Center for Internet Security®

No Cost and Fee-based Services

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

The MS-ISAC® is the U.S. Department of Homeland Security (DHS) designated key resource for cyber threat prevention, protection, response, and recovery for all U.S. State, Local, Tribal, and Territorial (SLTT) governments. Funded through a Cooperative Agreement with DHS, the MS-ISAC is a cooperation between DHS and CIS® (Center for Internet Security®), a 501(c)(3) nonprofit. MS-ISAC membership is a voluntary and collaborative relationship with all 50 states, 6 territories, the 79 DHS-recognized fusion centers, and thousands of local and tribal governments, including school districts, public safety, and public utilities. https://www.cisecurity.org/ms-isac/ or info@cisecurity.org.

MS-ISAC Membership is open to all SLTT government organizations, including public K-12 education entities, public institutions of higher education, authorities, and any other non-federal public entity in the United States of America.

Elections Infrastructure ISAC®

The EI-ISAC® operates under a Cooperative Agreement with DHS and provides eligible agencies an elections-focused cyber defense suite, including sector-specific threat intelligence products, incident response, threat and vulnerability monitoring, cybersecurity awareness and training products, and tools for implementing security best practices. https://www.cisecurity.org/ei-isac/ or elections@cisecurity.org.

EI-ISAC Membership is open to all SLTT government organizations that support the elections officials of the United States of America, and associations thereof.

MS-ISAC/EI-ISAC Partnerships are formal agreements between the ISACs and agencies that provide value to SLTT governments.

Available to Everyone:

- **National Webcasts.** Webcasts are held every other month in cooperation with DHS. The National Webcasts bring relevant speakers on timely topics.
- **Cybersecurity Advisories.** Patch and vulnerability notices are distributed on an ad-hoc basis for the most common software.
- **Cyber Tips Newsletters.** Monthly newsletters are targeted to provide end-user cybersecurity education and available for download as a Word document.

No Cost Services for ISAC Members, Partners, and SLTT Governments:

- **Security Operations Center (SOC).** CIS operates a 24x7 operations floor that serves as a centralized triage point for threat and vulnerability detection, analysis, notifications, and assistance. Email soc@cisecurity.org or call 1-866-787-4722.
- **IP Address & Domain Monitoring.** A variety of services based on knowledge of SLTT government, critical infrastructure, and partner IP addresses and domains, including potential Account Compromise, Darkspace, Web Profiler and Port Profiler notifications, as well as Botnet Notifications in cooperation with Spamhaus. Contact info@cisecurity.org for more information.
- **Malware IP Address and Domain List.** A list of identified IP addresses and domains related to malware activity that is distributed weekly. Contact soc@cisecurity.org for more information.
- **Threat-Based Vulnerability Assessments.** SLTT governments experiencing a targeted cyber threat have access to a free one-time network and web application vulnerability assessment of up to 10 public facing IP addresses and 5 public facing web applications. These assessments include a manual analysis and verification of vulnerabilities discovered, prioritized remediation steps, customized reporting, and remediation support. Contact vmp@cisecurity.org for more information.

For more information on officially partnering with the ISACs, send an email to info@cisecurity.org with the subject line: Partnership Request.

No Cost Services for ISAC Members and SLTT Governments:

- **Computer Emergency Response Team (CERT).** Incident response, computer forensics, and malware analysis services are available. Contact soc@cisecurity.org to engage these services.
- **Nationwide Cyber Security Review (NCSR).** Based on the NIST Cyber Security Framework, and sponsored by the MS-ISAC and DHS, the NCSR is an anonymous, annual self-assessment designed to measure gaps and capabilities of SLTT governments' cybersecurity programs. More information is available at https://www.cisecurity.org/ms-isac/services/ncsr/.
- CIS SecureSuite® Membership. CIS SecureSuite Membership. Membership includes access to multiple CIS resources, such as full-format CIS Benchmarks; CIS Workbench; and the CIS Configuration Assessment Tool (CIS-CAT) Pro, which provides a fast, detailed assessment of target systems' conformance with CIS Benchmarks. Contact freesecuresuite@cisecurity.org for more information.

No Cost Services for ISAC Members and Partners:

ISAC members and partners are encouraged to contact info@cisecurity.org for more information about any of the following services.

- **Situational Awareness Reports.** Reports highlight recent operational statistics, incidents, malware, malicious IP addresses, and SLTT government trends. A quarterly version of this report is issued specifically for the elections community.
- **Cyber Alerts.** Short, timely emails contain intelligence on a specific cyber incident, threat, actor, trend, pattern, or new tactic, technique, or procedure (TTP). Elections officials and partners are eligible to receive specialized election products tailored to this unique environment.
- **Intel Products.** Weekly, monthly, and ad hoc alerts and notifications focus on timely issues with actionable recommendations for improving cybersecurity. Elections officials and partners are eligible to receive specialized election products tailored to this unique environment.
- **Members and Partner-Only Webinars.** Monthly, bimonthly, and ad-hoc webinars focus on special topics, incidents, and the State of the ISACs to increase cyber awareness and education.

No Cost Services for ISAC Members:

ISAC members are encouraged to contact info@cisecurity.org for more information about any of the following services.

- **DHS's Homeland Security Information Network (HSIN).** Members have access to the DHS HSIN portal and the ISAC Communities of Interest, containing the alert maps, recorded webcasts, discussion areas, and a library of historical documents.
- **Cybersecurity Awareness Toolkit.** Annually, educational materials, including posters and calendars, are distributed to raise end user cybersecurity awareness. Digital and hard copy materials are available for order at no cost.
- **Working Groups.** SLTT governments can participate in the Mentoring Working Group as mentors or mentees or in the Application Security, Business Resiliency, Education and Awareness, Intelligence and Analysis, or Metrics working groups.
- **Annual Meeting.** An annual multi-day event brings all members together, along with the DHS representatives.
- **Election Day Situation Room.** For members, the EI-ISAC established a Cyber Situational Awareness Room, which allows officials across multiple jurisdictions to communicate with each other regarding ongoing threats during elections.
- **Malicious Code Analysis Platform (MCAP).** A web-based service enables members to submit suspicious files and URLs for analysis in a controlled and non-public fashion. ISAC members may contact mcap@cisecurity.org to sign up for an account.
- **Anomali.** A STIX/TAXII offering that includes two tools for analyzing and sharing indicators, STAXX and ThreatStream. STAXX is a free tool that can subscribe to and publish STIX/TAXII feeds. Members also receive access to Anomali ThreatStream, an advanced platform for threat information sharing, research, and analysis. Contact indicator.sharing@cisecurity.org to sign up for an account.

NO COST AND FEE-BASED SERVICES

For more information on officially partnering with the ISACs, send an email to info@cisecurity.org with the subject line: Partnership Request.

Cost Effective Services from CIS:

CIS offers additional services for a fee to U.S. SLTTs. Contact services@cisecurity.org for more information about these services.

- 

Albert: CIS Networking Monitoring. CIS offers a unique network Intrusion Detection System (IDS) tailored to the SLTT government environment. Actionable notifications are sent after the SOC conducts an in-depth review to eliminate the majority of false positives and non-actionable activity.
- **Managed Security Services (MSS).** Expert analysis and auditing of firewalls, routers, endpoints, servers, and more.
- **Vulnerability Assessments.** Assessments include a combination of automated and manual analysis that assesses networks to identify and report on critical vulnerabilities with prioritized remediation steps and support. Payment Card Industry (PCI) compliance scanning is also available.
- **Penetration Tests.** Network, web application, wireless, and other penetration testing services simulate a real-world cyber attack, allowing organizations to safely review the security posture of their networking devices and web applications.
- **Phishing Engagements.** Customized assessments aid organizations in assessing their vulnerability to phishing attacks.
- **CIS CyberMarket®** A collaborative purchasing program serves SLTT government organizations, not-for-profit entities, and public health and education institutions to improve cybersecurity through cost-effective group procurement. Contact info@cisalliance.org for more information.
- **CIS Hardened Images™** Virtual machine images hardened in accordance with the CIS Benchmarks secure configuration guidelines. Available from major cloud computing platforms like AWS, Azure, and Google Cloud Platform.