IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

DEFEND TODAY,
SECURE TOMORROW

REGION 5

The Cybersecurity and Infrastructure Security Agency (CISA) delivers services to support the security and resilience of critical infrastructure owners and operators and state, local, tribal, and territorial partners through 10 regions, inclusive of all states and territories.

CISA regional personnel work with critical infrastructure partners and communities to:

- **Support** preparation, response, and recovery efforts for hazards impacting critical infrastructure
- **Safeguard** soft targets and crowded places
- **Conduct** and **integrate** infrastructure assessments and analysis, including dependencies and cascading effects, on critical infrastructure to influence decision-making at all phases of emergency management
- **Facilitate** information sharing between public and private sector critical infrastructure partners
- **Enhance** election infrastructure security and other critical infrastructure cyber systems
- **Improve** situational awareness of cybersecurity risks and incidents

AT-A-GLANCE

Regional Office: Chicago, Ill.

Coverage Area: Illinois, Indiana, Michigan, Minnesota, Ohio, Wisconsin; 34 Tribal Nations

Size: 388,306 square miles

Estimated Population: 52.5 million; 16% of the country

Key Facts:

- Home to the largest body of fresh water in the world
- Major hub for critical manufacturing, transportation (rail, air, maritime locks/dams), agricultural, financial, and commercial facilities
- 25% of all U.S.–Canada trade passes through the Detroit-Windsor corridor

Through a regional office in Chicago, Region 5 personnel manage mission execution through steady state and incident operations, critical infrastructure analysis, and strategic outreach to critical infrastructure partners. Protective Security Advisors (PSA), Chemical Security Inspectors (CSI), Cyber Security Advisors (CSA), and Emergency Communications Coordinators (ECC) coordinate their critical infrastructure protection missions through the regional office and collaborate on regional critical infrastructure efforts. Regional office personnel include external affairs specialists, analysts, administrative officers, and coordinators for training, outreach, and operations.

CYBERSECURITY

CSAs conduct security assessments in partnership with stakeholders, including critical infrastructure owners and operators. Core assessments, including the **Cyber Infrastructure Survey, Cyber Resilience Review**, and **External Dependency Management**, provide a strategic, all-encompassing assessment of an organization's cyber posture.

CSAs host **cyber workshops**, joining stakeholders across existing cybersecurity initiatives and groups to enhance information sharing. CSAs can also connect critical infrastructure partners to a variety of cyber risk management capabilities through the Critical Infrastructure Cyber Community Voluntary Program. CISA also offers cybersecurity services to election officials throughout the country to safeguard their election systems.

INFRASTRUCTURE SECURITY

PSAs conduct Assist Visits to meet with facility owners and operators and provide critical infrastructure facilities with an overview of available DHS and CISA services.

Assist Visits are often followed by security surveys using the **Infrastructure Survey Tool** (IST), **Security Assessment at First Entry** (SAFE), or delivery of other CISA services. The IST and the **Rapid Survey Tool** examine the most critical aspects of a facility's security and resilience posture, and an IST will compare a facility against the national average for similar

facilities. The SAFE tool, suited for all facilities, assesses the current security posture and identify options for facility owners and operators to mitigate relevant threats.

CISA also provides trainings, tools and resources on active shooter preparedness, soft targets/crowded places, counter-improvised explosive devices, K-12 school security, and faith-based organizations/houses of worship preparedness.

EMERGENCY COMMUNICATIONS

CISA supports and promotes the nationwide improvement of emergency communications capabilities. ECCs engage with stakeholders and address the complex issues facing the emergency communications ecosystem.

ECCs seek to build partnerships between federal, state, local, tribal, and territorial government stakeholders as well as the private sector. These partnerships result in a united effort to improve the Nation's operable and interoperable emergency communications.

CHEMICAL SECURITY

CSIs perform regulatory activities for **high-risk chemical facilities** under the Chemical Facility Anti-Terrorism Standards program. These facilities must meet and maintain risk-based performance security standards appropriate to the facilities and the risks they pose.

CSIs conduct regulatory inspections, respond to facilities' **compliance assistance** requests, and support facility **security plan development**. CSIs also engage in outreach with stakeholders; private industry; and federal, state, and local partners to coordinate the protection of covered facilities with local first responders, identify potential chemicals of interest, and share information.

EVENT SUPPORT

Regional personnel provide risk assessments, security-focused strategic planning expertise, threat and hazard information, and on-site support for **National Special Security Events** and **Special Event Activity Rating** events occurring in the region, as well as other major events, as requested by state and local partners.

FEDERAL FACILITY SECURITY

Working closely with federal partners, the regional team implements the Interagency Security Committee **security standards** and **best practices** for nonmilitary federal facilities.

INCIDENT SUPPORT AND ANALYSIS

Regional personnel provide pre- and post-incident analysis, assessment, and stakeholder communication to support strong decision-making and improved resilience. Additionally, they provide critical infrastructure prioritization information, geospatial analysis, and share information with DHS HQ and other federal agencies during special events and in response to threats and incidents.

The region administers the **Regional Resiliency Assessment Program** (**RRAP**), a voluntary cooperative assessment of specific critical infrastructure within a designated geographic area and a regional analysis of the surrounding infrastructure. RRAPs address a range of infrastructure resilience issues that could have regionally- and nationally-significant consequences.

TRAINING AND EXERCISES

Physical and cybersecurity **exercises, ranging from seminars, workshops, tabletops to full-scale exercises**, are supported by the Region to test facility plans and procedures, identify gaps, and recognize lessons learned and best practices. The Region also provides support to federal, state, local, and regional exercises organized by other organizations.

For more information on Region 5:

- Visit the Regional Office website: cisa.gov/region-5
- Contact regional staff at CISARegion5@hq.dhs.gov