverage these clearances to access actionable, timely, and relevant classified information, which is then used to strengthen systems and inform resource decisions. For additional details, or to learn more about the nomination process, please contact your Sector Risk Management Agency point of contact, or email CISA.SLTPS@cisa.dhs.gov.

CONCLUSION

In conclusion, the CISA 2026 Election Infrastructure Security Plan represents a comprehensive commitment to safeguarding the integrity of the United States electoral process. By leveraging collaborative partnerships, robust cyber defenses, and ongoing threat intelligence, the plan ensures that all stakeholders are prepared to address evolving risks. Continued vigilance, adaptability, and transparency will be essential as we work together to protect the foundations of our Constitutional Republic and maintain public trust in our elections.

For more information about election security and resources to protect elections, see the CISA election security resources at https://www.cisa.gov/topics/election-security.