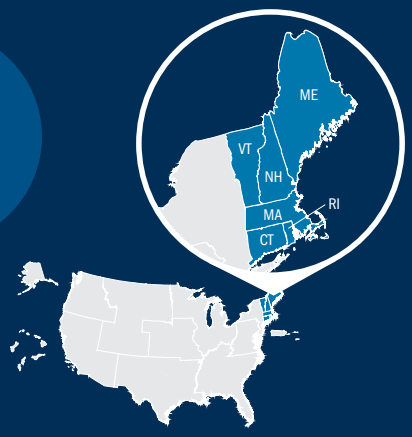
CISA
CYBER+INFRASTRUCTURE



CYBERSECURITY + INFRASTRUCTURE SECURITY AGENCY

REGION I

REGION I AT-A-GLANCE

REGIONAL OFFICE:	LOCATION:	SIZE:	ESTIMATED POPULATION:	KEY FACTS:
BOSTON, MA	**6 STATES 10 TRIBAL NATIONS**	**71,992 SQUARE MILES**	**14,810,001**	· 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

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 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 at the regional, state, county, tribal, and local levels 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

A Regional Director leads a cadre of security professionals located throughout the region. Through a regional office strategically located in Boston,MA, regional personnel manage mission execution through steady state and incident operations, critical infrastructure analysis, and strategic outreach to critical infrastructure partners. Protective Security Advisors (PSAs), Chemical Security Inspectors (CSIs), Cyber Security Advisors (CSAs), Emergency Communications Division Coordinators, and visiting CISA staff all coordinate their critical infrastructure protection missions through the regional offices, and collaborate on regional critical infrastructure efforts, as needed. Regional personnel coordinate training events and exercises for stakeholders; participate in external planning with state, local, tribal, territorial, 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.

CISA
CYBER+INFRASTRUCTURE

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

REGION I

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

- CSIs perform regulatory activities for **high-risk chemical facilities** under the Chemical Facility Anti-Terrorism Standards (CFATS) 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 program 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.

TRAINING AND EXERCISES

- Regional personnel facilitate or deliver **DHS Active Shooter Training/ Workshops, Supply Chain Workshops, Dams Security Workshops,** and others.
- Regional personnel facilitate delivery of DHS Office for Bombing Prevention training courses 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. Courses are provided in-person and virtually.
- 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.
- 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.

ASSESSMENTS

- PSAs conduct **Assist Visits** to provide critical infrastructure facilities with an overview of available DHS services and/or provide a "facility walk-through." PSAs may conduct more detailed security assessments, upon request.
- PSAs conduct assessments using the **Infrastructure Survey Tool** (**IST**) or **Rapid Survey Tool** (**RST**). Both tools help PSAs 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.
- 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. RRAPs address a range of infrastructure resilience issues that could have regionally- and nationally- significant consequences.
- CSAs offer three types of assessments: **Cyber Infrastructure Survey, Cyber Resilience Review,** and **External Dependency Management**, to provide a strategic, all-encompassing assessment of an organization's cyber posture.

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***