



## NATIONAL CYBERSECURITY ASSESSMENTS AND TECHNICAL SERVICES (NCATS)

The NCATS team is a component of the Department of Homeland Security’s (DHS) NCCIC and supports Federal, State and Local governments and Critical Infrastructure partners by providing proactive testing and assessment services. NCATS provides its stakeholders with an objective third-party perspective of their operational cybersecurity posture and identifies security control strengths and weaknesses. These insights are culminated into actionable reports that champion the implementation of mitigations and controls capable of positive impact toward reduction of overall risk.

**Vision: To be the premier, trusted agent for change and key instrument in proactively identifying risks and increasing national cybersecurity resilience.**

### Objectives

- Identify and eliminate remote attack paths prior to exploitation by malicious actors
- Champion and promote effective, data-driven standards, policies, guidelines, and capabilities
- Influence, measure, and monitor the implementation of mature operational capabilities and adoption of positive operational behaviors
- Drive effective cybersecurity risk mitigation strategies
- Improve policy makers’ ability to drive informed, risk-based decisions

### Service Offerings

<b>Cyber Hygiene: Vulnerability Scanning</b>
Near persistent scanning of Internet accessible systems for vulnerabilities, configuration errors, and suboptimal security practices.
<b>Phishing Campaign Assessments</b>
Measures propensity to click on email phishing lures to increase training and awareness.
<b>Risk Assessments</b>
<b>Risk and Vulnerability Assessments</b>
Combines national threat information with data collected and vulnerabilities identified through onsite assessment activities in order to provide tailored risk analysis reports.
<b>Remote Penetration Testing</b>
Focus solely on Internet accessible systems, such as firewalls, routers, web portals, and the elimination of remote attack paths.
<b>Red Team Assessments</b>
Penetration testing that closely mirrors an attack by an advanced adversary to test a stakeholder’s operational capabilities and maturity.
<b>Validated Architecture Design Review</b>
Evaluates resiliency of a stakeholder’s systems, networks, and security services.
<b>Training and Qualification</b>
Assistance in training third-party organization teams with DHS assessment standards.



## About

### Our Team

NCATS is a group of highly trained information security experts within DHS NCCIC. Our mission is to measurably reduce the cybersecurity risks to our Nation's cybersecurity infrastructure.

DHS is responsible for protecting the Nation's infrastructure from physical and cyber threats, including those impacting business and government operations.

### Our Work



**A proactive, risk-based approach** to analyzing stakeholder systems



**Expertise** in identification of vulnerabilities, risk evaluation, and prioritized mitigation guidance



**Empowering stakeholders** to increase speed and effectiveness of their cyber-attack response capabilities

### Additional Information

NCATS security services are available at no-cost. Our stakeholders include Federal, State, Local, Tribal and Territorial levels of governments, as well as Critical Infrastructure Private Sector companies.

NCATS does not share attributable information collected during assessments without written and agreed consent from the stakeholder. However, anonymized data is used to develop non-attributed reports for trending and analysis purposes.

Assessments are not conducted in response to an incident, but to identify, mitigate, and remediate vulnerabilities prior to exploitation by an attacker.

## Get Started

NCATS' capabilities and service delivery timelines are available upon request. Testing availability is limited so contact us soon to get started.

[NCATS\\_INFO@HQ.DHS.GOV](mailto:NCATS_INFO@HQ.DHS.GOV)

*In support of our national mission, the NCATS 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 many stakeholders that the NCCIC and NCATS support.*