



# CYBER SERVICES FACT SHEET SPECIAL EVENTS



## OVERVIEW

CISA supports both public and private sector partners by providing proactive testing and assessment services. These services provide an objective third-party perspective of stakeholder operational cybersecurity posture and identify security control strengths and weaknesses. CISA aggregates these insights into actionable reports that champion the implementation of mitigations and controls capable of positive impact toward overall risk reduction.

## OBJECTIVES

- Reduce stakeholder risk.
- Enable data-driven decisions.
- Influence operational behaviors.
- Increase national resilience

## OFFERINGS TO INCREASE CYBER RESILIENCE

**Vulnerability Scanning (VS)** is a persistent scanning service of Internet-accessible systems for vulnerabilities, configuration errors, and suboptimal security practices.

**Web Application Scanning (WAS)** evaluates known and discovered publicly accessible websites for bugs, known vulnerabilities, and weak configurations and provides recommendations for mitigating web application security risks.

**Remote Penetration Test (RPT)** focuses on testing Internet exposure to eliminate exploitable pathways.

**Risk and Vulnerability Assessment (RVA)** combines national threat information with data collected and vulnerabilities identified through remote and on-site stakeholder assessment activities to provide a tailored risk analysis report.

**Validated Architecture Design Review (VADR)** evaluates an organization's systems, networks, and security services to determine if they are designed, built, and operated in a reliable and resilient manner.

**Exercises** CISA conducts [cyber and physical security exercises](#) with government and industry partners to enhance security and resilience of critical infrastructure.

**Workshops** CISA conducts workshops to build capacity within stakeholder's organizations. Several workshop options to choose from including Incident Management.

**Training Opportunities to increase cyber knowledge and skills in:** [ICS Incident Response](#) [CISA Learning](#)

**Incident Coordination** Use the [Incident Response Portal](#) to report an incident and obtain service from CISA in areas of incident response, threat hunting, coordination and support.

**Cyber Security Awareness Secure Our World.** Simple ways to protect yourself, your family, and business from threats.

[Strong Passwords](#)

[Recognize and Report Phishing](#)

[Patch Systems](#)

[Multi-factor Authentication](#)

## HOW TO GET STARTED

Contact the local Cybersecurity Advisor at [CISARegion6@cisa.dhs.gov](mailto:CISARegion6@cisa.dhs.gov) to get started. Please keep in mind:

- CISA's assessments are available to both public and private organizations at no cost.
- Service availability is limited; service delivery timelines are available upon request. CISA prioritizes service delivery queues on a continuous basis to ensure no stakeholder/sector receives a disproportionate allocation of resources and the data collected is a diverse representation of the nation.