GOBIERNO DE PUERTO RICO

Corporación Pública para la Supervisión y
Seguro de Cooperativas de Puerto Rico

22 de septiembre de 2020

CARTA INFORMATIVA 2020-29

A TODAS LAS COOPERATIVAS DE AHORRO Y CREDITO

Emilio Torres Antuñano
Presidente Ejecutivo

PRUEBAS Y EVALUACIONES DE SEGURIDAD CIBERNETICA POR LA AGENCIA DE SEGURIDAD DE INFRAESTRUCTURA Y CIBERSEGURIDAD (CISA)

La Agencia de Seguridad de Infraestructura y Ciberseguridad (o CISA, por sus siglas en inglés) de los Estados Unidos adscrita al Departamento de Seguridad Nacional ("Department of Homeland Security" o DHS, por sus siglas en inglés) ha publicado que está ofreciendo servicios relacionados a evaluaciones y pruebas de seguridad cibernética a entidades tales como agencias del gobierno federal, estatal, local, así como entidades del sector de infraestructura crítica. Entidades del sector de infraestructura crítica incluyen aquellas cuyos activos, sistemas y redes, ya sean físicos o virtuales, se consideran tan vitales para los Estados Unidos que su interrupción o destrucción tendría un efecto debilitante en la seguridad nacional, seguridad económica, salud pública o cualquier combinación de estos. En este sector se incluyen a nuestras cooperativas de ahorro y crédito. Estos servicios son proporcionados sin costo alguno a aquellas entidades aplicables que así lo soliciten.

En resumen, entidad federal está ofreciendo servicios que incluyen, entre otros, los siguientes aspectos:

1. Escaneo de vulnerabilidades para evaluar el "estado de salud" de los dispositivos tecnológicos accesibles a través del Internet. Incluye procedimientos de escaneo de vulnerabilidades y evaluación de la presencia de las mejores prácticas de seguridad en las plataformas web y correo electrónico.

2. Simulación de "Phishing" para medir la propensión de los usuarios de hacer "clic" en señuelos de "phishing" por correo electrónico, que se utilizan comúnmente por los cibercriminales para recopilar información confidencial o para obtener acceso a una red.

   Las evaluaciones incluyen determinar la susceptibilidad de los usuarios para hacer "clic" en enlaces atractivos en correos electrónicos de "phishing" diseñados por expertos que emulan a atacantes del mundo real. Los resultados de la evaluación se pueden utilizar para brindar orientación a las cooperativas para establecer medidas efectivas de capacitación y concienciación del personal de la cooperativa contra el "phishing".

3. Evaluación de riesgos y vulnerabilidades donde combina información de vulnerabilidades y cibernéticas identificadas a nivel nacional, con datos recopilados en la configuración tecnológica de la cooperativa para proporcionar informes de análisis de riesgo con recomendaciones de remediación priorizadas por nivel de gravedad y riesgo. Las evaluaciones incluyen:

   - Pruebas de penetración de aplicaciones, sistemas y redes.
   - Revisión y análisis de la configuración tecnológica de la institución (sistema operativo y bases de datos) y comparación con los estándares, pautas y mejores prácticas de la industria para identificar problemas de seguridad.

4. Evaluación integral del entorno tecnológico (personas, procesos, tecnologías responsables de proteger la red y los sistemas de información de la institución) para brindar información sobre la postura de ciberseguridad y capacitación práctica para el personal técnico. La evaluación incluye pruebas de las redes simulando ciberataques donde se obtiene acceso a una red y se permanece sin ser detectado durante un período de tiempo prolongado para robar datos.

5. Evaluación diseño de la arquitectura tecnológica basada en los estándares, pautas y mejores prácticas establecidas en el gobierno federal e industria. La evaluación incluye:

   - Revisión del diseño de la arquitectura tecnológica y su interconectividad con sistemas internos y externos para enfocarse en estrategias defensivas.

- Revisión detallada de la configuración y actividad del sistema para determinar la susceptibilidad a posibles ataques y anomalías.
- Análisis del tráfico de la red utilizando una combinación de herramientas para identificar comunicaciones anómalas que podrían indicar una actividad sospechosa o una mala configuración.

6. Ejecución de pruebas de penetración remotas para evaluar e identificar vulnerabilidades y establecer curso de acción para eliminar rutas explotables. Estas pruebas se enfocan en los sistemas accesibles externamente. Las pruebas incluyen:

    - Verificar si la red es accesible desde el dominio público por un usuario no autorizado. Estas pruebas incluyen la evaluación de puertos abiertos, protocolos y servicios.
    - Evaluación de aplicaciones web para identificar posibles vulnerabilidades explotables.
    - Pruebas de vectores de ataques originados por correo electrónico.

Para solicitar estos servicios la cooperativa debe enviar un comunicado a la agencia federal vía correo electrónico solicitando información detallada del alcance de los servicios que ofrecen y documentación para solicitar dichos servicios a los siguientes correos electrónicos:

- cisaservicedesk@cisa.dhs.gov
- vulnerability_info@cisa.dhs.gov

(En el correo electrónico es importante que se proporcione el detalle de la institución solicitante e información de contacto).

Recomendamos que se consideren estos servicios por parte de las cooperativas, proporcionados por la agencia federal de los Estados Unidos de más alto rango en el tema de Ciberseguridad, para evaluar su postura de seguridad cibernética que tanta relevancia y potencial de riesgo tienen en estos tiempos. Además, es importante que para todo tipo de iniciativas relacionadas a evaluaciones y pruebas de seguridad las cooperativas consideren los siguientes aspectos:

1. Definir e implementar acciones afirmativas de seguimiento y remediación derivadas como resultado de procedimientos de evaluaciones y pruebas para reforzar y/o mejorar los controles de seguridad cibernética.

2. Proporcionar, por parte de la Administración, una supervisión adecuada en el desarrollo de marcos de seguridad y controles que deben consistir en políticas, medidas, prácticas, procedimientos y la asignación apropiada de roles y responsabilidades relacionadas.

3. Informar a la Junta de Directores sobre las actividades relacionadas a evaluaciones y pruebas de seguridad, resultados, medidas de seguimiento y remediación por parte de la cooperativa

Adjunto incluimos documentos de los servicios propuestos por la entidad.

- CyHy_NCATS Fact Sheet.pdf
- PCA_NCATS Fact Sheet.pdf
- RVA_NCATS Fact Sheet.pdf
- RTA_NCATS Fact Sheet.pdf
- VADR_NCATS Fact Sheet.pdf
- RPT_NCCIC Fact Sheet.pdf

De tener inconvenientes con cumplir con lo establecido en nuestra carta se puede comunicar con nosotros a los correos electrónicos wocasio@cossec.pr.gov y gcordero@cossec.pr.gov.

NCCIC

National Cybersecurity and
Communications Integration Center

NATIONAL CYBERSECURITY ASSESSMENTS AND TECHNICAL SERVICES (NCATS)

RISK AND VULNERABILITY ASSESSMENT

A NCATS 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 on-site assessment activities to provide actionable risk analysis reports with remediation recommendations prioritized by severity and risk.

Capabilities

Penetration Testing

NCATS 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

NCATS reviews and analyzes operating system and database settings and configurations and compares them 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

Assessment Timeline

[1] Pre-Planning

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

[2] Planning

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

[3] Execution (10 days)

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

[4] Post-Execution

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

NCCIC

National Cybersecurity and
Communications Integration Center

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

Our Services

NCATS also offers the following services:

[+] Cyber Hygiene: Vulnerability Scanning

[+] Phishing Campaign Assessments

[+] Red Team Assessments

[+] Validated Architecture Design Review

[+] Training and Qualification for Third Party Assessment Organizations

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

To learn more about NCATS or request service, contact us using the information below. Testing availability is limited so contact us soon to get started.

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.

NCCIC

National Cybersecurity and
Communications Integration Center

NATIONAL CYBERSECURITY ASSESSMENTS AND TECHNICAL SERVICES (NCATS)

RED TEAM ASSESSMENT

A NCATS Red Team Assessment (RTA) is a comprehensive evaluation of an IT environment. Emulation of Advanced Persistent Threats (APT) assist customers in determining their security posture by analyzing effectiveness of response capabilities to a determined adversarial presence. RTAs are specifically crafted to test the people, processes, and technologies defending a network.

Assessment Phases

Threat Emulation

An emulation of APT **tactics**, **techniques**, and **procedures** using *publicly available tools and data* to access, navigate, and persist **in a customers's environment**.

Measurable Events

Once entrenched in the network, a series of events are initiated specifically intended to **provoke** a security response.

Measured effectiveness of the **people, processes, and technologies** defending a customers's network is determined by observable response-driven metrics.

Assessment Objectives

- Test customer's networks using real-world APT attacker methodologies
- Evaluate people, processes, and technologies responsible for defending the customer's network and information systems
- Provide customer executives actionable insight to their cybersecurity posture and practical training for technical personnel

Assessment Timeline

[1] Pre-Execution

- Request assessment
- Receive RTA capabilities brief
- Sign and return documents

[2] Planning

- Confirm assessment schedule
- Define scope and set expectations
- Establish Trusted Agent

[3] Execution (90 days)

- Conduct Information Gathering
- Emulate APT activities
- Initiate Measurable Events

[4] Post-Execution

- On-site out-brief and technical training
- Final report review and receipt

NCCIC

National Cybersecurity and
Communications Integration Center

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

Our Services

NCATS also offers the following services:

[+] Cyber Hygiene: Vulnerability Scanning

[+] Phishing Campaign Assessments

[+] Risk and Vulnerability Assessments

[+] Remote Penetration Testing

[+] Validated Architecture Design Review

[+] Training for Third Party Organizations

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

To learn more about NCATS or request service, contact us using the information below. Testing availability is limited so contact us soon to get started.

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.

NCCIC

National Cybersecurity and
Communications Integration Center

NATIONAL CYBERSECURITY ASSESSMENTS AND TECHNICAL SERVICES (NCATS)

REMOTE PENETRATION TESTING

An NCATS Remote Penetration Test (RPT) utilizes a dedicated remote team to assess and identify vulnerabilities and work with customers to eliminate exploitable pathways. RPTs are similar to risk and vulnerability assessments but focus only on externally accessible systems with a tradeoff made for more service capacity at the expense of assessment scope. As a remote service, it is more cost effective and scalable than onsite offerings at the expense of organizational insight and context.

Scenarios

External Penetration Test
Verify if the stakeholder network is accessible from the public domain by an unauthorized user by assessing open ports, protocols, and services.

External Web Application Test
Evaluating web applications for potential exploitable vulnerabilities can include automated scanning, manual testing, or a combination of both methods.

Phishing Assessment
Testing through an email attack vector. The team generates and sends carefully crafted phishing emails to the Trusted Point of Contact containing a variety of malicious payloads.

Assessment Objectives

- Conduct assessments to identify vulnerabilities and work with customers to eliminate exploitable pathways
- Simulate the tactics and techniques of real-world threats and malicious adversaries
- Test centralized data repositories and externally accessible assets/resources
- Avoid causing disruption to the customer organization’s mission, operation, and/or network infrastructure

Assessment Timeline

[1] Pre-Planning

- Request RPT
- Receive RPT Capabilities Brief
- Sign and return RPT Rules of Engagement

[2] Planning

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

[3] Execution (Up to 6 weeks)

- Dependent on resource availability
- Critical findings are immediately disclosed

[4] Reporting

- Briefing and initial recommendations
- Final report review and receipt – 10 days
- Follow-up on mitigation actions – 180 days

NCCIC

National Cybersecurity and
Communications Integration Center

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 critical infrastructure from physical and cyber threats, including those impacting business and government operations.

Our Work

A proactive, risk-based approach to analyzing stakeholder systems

Expert identification of vulnerabilities, risk evaluation, and prioritized mitigation guidance

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

Our Services

NCATS additionally offers the following services:

[+] Cyber Hygiene – Vulnerability Scanning

[+] Phishing Campaign Assessments

[+] Red Team Assessment

[+] Validated Architecture Design Review

[+] NCATS Methodology and Approach

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

To learn more about NCATS or request service, contact us using the information below. Testing availability is limited so contact us soon to get started.

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.

NCCIC

National Cybersecurity and
Communications Integration Center

NATIONAL CYBERSECURITY ASSESSMENTS AND TECHNICAL SERVICES (NCATS)

PHISHING CAMPAIGN ASSESSMENT

Do you TAKE the BAIT or SPOT the TRAP?

A NCATS Phishing Campaign Assessment (PCA) measures an organization’s propensity to click on email phishing lures, commonly used to collect sensitive information or as initial access to a network. PCA results can be used to provide guidance for anti-phishing training and awareness.

Based on NCATS assessment testing, email phishing is the number one proven means of access into a private network.

Capabilities

Test
Assess the susceptibility of a specified target user base to click on enticing links in expertly crafted phishing emails emulating real world attackers.
Inform
Provide leadership on potential training and awareness improvements based on the metrics gathered through the course of the assessment.

Assessment Objectives

- Reduce risk to malicious phishing email attempts by testing and informing users
- Understand how users are enticed to click on links and report suspicious activity
- Properly emulate malicious phishing activity to provide a quality learning experience

Assessment Timeline

[1] Pre-Planning

- Request assessment
- Receive PCA brief
- Sign and return documents

[2] Planning

- Confirm schedule
- Approve email templates
- Test email delivery/receipt

[3] Execution (6 weeks)

- Receive increasingly complex phishing emails from preapproved templates
- Conduct mid-testing training event

[4] Post-Execution

- Receive weekly click-rate summaries
- Final report review and receipt
- Optional 180-Day retest available

NCCIC

National Cybersecurity and
Communications Integration Center

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

Our Services

NCATS also offers the following services:

[+] Cyber Hygiene: Vulnerability Scanning

[+] Risk and Vulnerability Assessments

[+] Remote Penetration Testing

[+] Red Team Assessments

[+] Validated Architecture Design Review

[+] Training and Qualification for Third Party Assessment Organizations

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

To learn more about NCATS or request service, contact us using the information below. Testing availability is limited so contact us soon to get started.

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.

NCCIC

National Cybersecurity and
Communications Integration Center

NATIONAL CYBERSECURITY ASSESSMENTS AND TECHNICAL SERVICES (NCATS)

CYBER HYGIENE: VULNERABILITY SCANNING

The NCATS Cyber Hygiene: Vulnerability Scanning activities continuously assess the “health” of external stakeholder endpoints reachable via the Internet. Activities consist of voluntary target discovery, vulnerability scanning, and checks of web and email best practices.

Scanning Phases

Target Discovery

Process of identifying all active Internet accessible assets (networks, systems and hosts) to be scanned for vulnerabilities.

Vulnerability Scanning & Configuration Tests

Occurs as a continuous series of non-intrusive checks in order to identify existing or potential vulnerabilities and configuration weaknesses.

Scanning Objectives

- Maintain a continually updated enterprise view of the cybersecurity posture of stakeholder’s Internet accessible systems
- Understand how systems and infrastructure appear to potential attackers
- Drive proactive mitigation of vulnerabilities and reduce risk

Scanning Timeline

[1] Pre-Planning

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

[2] Planning

- Confirm scanning schedule
- Pre-scan notification

[3] 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”

[4] Post-Execution

- Scanning summary report with Report Card
- Vulnerability mitigation recommendations
- Detailed findings included as exports
- Weekly reporting intervals

NCCIC

National Cybersecurity and
Communications Integration Center

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

Our Services

NCATS also offers the following services:

[+] Phishing Campaign Assessments

[+] Risk and Vulnerability Assessments

[+] Remote Penetration Testing

[+] Red Team Assessments

[+] Validated Architecture Design Review

[+] Training and Qualification for Third Party Assessment Organizations

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

To learn more about NCATS or request service, contact us using the information below. Testing availability is limited so contact us soon to get started.

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.

NCCIC

National Cybersecurity and
Communications Integration Center

NATIONAL CYBERSECURITY ASSESSMENTS AND TECHNICAL SERVICES (NCATS)

VALIDATED ARCHITECTURE DESIGN REVIEW

A NCATS Validated Architecture Design Review (VADR) is an assessment based on Federal and industry standards, guidelines, and best practices. Assessments can be conducted on Information Technology (IT) or Operational Technology (OT) infrastructures.

Capabilities

Architecture Design Review

In-depth review of network architecture design and interconnectivity to internal and external systems focused on defensive strategies.

System Configuration and Log Review

Detailed review of system settings and activity to determine the susceptibility to potential attacks and baseline normal behavior to find anomalies.

Network Traffic Analysis

Utilizes a combination of open-source and commercial tools to identify anomalous communications which could indicate suspicious activity or misconfiguration.

Assessment Objectives

- Reduce risk to the Nation's Critical Infrastructure components
- Analyze systems based on standards, guidelines, and best practices
- Ensure effective defense-in-depth strategies
- Provide findings and practical mitigations for improving operational maturity and enhancing cybersecurity posture

Assessment Timeline

[1] Pre-Planning

- Request VADR
- Receive VADR Capabilities Brief
- Sign and return documents

[2] Planning

- Submit network diagram
- Schedule scoping meeting
- Submit network configurations, logs, and packet captures
- Schedule execution activities

[3] Execution

- Review submitted architecture
- Analyze packet captures
- Interviews with key personnel

[4] Post-Execution

- Out-Brief - provide initial findings
- Final report (+6 weeks)
- Follow-up on remediation actions - 180 days

NCCIC

National Cybersecurity and
Communications Integration Center

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

Our Services

NCATS also offers the following services:

[+] Cyber Hygiene: Vulnerability Scanning

[+] Phishing Campaign Assessments

[+] Risk and Vulnerability Assessments

[+] Remote Penetration Testing

[+] Red Team Assessments

[+] Training and Qualification for Third Party Assessment Organizations

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

To learn more about NCATS or request service, contact us using the information below. Testing availability is limited so contact us soon to get started.

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.