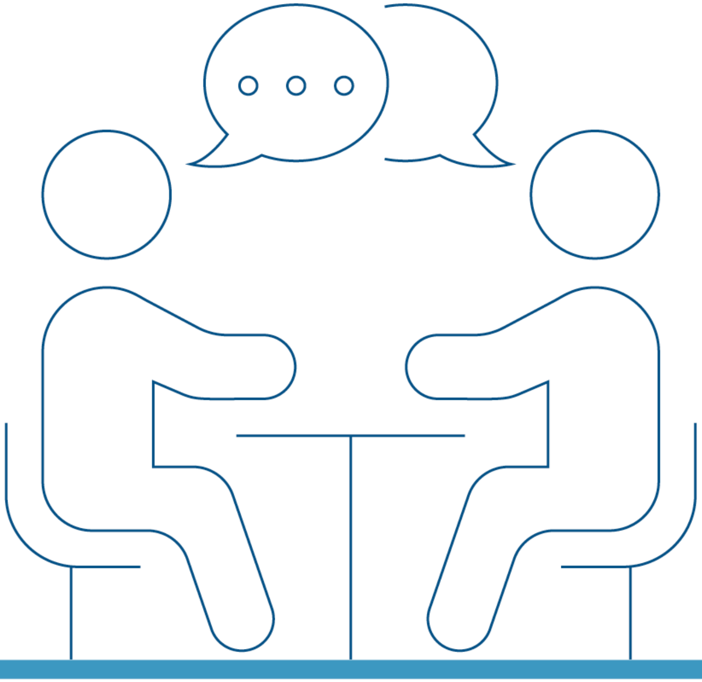
CISA

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

UNITED EFFORTS
CISA AND CRITICAL INFRASTRUCTURE

Stakeholder Engagement



CISA's Stakeholder Engagement Division builds and maintains national and international partnerships and engagements while serving as the hub for the shared stakeholder information that advances unified risk reduction efforts.

HOW CISA IS CARRYING OUT ITS STAKEHOLDER ENGAGEMENT MISSION:

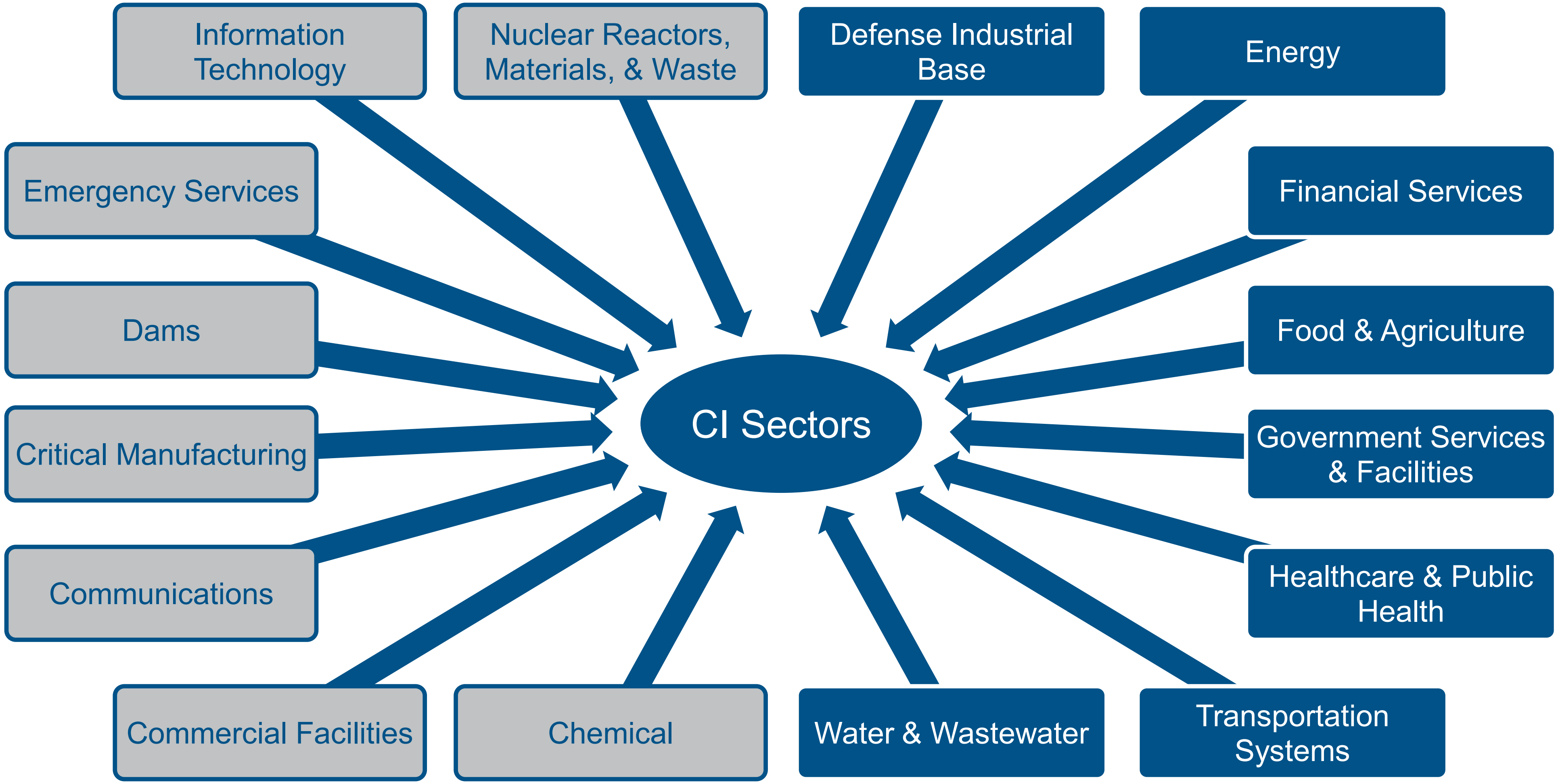
- Plan and Implement Collaboratively Stakeholder Engagements and Partnership Activities to Advance a Unified Mission Delivery
- Use Stakeholder Insights and Feedback to Inform CISA Product Development and Mission Delivery
- Ensure Stakeholders Have Easy Access to CISA Programs, Products, Services, and Information

Sector Risk Management Agencies

The SRMAs:

- Coordinate and collaborate with DHS and other relevant Federal departments and agencies, with critical infrastructure owners and operators, where appropriate with independent regulatory agencies, and with SLTT entities, as appropriate, to implement PPD-21.
- Serve as a day-to-day Federal interface for the dynamic prioritization, collaboration, and coordination of sector-specific activities.
- Carry out incident management responsibilities consistent with statutory authority and other appropriate policies, directives, or regulations.
- Provide, support, or facilitate technical assistance and consultations for that sector to identify vulnerabilities and help mitigate incidents, as appropriate.
- Support the Secretary of Homeland Security's statutory reporting requirements by providing, on an annual basis, sector-specific critical infrastructure information.

Critical Infrastructure



CI Sectors – CISA Managed

Chemical Sector

Several hundred thousand U.S. chemical facilities use, manufacture, store, transport, or deliver potentially dangerous chemicals on which other critical infrastructure sectors rely, along a complex, global supply chain. ChemicalSector@mail.cisa.dhs.gov

Commercial Facilities Sector

Includes a wide range of sites that draw large crowds of people for shopping, business, entertainment, or lodging and operate on the principle of open public access, meaning that the general public can move freely without the deterrent of highly visible security barriers. CommercialFacilitiesSector@mail.cisa.dhs.gov

CI Sectors – CISA Managed

Communications Sector

Provides products and services that support the efficient operation of today's global information-based society. CommunicationsSector@mail.cisa.dhs.gov

Critical Manufacturing Sector

Comprises manufacturing that is crucial to the economic prosperity and continuity of the United States. Processes raw materials and primary metals, produces engines, turbines, and power transmission equipment; produces electrical equipment and components; and manufactures cars, trucks, commercial ships, aircraft, rail cars, and their supporting components. CriticalManufacturingSector@mail.cisa.dhs.gov

CI Sectors – CISA Managed

Dams Sector

Delivers critical water retention and control services in the United States, including hydroelectric power generation, municipal and industrial water supplies, agricultural irrigation, sediment and flood control, river navigation for inland bulk shipping, industrial waste management, and recreation. DamsSector@mail.cisa.dhs.gov

Information Technology Sector

Virtual and distributed functions produce and provide hardware, software, and information technology systems and services, and—in collaboration with the Communications Sector—the Internet. ITSector@mail.cisa.dhs.gov

CI Sectors – CISA Managed

Nuclear Reactors, Materials, and Waste Sector

From the power reactors that provide electricity to millions of Americans, to the medical isotopes used to treat cancer patients, the Nuclear Reactors, Materials, and Waste Sector covers most aspects of America’s civilian nuclear infrastructure. NuclearSector@mail.cisa.dhs.gov

Emergency Services Sector

The Emergency Services Sector (ESS) maintains public safety and security, performs lifesaving operations, protects property and the environment, and assists communities impacted by disasters and provides a wide range of prevention, protection, mitigation, response, and recovery activities. The ESS is geographically distributed across every jurisdiction in the Nation at the federal, state, local, tribal, and territorial levels of government, as well as private-sector resources. EmergencyServicesSector@mail.cisa.dhs.gov

Emergency Services Subsectors

Emergency Management is an essential government service whose purpose is to apply resources and efforts to mitigate, prevent when possible, protect where feasible, and to respond and recover from all threats and hazards that impact the safety and security of the nation.

Emergency Medical Services, commonly known as EMS, is a system that provides pre-hospital, emergency medical care for serious illness or injury and is a system of coordinated response and victim transport.

Emergency Services Subsectors

Fire and Rescue Services respond to natural disasters, such as earthquakes, floods, tornadoes, and hurricanes, as well as to man-made catastrophes, such as hazmat spills, arson, and terrorism, and perform fire suppression, fire prevention, hazardous materials control, emergency rescue, building code enforcement, and public fire safety education.

Law Enforcement is responsible for enforcing laws, maintaining public order, and managing public safety. The primary duties of law enforcement include the investigation, apprehension, and detention of individuals suspected of criminal offenses.

Emergency Services Subsectors

Public Works provides and sustains structures and services essential to the welfare and acceptable quality of life for the public, including providing water, power, waste disposal, and transportation.

CI Sectors – Non-CISA Managed

The **Defense Industrial Base Sector** is the worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet U.S. military requirements. Department of Defense

The **Energy Sector** protects a multifaceted web of electricity, oil, and natural gas resources and assets to maintain steady energy supplies and ensure the overall health and wellness of the nation. Department of Energy

CI Sectors – Non-CISA Managed

The **Financial Services Sector** includes thousands of depository institutions, providers of investment products, insurance companies, other credit and financing organizations, and the providers of the critical financial utilities and services that support these functions. Department of the Treasury

The **Food and Agriculture Sector** is almost entirely privately owned and composed of an estimated 1.9 million farms, over 700,000 restaurants, and more than 220,000 registered facilities in food manufacturing, processing, and storage. Department of Agriculture

CI Sectors – Non-CISA Managed

The **Government Services and Facilities Sector** includes a wide variety of buildings, located in the United States and overseas, that are owned or leased by federal, state, local, and tribal governments. General Services Administration

The **Healthcare and Public Health Sector** provides goods and services integral to maintaining local, national, and global health security. Department of Health and Human Services

CI Sectors – Non-CISA Managed

The **Transportation Systems Sector** quickly, safely, and securely moves people and goods through the country and overseas. Department of Homeland Security and Department of Transportation

The **Water and Wastewater Sector** ensures a reliable supply of clean drinking water and effective wastewater treatment. Environmental Protection Agency

TLP:WHITE

CISA Mission

The Cybersecurity and Infrastructure Security Agency's (CISA) mission is to ensure the **security and resiliency** of our critical infrastructure.

Serve as the **national coordinator for critical infrastructure security and resilience**, leading efforts to understand, manage and reduce cyber and physical risk:

- Maintain public-private **partnerships** dedicated to sharing risk information;
- Work by, with, and through **regional experts** responsible for on-site vulnerability assessments and partnering with owner/operators to mitigate risk;
- Participate in national and international level dialogues to learn more about threats and **share lessons learned**.

CISA.GOV

CISA STRATEGIC PLAN 2023–2025

GOAL 1

CYBER DEFENSE:
Spearhead the National Effort to Ensure Defense and Resilience of Cyberspace

GOAL 2

RISK REDUCTION & RESILIENCE:
Reduce Risks to, and Strengthen Resilience of, America’s Critical Infrastructure

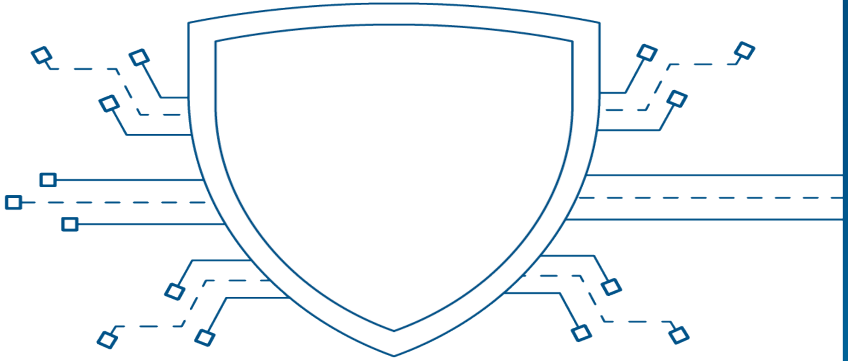
GOAL 3

OPERATIONAL COLLABORATION:
Strengthen Whole-of-Nation Operational Collaboration and Information Sharing

GOAL 4

AGENCY UNIFICATION:
Unify as One CISA Through Integrated Functions, Capabilities, and Workforce

Cybersecurity Mission



CISA's Cybersecurity Division leads the national effort to reduce the prevalence and impact of cyber incidents by providing services, guidance, and capabilities that address immediate risks and advance toward a secure cyber ecosystem.

HOW CISA IS CARRYING OUT ITS CYBERSECURITY MISSION:

- Catalyze Persistent Collaboration Across Government and the Private Sector
- Expand Operational Visibility into Threats and Vulnerabilities
- Drive Prioritization and Measure Adoption of the Most Effective Security Measures
- Serve as the Operational Lead for Federal Civilian Cybersecurity
- Advance a Technology Product Ecosystem that is Secure by Design

Jana Spring & David Lee
April 17, 2025

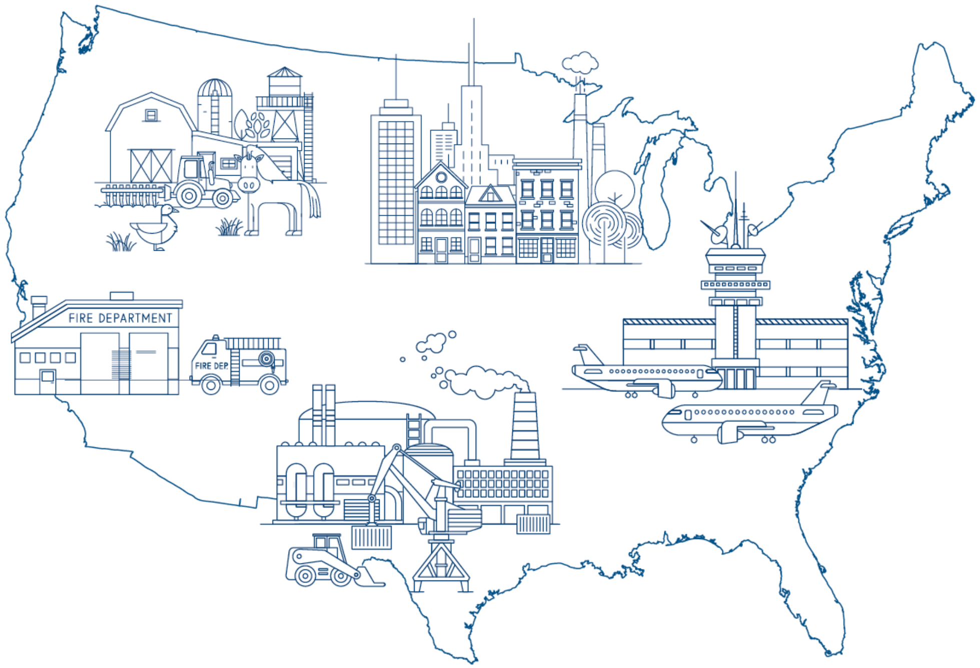
Infrastructure Security Mission

CISA's Infrastructure Security Division leads the coordinated effort to reduce risks posed to our critical infrastructure, whether from man-made or natural causes.

HOW CISA IS CARRYING OUT ITS INFRASTRUCTURE SECURITY MISSION:

- Combat Terrorism and Targeted Violence
- Conduct Exercise and Training Programs
- Enhance School Safety with our School Safety Task Force
- Assess and Analyze Critical Infrastructure
- Identify and Prioritize Critical Infrastructure
- Strengthen Chemical Security with ChemLock

Integrated Operations

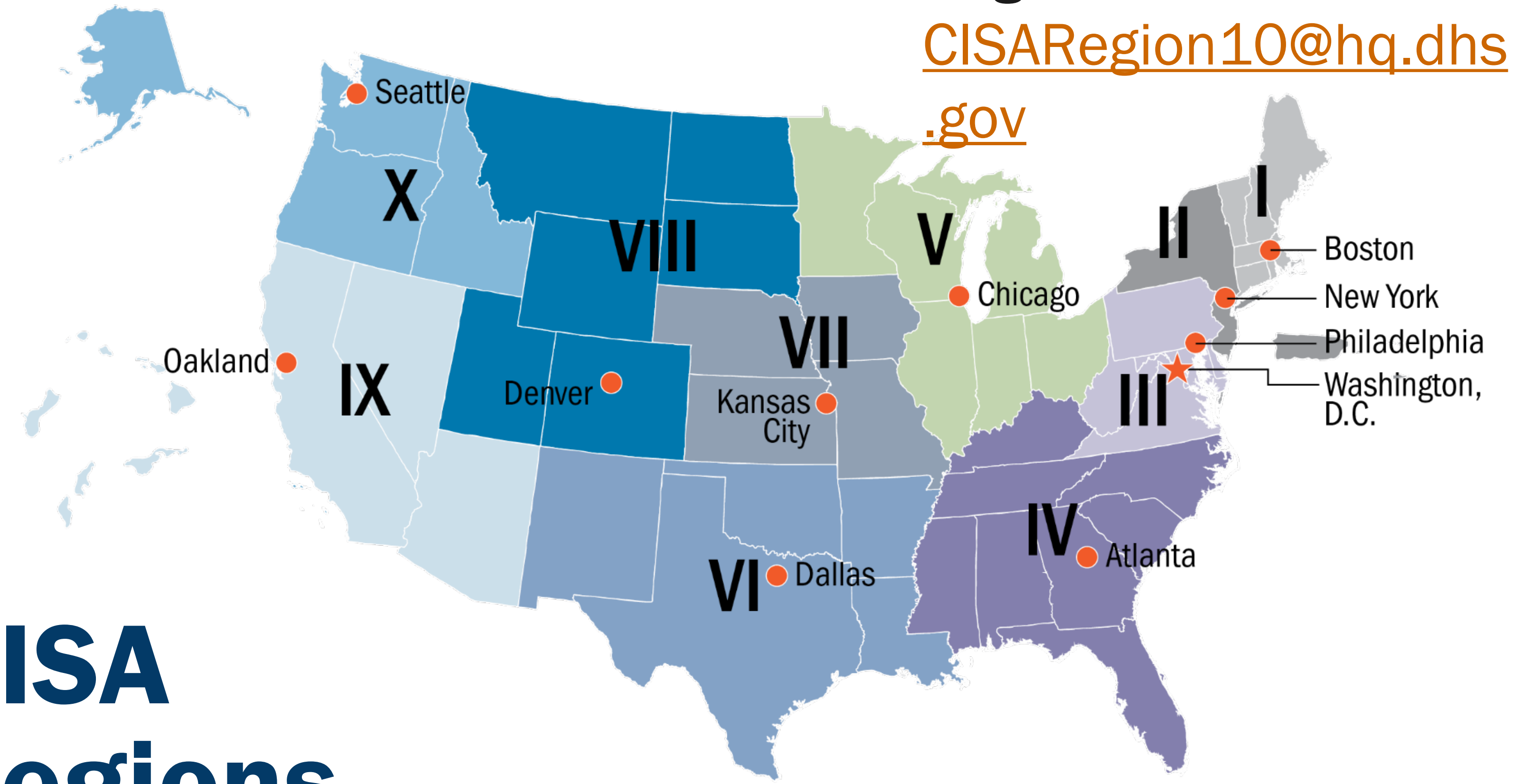


HOW CISA IS CARRYING OUT ITS INTEGRATED OPERATIONS MISSION:

- Provide Operational Visibility to Understand, Manage, and Reduce Risk to the Nation
- Offer a Unified Regional Approach to Sharing Information and Delivering CISA Services

CISA's Integrated Operations Division enhances the resilience of our nation's critical infrastructure by taking an integrated approach to delivering services and sharing information. By meeting our stakeholders where they are, we help critical infrastructure owners and operators mitigate risk.

Region 10:
CISARegion10@hq.dhs.gov



CISA Regions

Information Exchange

Incident Response

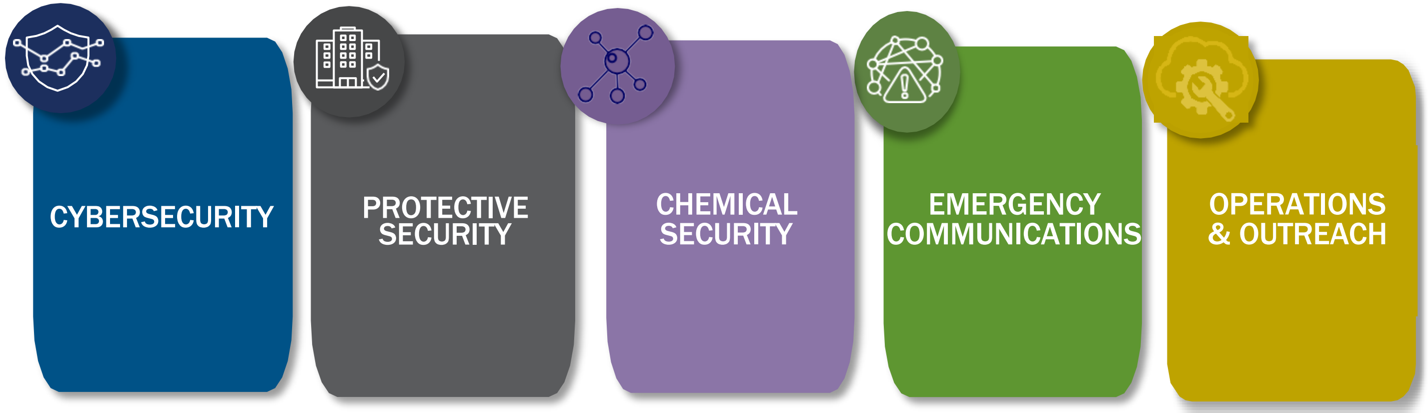
Risk & Cybersecurity Assessments

Exercises & Training

CISA Region 10 Overview

TLP:WHITE

- Expertise and a history of success providing services to Unclassified Information and Operational Technology (IT and OT) environments
- Proactive services to government and critical infrastructure clients to assess and improve cybersecurity posture, understand risk, and identify operational strengths and weaknesses



CYBERSECURITY

PROTECTIVE SECURITY

CHEMICAL SECURITY

EMERGENCY COMMUNICATIONS

OPERATIONS & OUTREACH

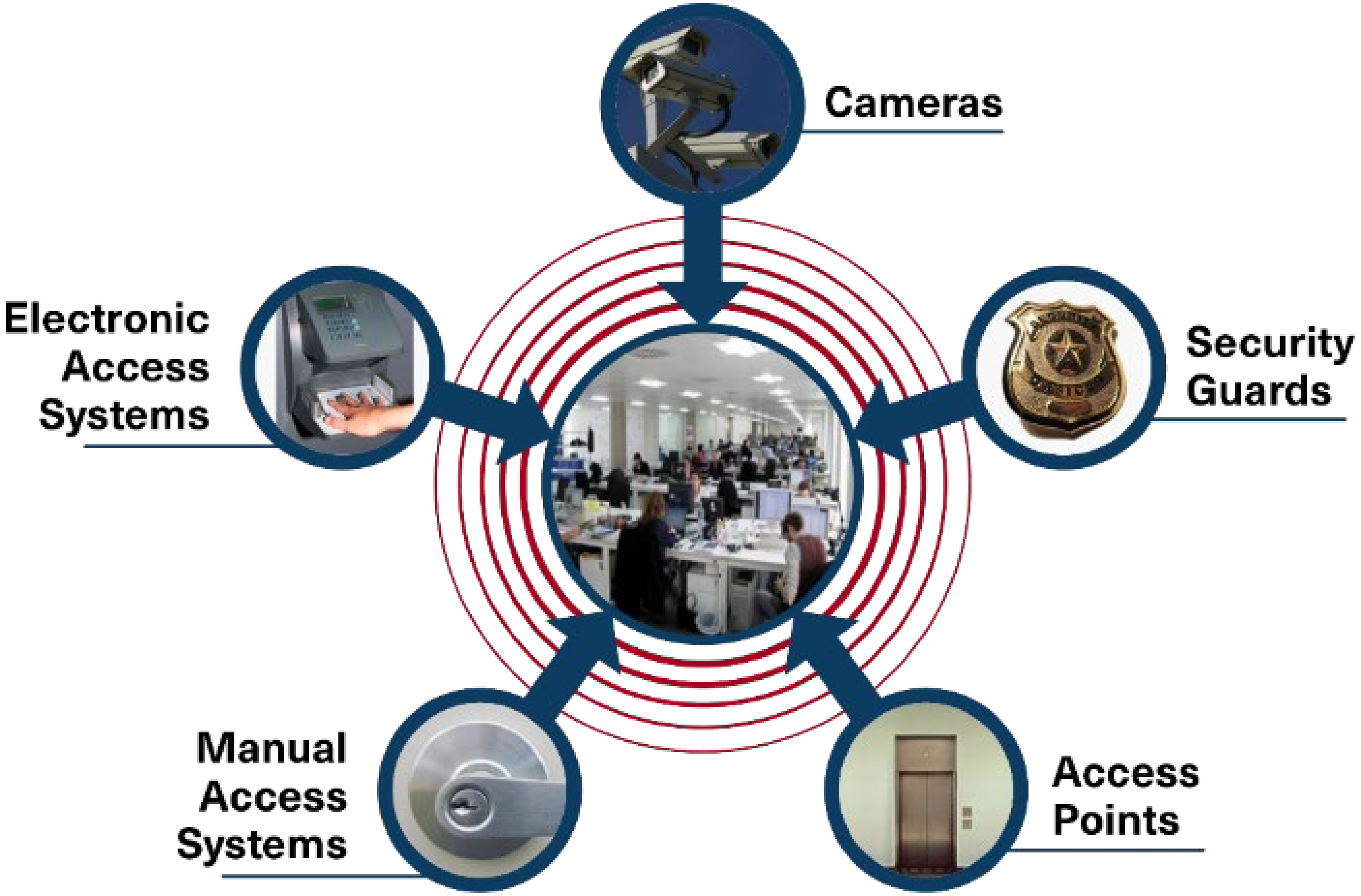
Services are provided at “no cost” to our customers

Our “payment” is authorization to use anonymized, non attributable, data to enhance national situation awareness and enable our stakeholders to make data driven decisions

RESOURCES FOR CRITICAL INFRASTRUCTURE RESILIENCE

Jana Spring & David Lee
April 17, 2025

Protective Security Measures



Cameras

Security Guards

Access Points

Manual Access Systems

Electronic Access Systems

Jana Spring & David Lee
April 17, 2025

Protection and Mitigation Measures

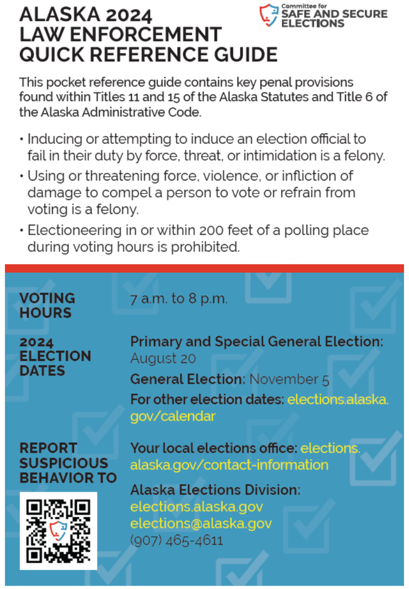
Protection

- Utilize early warning and mass notification systems
- Utilize barrier systems to deny access to critical areas and create safe havens
- Do you have a non-ambulatory population that cannot evacuate?
- Multiple evacuation routes

Additional Mitigation Considerations

Mitigation

- Weapons Policy
- Signage / Cameras in public lobbies
- Additional Cameras
- Alternate Entrances
- CSSE Law Enforcement QRG



ALASKA 2024
LAW ENFORCEMENT
QUICK REFERENCE GUIDE

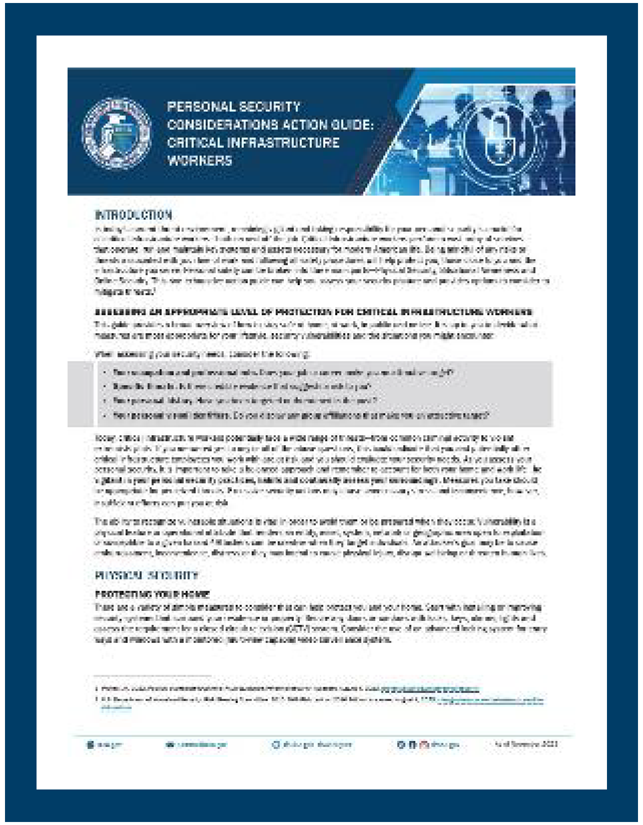
Committee for SAFE AND SECURE ELECTIONS

This pocket reference guide contains key penal provisions found within Titles 11 and 15 of the Alaska Statutes and Title 6 of the Alaska Administrative Code.

- Inducing or attempting to induce an election official to fail in their duty by force, threat, or intimidation is a felony.
- Using or threatening force, violence, or infliction of damage to compel a person to vote or refrain from voting is a felony.
- Electioneering in or within 200 feet of a polling place during voting hours is prohibited.

VOTING HOURS	7 a.m. to 8 p.m.
2024 ELECTION DATES	Primary and Special General Election: August 20 General Election: November 5 For other election dates: elections.alaska.gov/calendar
REPORT SUSPICIOUS BEHAVIOR TO	Your local elections office: elections.alaska.gov/contact-information Alaska Elections Division: elections.alaska.gov elections@alaska.gov (907) 465-4611

Personal Security Considerations Action Guide: Critical Infrastructure Workers



PERSONAL SECURITY CONSIDERATIONS ACTION GUIDE: CRITICAL INFRASTRUCTURE WORKERS

INTRODUCTION

[illegible]

ASSESSING AN APPROPRIATE LEVEL OF PROTECTION FOR CRITICAL INFRASTRUCTURE WORKERS

[illegible]

PHYSICAL SECURITY

PROTECTING YOUR HOME

[illegible]

- Enhance awareness of security postures for critical infrastructure workers at home, at work, in public, and online.
- Equip critical infrastructure workers with information, best practices, and tips to support their personal safety and security.

Audience

- Critical infrastructure workers

Overview

The Personal Security Considerations Action Guide: Critical Infrastructure Workers helps critical infrastructure workers asses their security posture and provide threat mitigation options.

PHYSICAL SECURITY

Assessing and taking proactive measures to enhance your person, home or work area.

SITUATIONAL AWARENESS

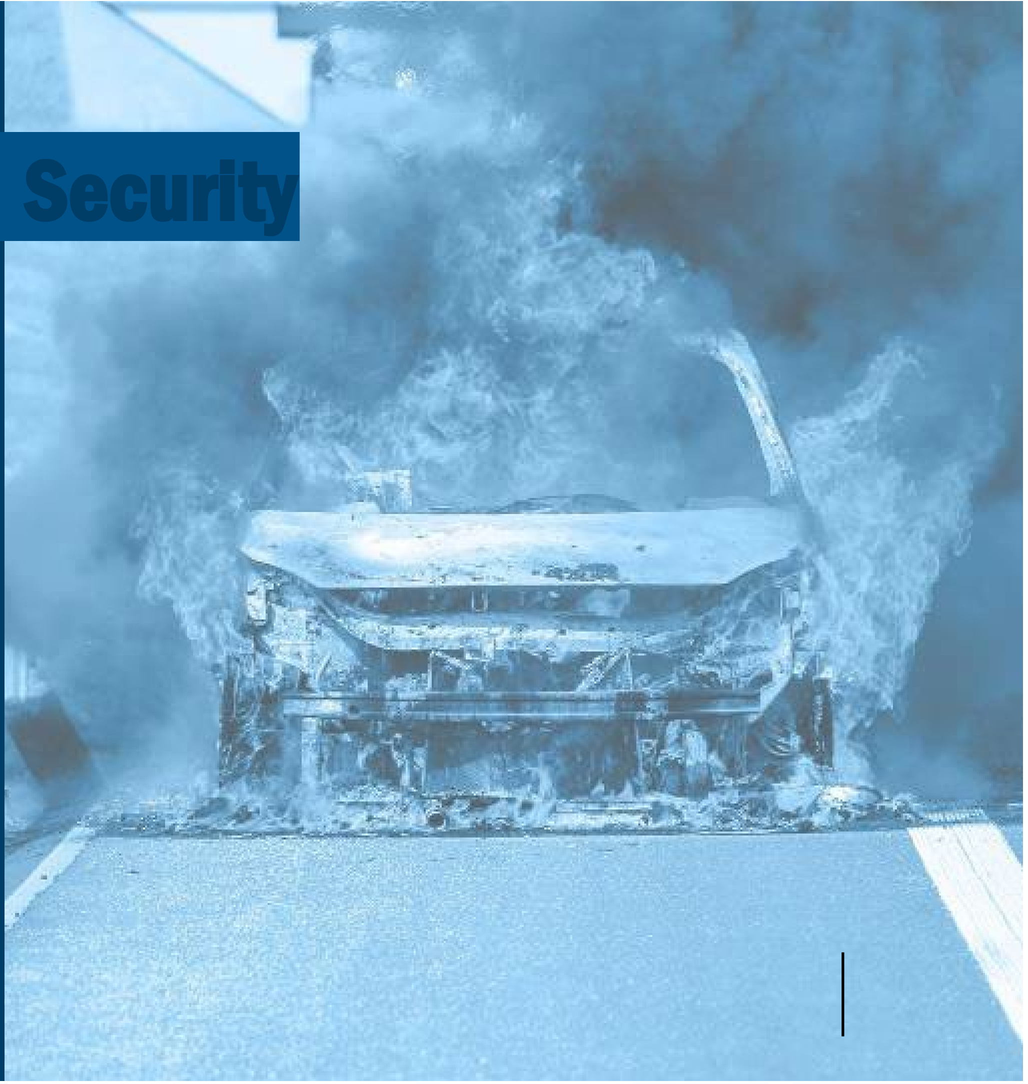
Adequately assessing your surroundings, taking everything into account and adjusting your behavior to reduce the risk of injury to you, your family or your coworkers.

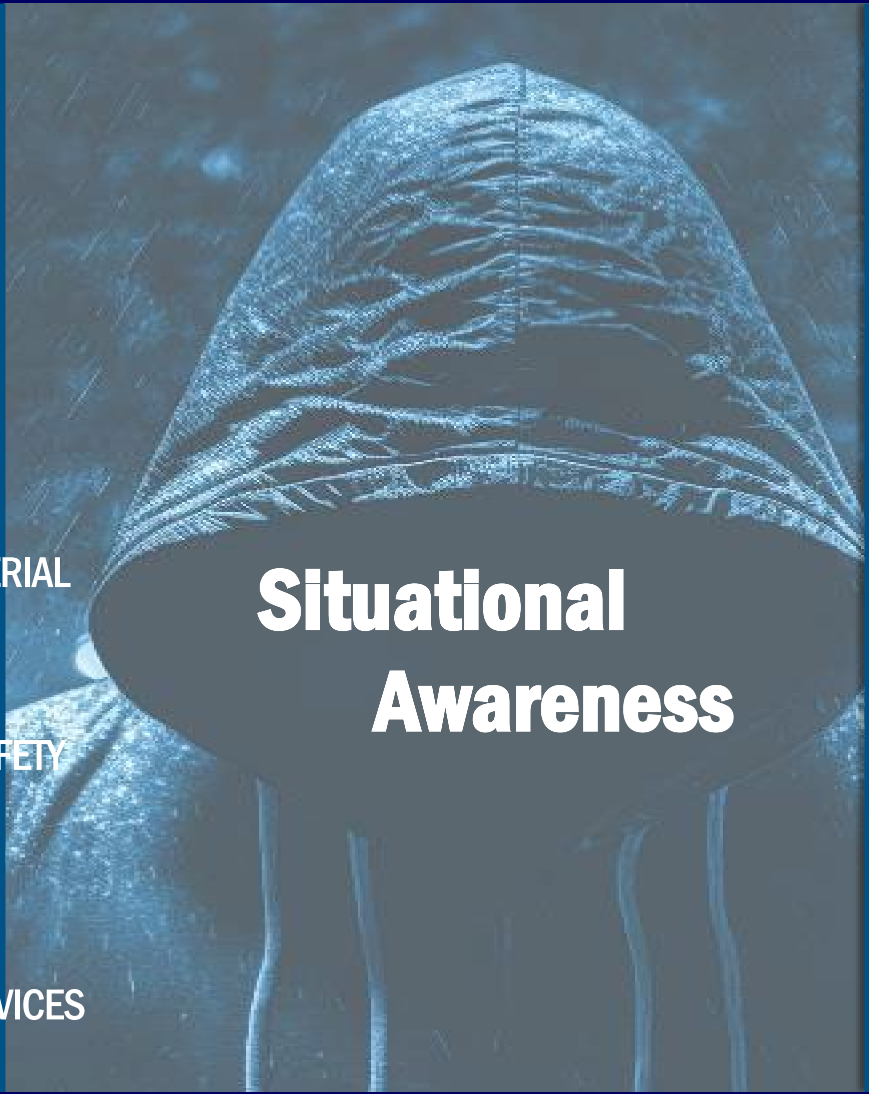
ONLINE SECURITY

Involves the security landscape surrounding online spaces such as email and social media platforms.

Physical Security

- Protecting Your Home
- Firearm Attacks
- Fire as a Weapon
- Improvised Explosive Devices (IED)
- Protests and Demonstrations



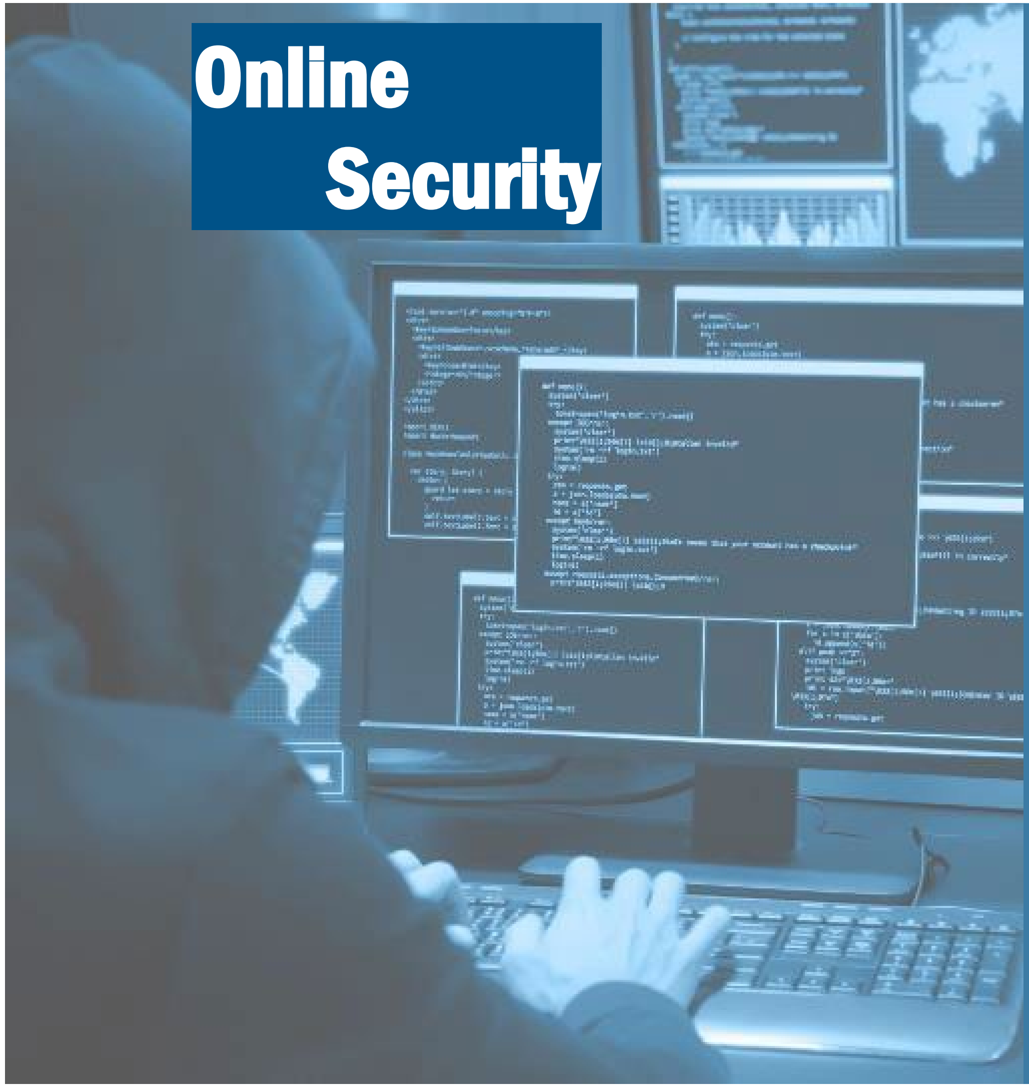


Situational Awareness

- Visitors
- Sensitive Material
- Pedestrian Safety
- Personal Protection Devices

- Recognizing and Reporting Suspicious Activity
- Confrontations
- Motor Vehicles and Travel
- Anonymous Phone Calls and Threats

Online Security



- Secure Downloads
- Use of Electronic Devices
- Social Media
- Doxing
- Email Security

Additional CISA Resources

Active Shooter Preparedness

Products, tools, and resources to help you prepare for, respond to, and recover from an active shooter incident

cisa.gov/topics/physical-security/active-shooter-preparedness

Pathway to Violence

Includes products and resources that provide information regarding the behavior indicators assailants often demonstrate before a violent act

cisa.gov/resources-tools/resources/pathway-violence

CISA Protective Security Advisors

Security experts who provide on-site vulnerability assessments, can help with security plans and local resources

cisa.gov/resources-tools/programs/protective-security-advisor-psa-program

Enhancing Security of Public Gatherings

Provides a compendium of resources for securing public gatherings to help organizations mitigate potential risks in today's dynamic and rapidly evolving threat environment

cisa.gov/topics/physical-security/securing-public-gatherings www.CISA.gov/Emergency-Services-Sector

EmergencyServicesSector@mail.cisa.dhs.gov

For more information:
cisa.gov

Questions?

For more information:

www.cisa.gov
www.dhs.gov/cp3

David Lee
Industrial Security Specialist
Cybersecurity and Infrastructure Security Agency
Stakeholder Engagement Division
Cell: **202-779-2384| Email:** David.Lee@mail.cisa.dhs.gov

Jana Spring
Protective Security Advisor, Region 10 (Western WA)
Cybersecurity and Infrastructure Security Agency
Integrated Operations Division
Cell: **360 259 3455** | Email: jana.spring@cisa.dhs.gov

Subscribe today to
receive new information on
Active Assailant Security

CYBERSECURITY & INFRASTRUCTURE

CISA

SECURITY AGENCY