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

REGION 1

The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future.

CISA regions lead and support public and private sector partners in developing and maintaining secure and resilient infrastructure. Regional personnel work with critical infrastructure partners and communities in the region to:

- **Improve** situational awareness of cybersecurity risks and incidents
- **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

AT-A-GLANCE

Regional Office: Boston, MA
Location: Conn., Maine, Mass., N.H., R.I., Vt.; 10 Tribal Nations
Size: 71,992 square miles
Estimated Population: 14,810,001
Key Facts:

- Smallest region (as measured in overall area) with one of the highest population densities (232 people per square mile). Fifty-five percent of New England residents live within the Boston metro area
- Five of the six states rank in the top 10 most energy-efficient states (2016)
- Home to the first subway system in North America

Led by a Regional Director located in Boston, MA, the Region 1 personnel provide cybersecurity, physical infrastructure security, chemical security and emergency communications services to critical infrastructure partners throughout New England. This cadre of security professionals manage mission execution through steady state and incident response support operations.

Regional personnel coordinate training events and exercises for stakeholders; participate in external planning with government and private sector partners; and provide advice and expertise to stakeholders on infrastructure protection, data tools and information sharing platforms, critical infrastructure sector specialties, and resilience and recovery.

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 (NSSEs)** and **Special Event Activity Rating (SEAR)** events occurring in the region, as well as other major events, as requested by state and local partners.

CHEMICAL SECURITY

Chemical Security Inspectors (CSIs) perform regulatory activities for high-risk chemical facilities under the Chemical Facility Anti-Terrorism Standards (CFATS) regulatory program (6 CFR). 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 program outreach with 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.

OUTREACH AND EXERCISES

Regional personnel organize physical and cyber security **exercises (ranging from seminars, workshops, tabletops to full-scale exercises)** that test facility plans and procedures, identify gaps, and recognize lessons learned and best practices. Regional personnel also provide support to federal, state, local, and regional exercises organized by other organizations.

Regional personnel offer **DHS Active Shooter Preparedness Training/Workshops, Supply Chain Workshops, Dams Security Workshops,** and others.

Regional personnel facilitate delivery of DHS Office for Bombing Prevention training courses (in-person and virtually) to prevent, protect against, respond to, and mitigate bombing incidents, including **Improvised Explosive Device (IED) Awareness and Safety Procedures, Bomb Threat Management Planning, Active Threat Awareness, IED and Vehicle-Borne Threat Detection, Sports and Entertainment Venues Bombing Prevention Solutions Portfolio,** and more.

CSAs conduct **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 (C3) Voluntary Program.

PHYSICAL AND CYBERSECURITY ASSESSMENTS

Protective Security Advisors (PSAs) conduct Assist Visits to provide critical infrastructure facilities with an overview of available services and/or provide a facility walk-through. PSAs conduct assessments using the Infrastructure Survey Tool (IST) or the Security Assessment at First Entry (SAFE) Tool to identify and document the overall security and resilience of a facility; and the Infrastructure Visualization Platform (IVP) to collect data to develop an interactive visual representation of critical infrastructure, which helps guide special event planning and incident response operations.

PSAs administer 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.

Cybersecurity Advisors (CSAs) cultivate partnerships with stakeholders and initiate information sharing. CSAs introduce organizations to various no-cost CISA cybersecurity products and services, along with other public and private resources. CSAs also collaborate with local and federal entities to facilitate delivery of cybersecurity services across the U.S. They conduct several types of no-cost cybersecurity assessments: Cyber Infrastructure Survey, Cyber Resilience Review, External Dependency Management Assessment Package.

INCIDENT SUPPORT AND ANALYSIS

Regional personnel provide pre- and post-incident analysis, assessment, and stakeholder communication to support strong decision-making and improved resilience.

Regional personnel provide critical infrastructure prioritization information, geospatial analysis, and information sharing to DHS HQ and other federal agencies during special events and in response to threats and incidents.

Regional personnel collaborate to determine impacts to regionally-significant critical infrastructure and cross-sector impacts within an incident area.

Regional personnel determine dependencies and cascading effects on critical infrastructure beyond the immediate incident area and directly affected critical infrastructure sectors.

Regions may deploy Infrastructure Specialists to Joint Field Offices, Emergency Operations Centers, and other command centers during a special event or incident, as necessary.

FEDERAL FACILITY SECURITY

Regional personnel work closely with Federal partners in the region to implement the Interagency Security Committee **security standards** and **best practices** for nonmilitary federal facilities.

For more information on Region I:

- Visit the Regional Offices website: https://www.dhs.gov/cisa/cisa-regional-offices
- Contact regional staff at CISARegion1@hq.dhs.gov