CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

RISK AND VULNERABILITY ASSESSMENT

The CISA team supports Federal, State, Local, Tribal and Territorial Governments and Critical Infrastructure partners by providing proactive testing and assessment services.

CISA's Risk and Vulnerability Assessment (RVA) is a one-on-one engagement with stakeholders that combines open-source national threat and vulnerability information with data collected through remote and onsite assessment activities to provide actionable risk analysis reports with remediation recommendations prioritized by severity and risk.

CAPABILITIES

Penetration Testing: CISA conducts an array of tests to determine susceptibility to an actual real-world attack by infiltrating the target environment using current tactics, techniques, and procedures. Specific types of testing and assessments include network, web application, wireless, war dial, and social engineering in the form of an email phishing campaign.

Configuration Review: CISA reviews and analyzes operating system and database settings and configurations, which the team compares to industry standards, guidelines, and best practices to identify security issues.

ASSESSMENT 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

ASSESEMENT TIMELINE

Pre-Planning

- Request RVA
- Receive RVA brief
- Sign and return documents

Planning

- Confirm schedule
- Establish Trusted Point of Contact
- Determine RVA services, scope, and logistics during pre-assessment call(s)

Execution (Ten Days)

- One week external testing
- One week internal testing
- Remote Penetration Testing – external only

Post-Execution

- Out-Brief – provide initial findings
- Report review and receipt – 10 days
- Follow-up on remediation actions – 180 day

ABOUT

Our Team

The CISA team is a group of highly trained information security experts. Our mission is to measurably reduce cybersecurity risks to our Nation.

CISA leads the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

Our services provide:

- **A proactive, risk-based approach** to analyzing stakeholder systems
- **Expertise** in identification of vulnerabilities, risk evaluation, and prioritized mitigation guidance
- **Comprehensive services that empower stakeholders** to increase speed and effectiveness of their cyber response capabilities

Additional Information

CISA's security services are available at no cost. Stakeholders include Federal, State, Local, Tribal and Territorial governments, as well as Critical Infrastructure private sector companies. CISA does not share attributable information without written and agreed consent from the stakeholder. CISA uses anonymized data to develop non-attributed reports for trending and analysis purposes.

GET STARTED

Capabilities and service delivery timelines are available upon request. Service availability is limited. Contact us at **vulnerability_info@cisa.dhs.gov** to get started. Service delivery queues are prioritized on a continuous basis to ensure no stakeholder or sector receives a disproportionate amount of resources and that the data collected is a diverse representation of the nation.

MISSION AND VISION

Mission: *Providing cybersecurity assessments to facilitate the identification of risk for the purpose of protecting the Nation’s cyber infrastructure.*

Vision: *To be the preeminent government leader providing comprehensive, innovative, and dynamic cybersecurity assessments for the purpose of facilitating and protecting the federal, state, private sector and critical infrastructure networks of the United States, reducing attack surfaces, eliminating threats, and fostering partnerships across the government landscape.*