CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

CYBER HYGIENE: VULNERABILITY SCANNING

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

CISA's Cyber Hygiene Vulnerability Scanning is "internet scanning-as-a-service." This service continuously assesses the "health" of your internet-accessible assets by checking for known vulnerabilities and weak configurations, and recommends ways to enhance security through modern web and email standards.

SCANNING OBJECTIVES

- 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

SCANNING PHASES AND STAGES

PHASES

- **Target Discovery:** Identify all active internet-accessible assets (networks, systems, and hosts) to be scanned
- **Vulnerability Scanning:** Initiate non-intrusive checks to identify potential vulnerabilities and configuration weaknesses

STAGES

Pre-Planning

- Request service
- Receive Cyber Hygiene brief
- Provide target list (scope)
- Sign and return documents

Planning

- Confirm scanning schedule
- Pre-scan notification

Execution

- Initial scan of submitted scope
- Rescan scope based on detected vulnerability severity:
  - 12 hours for "critical"
  - 24 hours for "high"
  - 4 days for "medium"
  - 6 days for "low"
  - 7 days for "no vulnerabilities"

Reporting

- Ongoing weekly summary report
- Vulnerability mitigation recommendations
- Detailed findings in consumable format

ABOUT

Our Team

The CISA Assessments 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 assessments' 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 **NCATS_INFO@hq.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.*