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

CISA REGION 9

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.

Personnel located in CISA's 10 regions work with public and private sector 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** 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: Oakland, California

Location: Four states (Arizona, California, Hawaii, Nevada); three territories (American Samoa, Guam, Commonwealth of the Northern Mariana Islands); 150 tribal nations

Size: 386,056 square miles (which crosses the International Dateline and the Equator)

Population: 51,249,625 (est.)

Key Facts:

- Produces more than half of the country's fruits, nuts, and vegetables.
- Includes three (Honolulu, Los Angeles, Oakland) of the top 10 ports in the U.S., by total container volume.
- Home to numerous Silicon Valley technology companies, including Facebook, Google, Apple and Tesla.

Led by a Regional Director based in Oakland, California, the Region 9 staff provides cybersecurity, physical infrastructure security, chemical security and emergency communications services to critical infrastructure partners throughout the region. This cadre of security professionals manage mission execution through steady state and incident response support operations.

Covering 386,056 square miles and comprised of islands, mountains, deserts, forests, and urban areas, Region 9's geography is varied and extreme. Natural risks impacting the area are equally as diverse. Earthquakes, drought and wildfires in California; volcano eruptions, hurricanes and tsunami in Hawaii and the Pacific Islands; dust storms and tornadoes in Arizona; and snow and ice storms in Nevada all pose significant threats to critical infrastructure and the surrounding communities. Adverse human-caused events, such as cyber and physical security attacks, chemical hazards, and shooting and bombing incidents, also have lasting and dramatic effects. Regardless of the nature or cause of an incident, CISA Region 9 staff is ready to help partners build resilience and readiness to mitigate risk, and to provide response support in the event of an incident. Learn more about some of the crucial services we provide below.

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. Region 9 personnel also 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 cybersecurity assessments using, among others, the following tools: Cyber Infrastructure Survey, Cyber Resilience Review, External Dependency Management Assessment Package.

CHEMICAL SECURITY

Chemical Security Inspectors (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 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.

EMERGENCY COMMUNICATIONS

Emergency Communications Coordinators (ECC) build trusted relationships, enhance collaboration, and stimulate the sharing of best practices and information between all levels of government, critical infrastructure owners and operators, and key non-government organizations.

ECCs build and maintain partnerships between Federal, state, local, tribal, and territorial government stakeholders, as well as the private sector, in an effort to improve the Nation's operable and interoperable emergency communications. ECCs function in outreach, planning, and response roles and coordinate with CISA's Emergency Communication Division to provide states, tribes, territories, and local agencies a wide range of technical assistance, including communication training; exercise development and support; governance development; response and resilience planning; and communication engineering assessments.

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.

TRAINING AND EXERCISES

Regional personnel facilitate or deliver a wide range of webinars and workshops on all 16 critical infrastructure sectors. They also facilitate delivery of Office for Bombing Prevention training courses to prevent, protect against, respond to, and mitigate bombing incidents. Courses are provided in-person and virtually. Additionally, CISA conducts regular cybersecurity training for Industrial Control Systems professionals across all critical infrastructure sectors. This training effort includes regional training events designed for asset owners and operators.

Regional staff coordinate physical and cybersecurity 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. They also participate in and provide support to federal, state, local, and regional exercises organized by other organizations.

CSAs conduct cybersecurity 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.

FEDERAL FACILITY SECURITY

Interagency Security Committee (ISC) Regional Advisors work closely with Federal partners in the region to implement the ISC security standards and best practices for nonmilitary federal facilities. ISC standards and best practices can be used to help federal security professionals understand and determine their Facility Security Level and to implement security policies and mandatory standards regarding physical security countermeasures in and around their facility.

For more information:
Visit the Region 9 website: Region 9 | CISA
Contact regional staff at *CISARegion9@hq.dhs.gov*