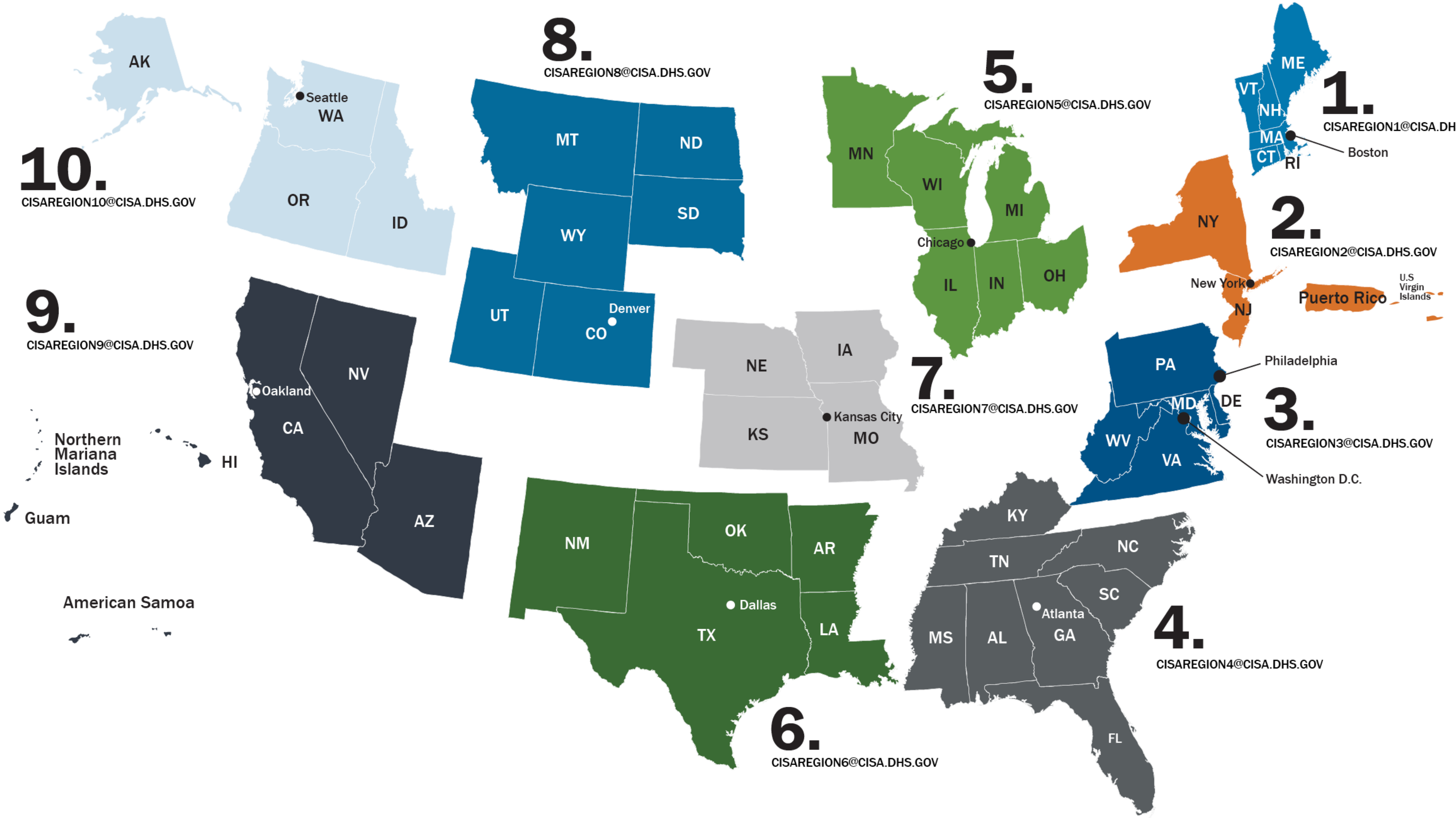
U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

CISA Regions

1	Boston, MA
2	New York, NY
3	Philadelphia, PA
4	Atlanta, GA
5	Chicago, IL
6	Dallas, TX
7	Kansas City, MO
8	Denver, CO
9	Oakland, CA
10	Seattle, WA



Security Advisor Programs

Security Advisors are field-based critical infrastructure security specialists who link State, local, tribal, territorial (SLTT) & private sector stakeholders with infrastructure protection resources

- **Assess:** Evaluate critical infrastructure risk.
- **Promote:** Encourage best practices and risk mitigation strategies.
- **Build Capacity:** Initiate, develop capacity, and support communities-of-interest and working groups.
- **Educate:** Inform and raise awareness.
- **Listen:** Collect stakeholder concerns & needs.
- **Coordinate:** Bring together incident support and lessons learned.

Protective Security Advisors (PSA): Security, Emergency Preparedness, and Business Continuity Programs

Cybersecurity Advisors (CSA): Cybersecurity for Information Technology & Operational Technology networks

Assist Visits/Cyber Protective Visits

Assist Visits/Cyber Protective Visits are the cornerstone of voluntary outreach.

- Establish and enhances CISA's relationship with SLTT governments or critical infrastructure owners and operators;
- Informs of the importance of their facilities and reinforce the need for continued vigilance;
- Explains how their facility or service fits into its specific critical infrastructure sector;
- Provides an overview of the CISA resources available to the organization to enhance security and resilience.

Visits are often followed by the delivery of other CISA services

Protective Security Advisors

Protective Security Advisors (PSAs):

- Plan, coordinate, and conduct security and resiliency surveys and assessments
- Plan and conduct outreach activities
- Support National Special Security Events (NSSEs) and Special Event Activity Rating (SEAR) events
- Provide vital link for information sharing during steady state and incident response
- Coordinate and support risk mitigation training

PSA Assessments

Organizational Maturity Around Security/Resiliency

Security Assessment at First Entry (SAFE)

- Programs Reviewed
  - Security
  - Emergency Preparedness
  - Business Continuity
- Time Requirement = Site Dependent; Tour of facility(s) followed by conference room meeting
- Written report provided

Infrastructure Survey Tool (IST)

- Programs Reviewed
  - Security
  - Emergency Preparedness
  - Business Continuity
  - Dependencies/Interdependencies
  - Information Technology
- Time Requirement = Typically two full days
- Written report provided

Security Assessment at First Entry

- The Security Assessment at First Entry (SAFE) is designed to assess the current security posture and identify options for facility owners and operators to mitigate relevant threats

- The SAFE is suited for all facilities, including smaller ones such as rural county fairgrounds, houses of worship with only weekend services and few members, and small health clinics

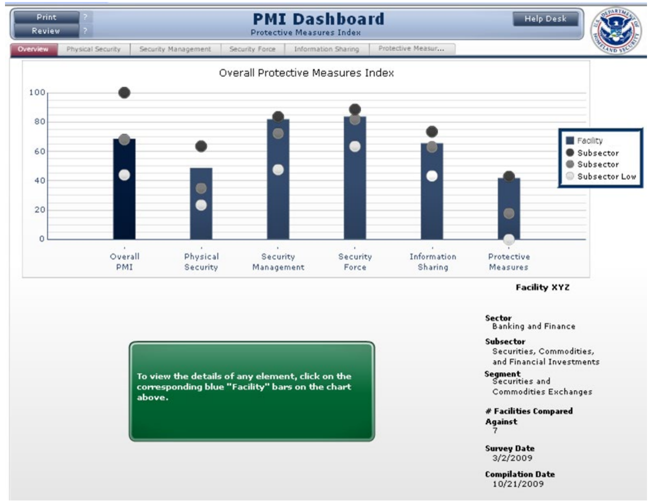
Infrastructure Survey Tool

- The Infrastructure Survey Tool (IST) is a web-based vulnerability survey tool that applies weighted scores to identify infrastructure vulnerabilities and trends across sectors

- Facilitates the consistent collection of security information
  - Criticality/Significant Assets
  - Physical Security
  - Security Management
  - Information Sharing
  - Protective Measures
  - Dependencies

- Generates the Protective Measures Index and

  Resilience Measurement Index



Facility XYZ

To view the details of any element, click on the corresponding blue "Facility" bars on the chart above.

Sector
Banking and Finance

Subsector
Securities, Commodities, and Financial Investments

Segment
Securities and Commodities Exchanges

# Facilities Compared Against
7

Survey Date
3/2/2009

Compilation Date
10/21/2009

Cybersecurity Advisors

Cybersecurity Advisors (CSAs):

- Advise FSLTT and private sector partners on risk levels, security posture, & cost-benefit analysis of information security programs & processes
- Review risk management programs by using evaluation results to create or enhance the effectiveness of the partner's information sharing
- Reduce risks to the nation's critical cyber infrastructure by delivering key mitigation capabilities
- Promote collaborative efforts to reduce risks and threats to critical information, enterprise, communications, and control systems
- Plan and conduct outreach activities relating to cybersecurity initiatives
- Build regional and local cybersecurity coalitions to promote information sharing

Cyber Services - Initial

Step One

Cyber Protective Visit (CPV):

- Initial visit with a Cyber Security Advisor (CSA) to gauge interest in CISA services, understand the organization’s needs, and develop the foundation for further engagements and offerings.

Step Two

Cyber Hygiene Vulnerability Scanning (CyHy):

- Maintain enterprise awareness of your internet-accessible systems
- Provide insight into how systems and infrastructure appear to potential attackers
- Drive proactive mitigation of vulnerabilities and reduce risk

Step Three

Cyber Security Evaluation Tool (CSET):

- The CSET provides a systematic, disciplined, and repeatable method for assessing infrastructure; compare multiple assessments to establish a baseline and determine trends; controls priority list.

Cyber Hygiene Services - Intermediate

Continuous Phishing Campaign Assessment (ConPCA):

Services provided by invite only

- **Objectives**
- Reduce risk to malicious phishing email attempts by testing and informing users
- Understand how users are enticed to click on links and report suspicious activity
- Properly emulate malicious phishing activity to provide a quality learning experience

Web Application Scanning

Services provided by invite only

- **Objectives**
- Maintain enterprise awareness of your publicly accessible web-based assets
- Provide insight into how systems and infrastructure appear to potential attackers
- Drive proactive mitigation of vulnerabilities to help reduce overall risk

Remote Penetration Testing (RPT)

Services provided by invite only

- **Objectives**
- Conduct assessments to identify vulnerabilities and work with customers to eliminate exploitable pathways.
- Simulate the tactics and techniques of real-world threats and malicious adversaries.
- Test centralized data repositories and externally accessible assets/resources.
- Avoid causing disruption to the customer's mission, operation, and network infrastructure.

Cyber Hygiene Services - Advanced

Risk and Vulnerability Assessment (RVA)

Services provided by invite only

- **Objectives**
- Identify weaknesses through network, system, and application penetration testing
- Test stakeholders using a standard, repeatable methodology to deliver actionable findings and recommendations
- Analyze collected data to identify security trends across all RVA stakeholder environments

Validated Architectural Design and Review (VADR)

Services provided by invite only

- **Objectives**
- Analyze systems based on standards, guidelines, and best practices.
- Ensure effective defense-in-depth strategies.
- Provide findings and practical mitigations for improving operational maturity and enhancing cybersecurity posture

Critical Product Evaluation (CPE)

Services provided by invite only

- **Objectives**
- Enumerate the vulnerabilities associated with the product's in-scope software, firmware, and hardware.
- Attempt exploitation of vulnerabilities that pose the greatest risk, using known exploits or new code/techniques.
- Assist in developing remediation or mitigation strategies.

CSA Assessments

Operational

Cyber Infrastructure Survey (CIS)

- Domains
  - Cybersecurity Management
  - Cybersecurity Forces
  - Cybersecurity Controls
  - Incident Response
  - Dependencies
- Time Requirement = 2 to 4-hour
- Access to interactive dashboard

Tactical

External Dependencies Management Assessment (EDM)

- Domains
  - Relationship formation
  - Relationship management and governance
  - Service protection and sustainment
- Time Requirement = 2 to 4-hour
- Written report provided.

Strategic

Cyber Resiliency Review (CRR)

- Domains
  - Asset Management
  - Controls Management
  - Configuration and Change Management
  - Vulnerability Management
  - **Incident Management**
  - Service Continuity Management
  - Risk Management
  - **External Dependency Management**
  - Training and Awareness
  - Situational Awareness
- Time Requirement = 6 to 8-hour
- Written report provided

CSA Assessments

Incident Management Review (IMR):

- Domains
  - Event Detection and Handling
  - Incident Declaration, Handling, and Response
  - Post-Incident Analysis and Testing
  - Integration of Organizational Capabilities
  - Protection and Sustainment of the Incident Management Function
  - Preparation for Incident Response
- Time Requirement = 2 to 4-hour
- Written report provided.

Cyber Resiliency Essentials (CRE):

- Domains
  - Identify Services and Assets
  - Control Access to Assets
  - Protect Data and Manage Recovery Capabilities
  - Protect and Monitor the Network
  - Prevent and Monitor Exposure to Malware
  - Manage Changes to Technology
  - Identify and Manage Vulnerabilities
  - Plan for Incident Management
  - Identify and Manage Risks
  - Manage External Dependency Risk
  - Perform Security Awareness and Training Activities
- Time Requirement = 2 to 4-hour
- Written report provided.

Cyber Performance Goals (CPGs):

- A set of high-impact security actions for critical infrastructure organizations that address both IT and OT/ICS considerations.
- Mapped to the relevant NIST Cybersecurity Framework subcategories, as well as other frameworks (e.g., IEC 62443).
- Domains
  - Account Security
  - Device Security
  - Data Security
  - Governance and Training,
  - Vulnerability Management,
  - Supply Chain/Third Party,
  - Response and Recovery
  - Other (network segmentation, email, etc,)

Outreach & Support

- **Drills & Exercises**
- **Special Event Security Planning**
- **Products:** Protective Measures, Resource Guides, Geographical Information System support, Infrastructure Visualization Platform (IVP)
- **Campaigns:** Operation Flashpoint, Elections Security, Securing Public Gatherings, School Security, Shields Up, etc.
- **Incident Support**

Training

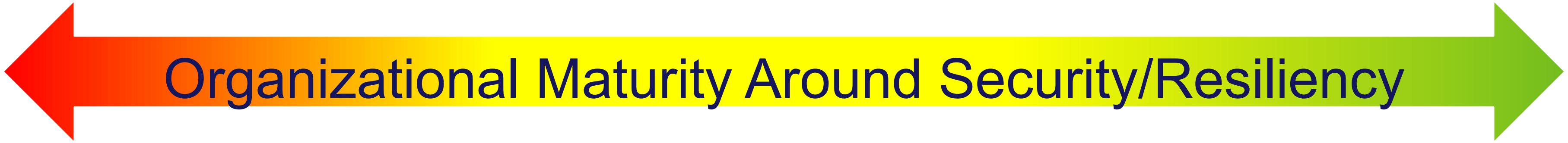
CISA offers a variety of training topics through various mediums:

- Independent Study Courses
- Videos
- Virtual Instructor-Led Courses
- Webinars
- Virtual and On-Site Presentations

Training and Presentations

- CISA 101
- Active Shooter
- Bombing Threat Management
- Bombing Prevention
- Insider Threat
- Cybersecurity Awareness
- Elections Security
- Targeted Violence
- De-Escalation Training for CI
- Securing Public Gatherings
- Hometown Security
- School Security
- Security of Soft Targets and Crowded Places
- See Something, Say Something
- Counter Unmanned Aircraft Systems
- Power of Hello
- Workplace Security
- Cyber Incident Response

Exercises



Organizational Maturity Around Security/Resiliency

Discussion-based Exercises

Seminar

Workshop

Tabletop

Operations-based Exercises

Drill

Functional

Full-Scale

Examples

- Natural Hazards
- Active Shooter
- Complex Coordinated Terrorist Attack
- Vehicle Ramming
- Improvised Explosive Device (IED)

- Phishing
- Ransomware
- Loss of Personally Identifiable Information (PII)
- Industrial Control Systems Compromise

Information Sharing

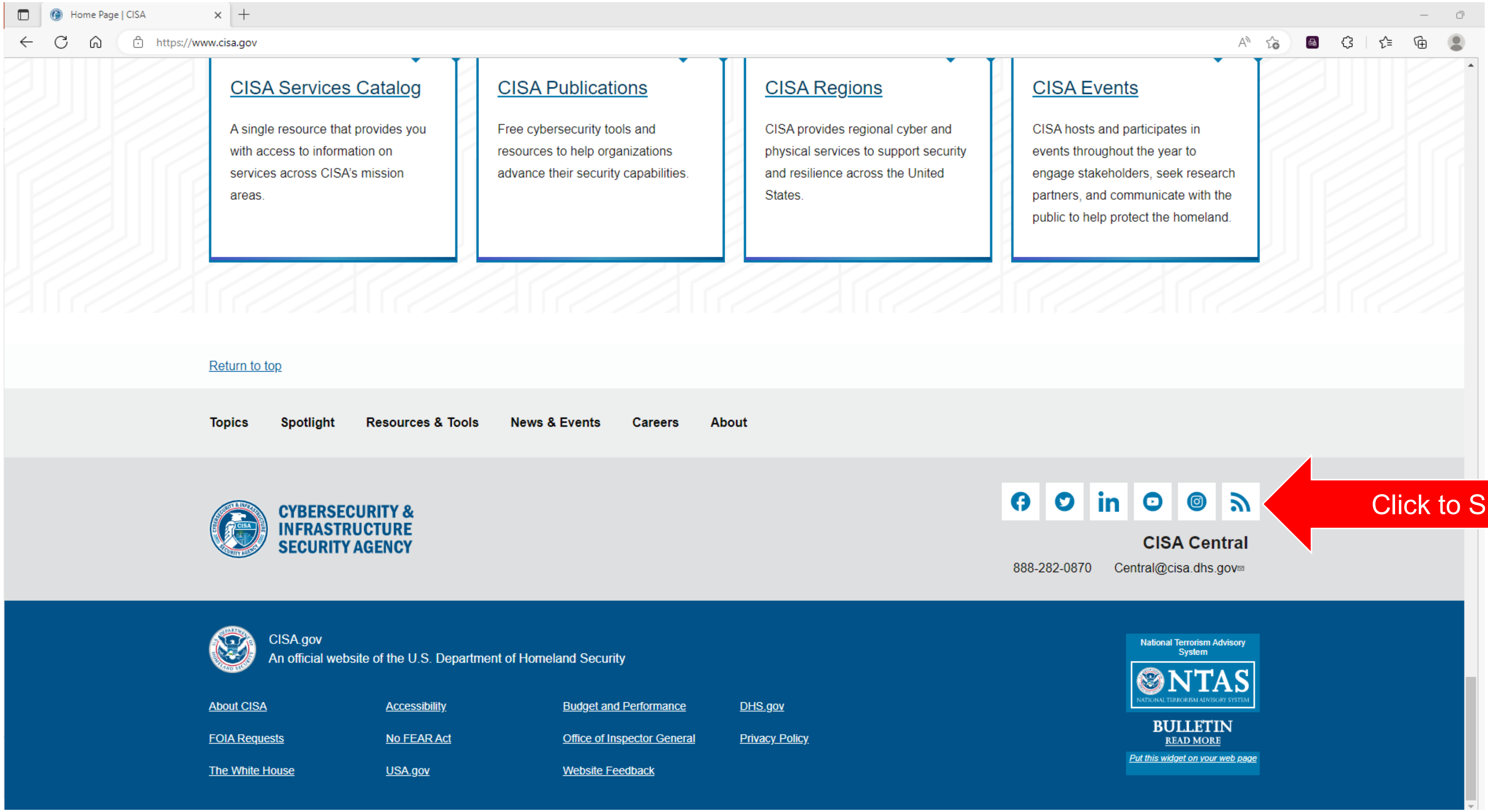
Intelligence and information sharing is essential to the protection of critical infrastructure – to enable informed decisions and timely actions:

- CISA.gov
- National Cyber Awareness System
- Homeland Security Information Network (HSIN)
- TRIPwire
- Information Sharing and Analysis Centers (ISACs)
- Information Sharing and Analysis Organizations (ISAOs)
- Fusion Centers
- Automated Indicator Sharing

Information Sharing & Analysis Centers (ISACs)

- American Chemistry Council
- Automotive ISAC
- Aviation ISAC
- Communications ISAC
- Downstream Natural Gas ISAC
- Elections Infrastructure ISAC
- Electricity ISAC
- Emergency Management & Response ISAC
- Financial Services ISAC
- Healthcare Ready
- Health ISAC
- Information Technology ISAC
- Maritime Transportation System ISAC
- Media & Entertainment ISAC
- Multi-State ISAC
- National Defense ISAC
- Oil & Natural Gas ISAC
- Real Estate ISAC
- Research & Education Networks ISAC
- Retail & Hospitality ISAC
- Small Broadband ISAC
- Space ISAC
- Surface Transportation, Public Transportation & Over-the-Road Bus ISACS
- Water ISAC

CISA.GOV



CISA Services Catalog

A single resource that provides you with access to information on services across CISA's mission areas.

CISA Publications

Free cybersecurity tools and resources to help organizations advance their security capabilities.

CISA Regions

CISA provides regional cyber and physical services to support security and resilience across the United States.

CISA Events

CISA hosts and participates in events throughout the year to engage stakeholders, seek research partners, and communicate with the public to help protect the homeland.

Return to top

CISA Central

888-282-0870 Central@cisa.dhs.gov

CISA.gov
An official website of the U.S. Department of Homeland Security

Click to Subscribe