



IT Security



Supply Chain



OT Security



Insider Threat



Physical Security



Interoperable Communications

# REGION 3



DEFEND TODAY,  
SECURE TOMORROW

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:

- **Improve** situational awareness of cybersecurity risks and mitigation strategies
- **Support** preparation, response, and recovery efforts for hazards impacting critical infrastructure
- **Safeguard** soft targets and crowded places
- **Conduct** and **integrate** infrastructure assessments, 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:** Philadelphia, Pa.

**Area:** 5 States & District of Columbia; 244 Counties; 7 Tribal Nations

**Size:** 127,324 square miles

**Estimated Population:** 30,724,788

### Key Facts:

- Region 3 includes Pa., Del., Md, W.Va., Va., and D.C.
- Region 3 is home to multiple major metropolitan areas.
- One of the most densely populated regions per square mile.

This region contains varied infrastructure, hosts a plethora of special events, and includes coastal areas.

A Regional Director leads a cadre of security professionals located throughout the region. Through a regional office located in Philadelphia, Pa., 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 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.

## 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 chemical facilities identified as high-risk under the Chemical Facility Anti-Terrorism Standards (CFATS) regulatory program (6 CFR). Facilities identified as high-risk must meet and maintain risk-based performance security standards appropriate to the facilities tier level and the risks they pose. CSIs conduct regulatory inspections and enforcement operations, respond to facilities' compliance assistance requests, and support facility site security plan development. CSIs also engage in program outreach with stakeholders, private industry owners/operators, and federal, state, and local partners to coordinate and communicate the protection of covered facilities with local first responders, identify potential chemicals-of-interest, and share critical information.

## TRAINING 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 facilitate or deliver **Active Shooter Preparedness Training/Workshops, Supply Chain Workshops, Dams Security Workshops**, and others.

Regional personnel facilitate delivery of 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.

## ASSESSMENTS

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.

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. as well as a facility-specific report.

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 significant consequences.

## INCIDENT SUPPORT AND ANALYSIS

Regional personnel:

- provide pre- and post-incident analysis, assessment, and stakeholder communication to support strong decision-making and improved resilience;
- 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;
- collaborate to determine impacts to critical infrastructure and cross-sector impacts within an incident area; and,
- 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 3:**

- Visit the Regional Offices website: <https://www.dhs.gov/cisa/cisa-regional-offices>
- Contact regional staff at [CISARegion3@hq.dhs.gov](mailto:CISARegion3@hq.dhs.gov)