U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

DEFEND TODAY,
SECURE TOMORROW

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Our Work

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

PARTNERSHIP DEVELOPMENT

INFORMATION AND DATA SHARING

CAPACITY BUILDING

INCIDENT MANAGEMENT & RESPONSE

RISK ASSESSMENT AND ANALYSIS

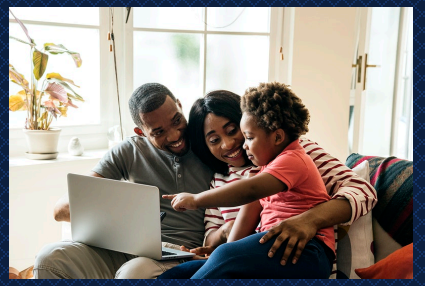
NETWORK DEFENSE

EMERGENCY COMMUNICATIONS

Cybersecurity Awareness Month 2021
CISA Cyber Summit 2021
Schedules

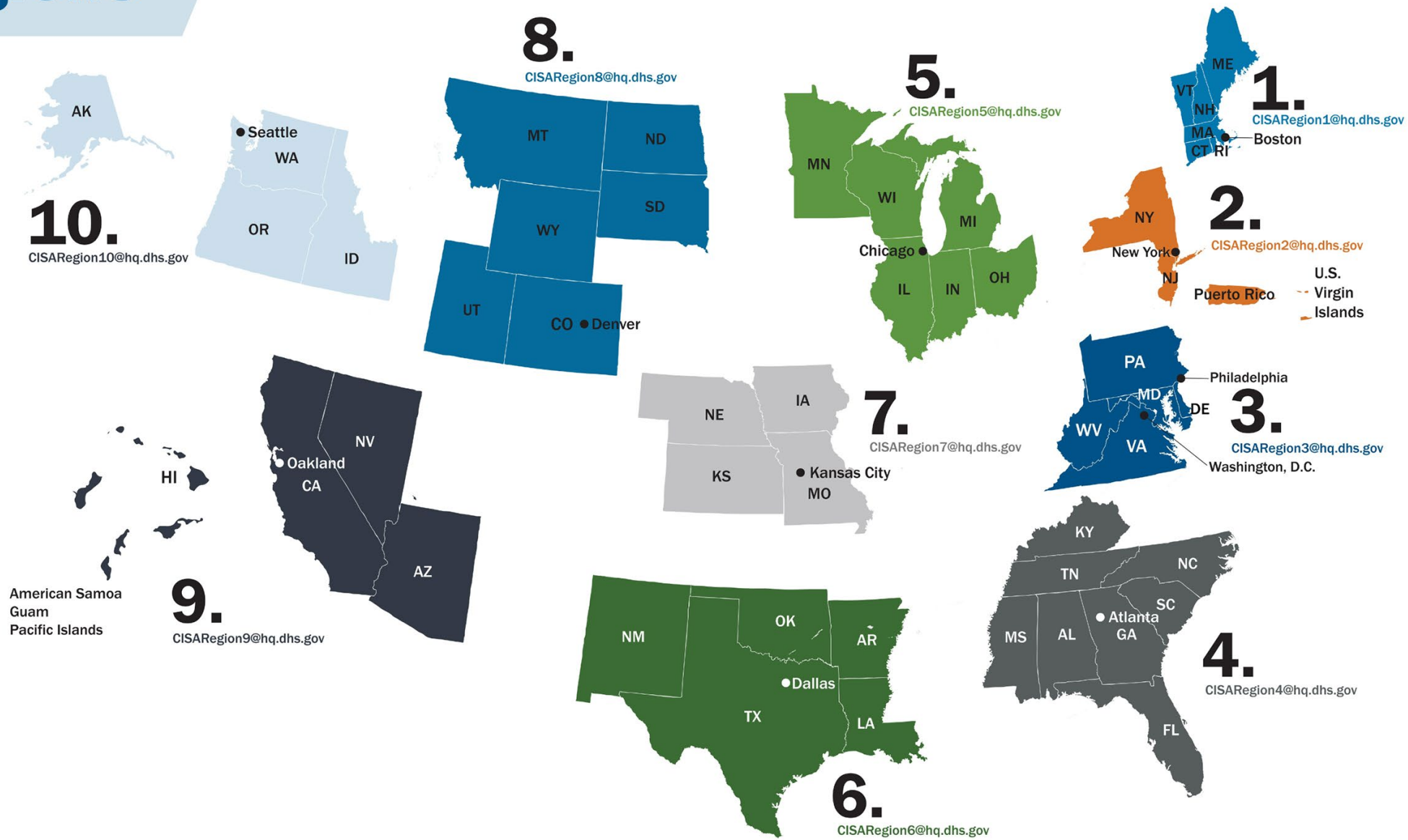






	October 1:	WEEK 1: Week of October 4	WEEK 2: Week of October 11	WEEK 3: Week of October 18	WEEK 4: Week of October 25
Cybersecurity Awareness Month	Official Kick-off	Be Cyber Smart.	Phight the Phish!	Explore. Experience. Share. (Cybersecurity Career Awareness Week)	Cybersecurity First
CISA Cyber Summit		Assembly Required: Pieces of the Vulnerability Management Ecosystem	Collaborating for the Collective Defense	Team Awesome: The Cyber Workforce	Power of Partnership

CISA Regions



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

CISA Services

- **Check out stopransomware.gov**
  - **https://www.cisa.gov/stopransomware**
  - **take the ransomware self-assessment in our CSET tool**
- **The Cyber Security Evaluation Tool (CSET®) is a stand-alone desktop application that guides asset owners and operators through a systematic process of evaluating Operational Technology and Information Technology**
  - **CSET was updated to include a new module: Ransomware Readiness Assessment (RRA)**
  - **The RRA is a self-assessment based on a tiered set of practices to help organizations better assess how well they are equipped to defend against and recover from a ransomware incident**
  - **https://www.cisa.gov/stopransomware/cyber-security-evaluation-tool-csetr**

CISA Services Continued

- CISA's Bad Practices
  - CISA is developing a catalog of Bad Practices that are exceptionally risky
    - Use of unsupported (or end-of-life) software
    - Use of known/fixed/default passwords and credentials
    - The use of single-factor authentication for remote or administrative access to systems
  - https://www.cisa.gov/stopransomware/bad-practices
- CISA Alerts
  - National Cyber Awareness System
  - sign up for CISA's alerts = https://us-cert.cisa.gov/ncas
- CISA Service Catalog
  - The CISA Services Catalog is a single resource that provides users with access to information on services across all of CISA's mission areas
  - https://www.cisa.gov/publication/cisa-services-catalog

CISA Services Continued

- **Cyber Hygiene Services**
  - CISA offers several scanning and testing services to help organizations reduce their exposure to threats by taking a proactive approach to mitigating attack vectors.
    - **Vulnerability Scanning**: Evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts.
    - **Web Application Scanning**: Evaluates known and discovered publicly-accessible websites for potential bugs and weak configuration to provide recommendations for mitigating web application security risks.
    - **Phishing Campaign Assessment**: Provides an opportunity for determining the potential susceptibility of personnel to phishing attacks. This is a practical exercise intended to support and measure the effectiveness of security awareness training.
    - **Remote Penetration Test:** Simulates the tactics and techniques of real-world adversaries to identify and validate exploitable pathways. This service is ideal for testing perimeter defenses, the security of externally-available applications, and the potential for exploitation of open-source information.
  - https://www.cisa.gov/cyber-hygiene-services

- Email us at vulnerability_info@cisa.dhs.gov with the subject line “Requesting Cyber Hygiene Services” to get started


CYBERSECURITY & INFRASTRUCTURE
SECURITY AGENCY
CISA