August 26, 2026 Version: 5.0

COMMUNICATIONS SECTOR COORDINATING COUNCIL

Resource Guide: CISA Support to Private Sector Critical Infrastructure Owners and Operators

Resources & Tools

For owners and operators of critical infrastructure across the country, the Cybersecurity and Infrastructure Security Agency (CISA) offers an array of no-cost resources and tools, such as technical assistance, exercises, cybersecurity assessments, no-cost training, and more. Within each CISA Region are local and regional Protective Security Advisors (PSAs), Cyber Security Advisors (CSAs), and Emergency Communications Coordinators (ECCs). These "field personnel" assess, advise, assist, and provide a variety of risk management and incident management services. Below is a sampling of the "local" services provided through CISA regional offices. Also visit https://www.cisa.gov/audiences/small-and-medium-businesses for featured services that support smaller communications and critical infrastructure entities with cybersecurity and risk management initiatives.

Physical Security

- **Assist Visits** help critical infrastructure owners and operators understand how their service fits into a critical infrastructure sector and explain the CISA resources available to enhance their security and resilience.
- **Security Assessment at First Entry (SAFE)** is a stand-alone assessment provided to critical infrastructure entities that features standard language, high level vulnerabilities, and options for consideration. It is designed to assess the current security posture and produce a report in under two hours.
- The **Infrastructure Survey Tool (IST)** is a voluntary, web-based assessment to identify and document the overall security and resilience of a facility.
- The **Infrastructure Visualization Platform (IVP)** is a data collection and presentation medium that combines immersive imagery, geospatial information, and hypermedia data of critical facilities and surrounding areas.
- CISA's **Be Air Aware**™ resources provide essential, ready-to-use information about UAS cyber and physical threats and steps to effectively manage risk to critical infrastructure and public gatherings.
- The **C-IED Technical Assistance Program (TAP)** strategically guides comprehensive Improvised Explosive Device (IED) incident risk management and provides preparedness assistance by leveraging resources from across the C-IED enterprise.

Cybersecurity

- **Cyber Hygiene Services** help secure internet-facing systems from weak configurations and known vulnerabilities. These remote scanning and testing services help organizations reduce their exposure to threats by taking a proactive approach to mitigating attack vectors.
- Cross-Sector **Cybersecurity Performance Goals** (CPGs) are a common set of practices all organizations should implement to kickstart their cybersecurity efforts. Small- and medium-sized organizations can use the CPGs to prioritize investment in a limited number of essential actions with high-impact security outcomes.
- The **Assessment Evaluation and Standardization (AES)** program is designed to enable organizations to have a trained individual that can perform several cybersecurity assessments and reviews in accordance with industry and/or federal information security standards.

Disclaimer: This information was compiled from publicly available content on the Cybersecurity and Infrastructure Security Agency (CISA) website. Programs, resources, and details referenced in this factsheet may change as CISA updates its site. Please visit cisa.gov to confirm that the programs and resources listed remain current and available.

- Additional **Services | CISA.** CISA has compiled a list of no-cost cybersecurity tools and services. The list includes cybersecurity services provided by CISA and other federal partners, widely used open-source tools, and no-cost tools and services offered by private and public sector organizations across the cybersecurity community.
- **Cybersecurity Resources for High-Risk Communities | CISA.** As America's cyber defense agency, CISA—through JCDC—has compiled a list of cybersecurity resources intended to help high-risk communities who are at heightened risk of being targeted by cyber threat actors because of their identity or work.

Emergency Communications

- The interactive **Public Safety Communications and Cyber Resiliency Toolkit** is kept up to date with the latest guidance to assist those responsible for communications networks in evaluating current resiliency capabilities, identifying ways to improve resiliency, and developing plans for mitigating the effects of potential threats.
- CISA offers three **Priority Telecommunications Services** that enable essential personnel to communicate when networks are degraded or congested due to weather events, mass gatherings, cyberattacks or events stemming from human error.

Training & Exercises

CISA offers a wide array of no-cost training programs. These web-based independent study courses, instructor-led courses, and associated training materials provide critical infrastructure owners and operators with the knowledge and skills needed to implement security and resilience activities. CISA provides end-to-end exercise planning and conduct support to assist stakeholders in examining their cybersecurity and physical security plans and capabilities. See the complete list at cisa.gov/critical-infrastructure-training.

- CISA offers a comprehensive set of **Active Shooter Preparedness Training** courses, materials, and workshops to enhance preparedness against an active shooter threat, focusing on behaviors that represent warning signs and characteristics of active shooter incidents.
- CISA hosts multiple **Conflict Prevention Information Sessions** tailored to offer strategies and techniques to assist with managing conflict and preventing incidents of targeted violence, including the Power of Hello, De-escalation, Personal Security Considerations, and Insider Threat Awareness and Mitigation.
- CISA offers a diverse curriculum of accredited training through multiple platforms to build **Counter-Improvised Explosive Device (C-IED)** capabilities. Topics include Bomb Threats, Suspicious Activity and Items, IED Awareness, Protective Measures and Planning and Preparedness.
- **CISA Tabletop Exercise Packages** are a comprehensive set of resources designed to assist stakeholders in conducting their own exercises and initiating discussions within their organizations about their ability to address a variety of threat scenarios. The packages include the scenario-specific situation manual, planner handbook, facilitator/evaluator handbook, and assorted forms and templates. Facilities can also request CISA expertise in facilitating a live tailored tabletop exercise.

Authors: Stephanie Woods (stephanie.m.woods@lumen.com) & Brianna Bace (bbace@ustelecom.org)