CISA ASSESSMENTS

The CISA Assessments team supports Federal, State, Local, Tribal and Territorial Governments and Critical Infrastructure partners by providing proactive testing and assessment services. The team also provides an objective third-party perspective of stakeholder operational cybersecurity posture and identifies security control strengths and weaknesses. CISA Assessments 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 Decision
- Influence Operational Behaviors
- Increase National Resilience

SERVICE OFFERINGS

- **Vulnerability Scanning** is the persistent scanning of internet-accessible systems for vulnerabilities, configuration errors, and suboptimal security practices.
- **Phishing Campaign Assessments** measure propensity to click on email phishing lures which increases organizational training and awareness.
- **Remote Penetration Testing** focuses on testing a stakeholder's internet exposure.
- **Risk and Vulnerability Assessments** combine national threat information with data collected and vulnerabilities identified through on-site assessment activities to provide tailored risk analysis reports.
- **Red Team Assessments** closely mirror an attack by an advanced adversary to test operational capabilities and maturity.
- **Validated Architecture Design Review** evaluates the resiliency of a stakeholder's systems, networks and security services.
- **Third-Party Qualification** qualifies third-party organizations to perform assessments and technical services following CISA Assessments standards, process and procedures.
- **Critical Product Evaluations** assess, within an isolated environment, the "out-of-the-box" security of products and solutions relevant to critical infrastructure operations and national resilience.
- **Cyber Resilience Review** identifies and evaluates cyber security management capabilities, maturity, and capacity to manage cyber risk during normal operations and times of operational stress.
- **External Dependency Management** assesses the activities and practices utilized by an organization to manage risks arising from external dependencies.
- **Cyber Infrastructure Survey** identifies cybersecurity controls and protective measures in place and provides an interactive dashboard for comparative analysis and valuation.

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.

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.
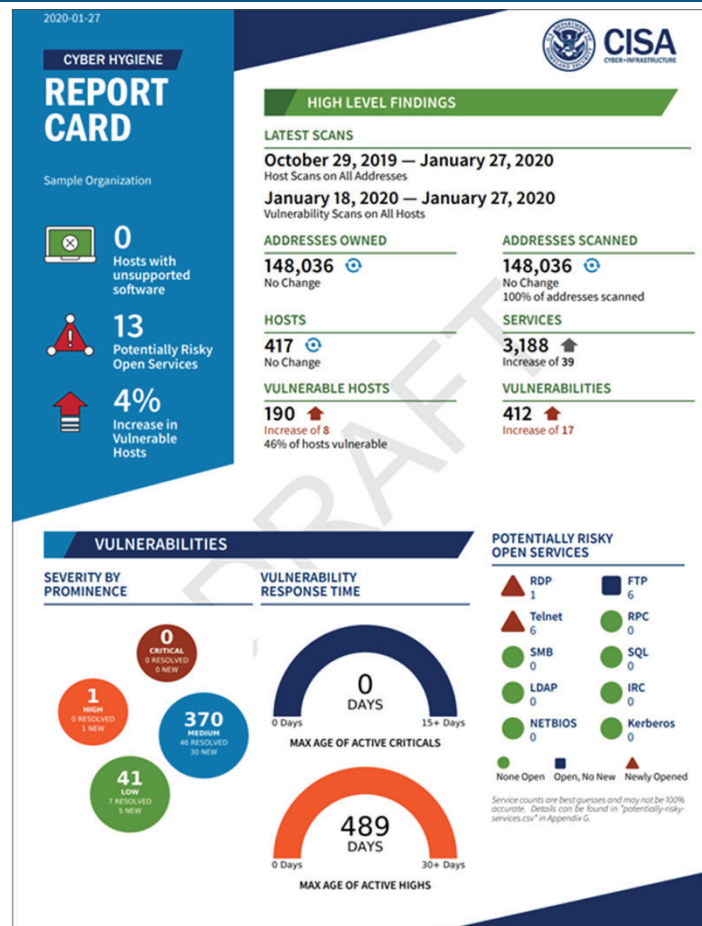
Report Card

High Level Findings

- Latest Scans
- Addresses Owned
- Addresses Scanned
- Hosts
- Services
- Vulnerable Hosts
- Vulnerabilities

Vulnerabilities

- Severity by Prominence
- Vulnerability Response Time
- Potentially Risky Open Services

HIGH VALUE ASSET ASSESSMENT

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

CISA Assessments' High Value Asset (HVA) Assessment is similar to a Risk and Vulnerability Assessment in knowledge, skills, tools, tactics, and methodology. However, an HVA entails specific, predefined attack scenarios used consistently across the assessment targeted at critical assets selected by the Office of Management and Budget.

OBJECTIVES

- Identify weaknesses through scenario-based network penetration testing, web application testing, and social engineering
- Test stakeholder networks using real world capabilities and methodologies
- Understand how systems and infrastructure appear to potential attackers
- Coordinate with CISA Hunt and Incident Response Team to provide follow-on services within the pertinent domain

ASSESSMENT SCENARIOS AND TIMELINES

SCENARIOS

- **External Access:** Determine if HVA is accessible from the internet by an unauthorized user.
- **Phishing Campaign Assessments** measure propensity to click on email phishing lures to increase training and awareness.
- **Web Application Assessment:** Identify any exploits in web applications.
- **Internal Access:** Determine if HVA system is accessible from the internal domain by an unauthorized user.
- **Internal Threat Emulation:** Examine access level of legitimate user on HVA system and associated data.
- **Data Exfiltration:** Test ability to transfer sensitive data to external site on the internet.

TIMELINES

Pre-Planning

- Receive selection for assessment
- Receive HVA brief
- Sign and return documents

Planning

- Confirm schedule
- Establish trusted points of contact

Execution

- Perform scenario activity
- On-site testing performed as required

Post-Execution

- On-site briefing and initial recommendations
- Final report review and receipt

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.

CYBER HYGIENE: WEB APPLICATION SCANNING (WAS)

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 Web Application Scanning is "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, we can recommend ways to enhance security in accordance with industry and government best practices and standards.
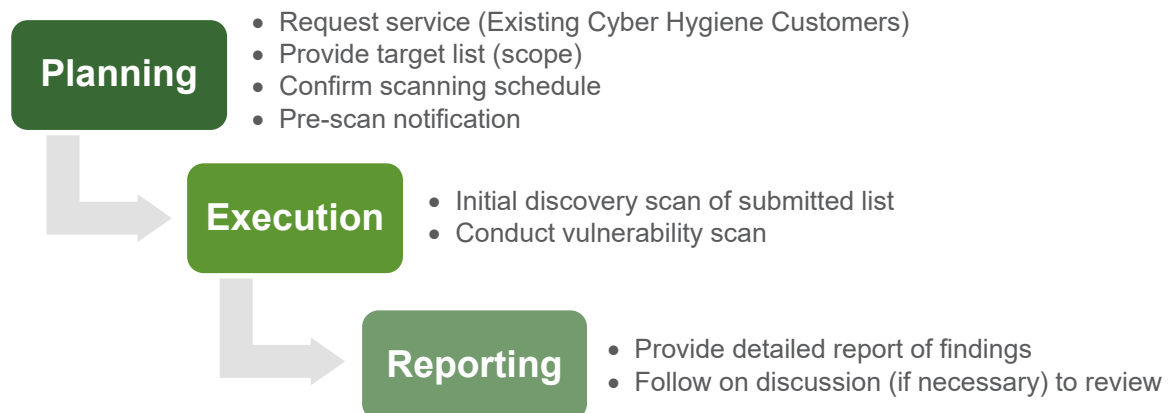
SCANNING OBJECTIVES

- Maintain enterprise awareness of your publicly accessible web-based assets
- Provide insight into how systems and infrastructure appear to potential attackers
- Drive proactive mitigation of vulnerabilities to help reduce overall risk

SCANNING PHASES AND OVERALL PROCESS

Scanning Phases

- **Discovery Scanning:** Identify active, internet-facing web applications
- **Vulnerability Scanning:** Initiate non-intrusive checks to identify potential vulnerabilities and configuration weaknesses

Overall Process

Planning
- Request service (Existing Cyber Hygiene Customers)
- Provide target list (scope)
- Confirm scanning schedule
- Pre-scan notification

Execution
- Initial discovery scan of submitted list
- Conduct vulnerability scan

Reporting
- Provide detailed report of findings
- Follow on discussion (if necessary) to review

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 Federal Government, SLTT and critical infrastructure networks.

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 currently limited to existing CISA customers. 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.

PHISHING CAMPAIGN ASSESSMENT

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

CISA Assessments' 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. Based on CISA Assessments' testing, email phishing is the number one means of initial access into a private network. PCA results can be used to provide guidance for anti-phishing training and awareness.

CAPABILITIES

Test: Assess the behavioral responses of a specified target user base when presented with expertly crafted phishing emails emulating real world threats.

Inform: Provide leadership information 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

Pre-Planning
- Request assessment
- Receive PCA briefing documents
- Sign and return forms

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

Execution (Six weeks)
- Receive increasingly deceptive phishing emails from pre-approved templates

Post-Execution
- Receive weekly click-rate summaries
- Final report review and receipt
- Optional retest available

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.

VALIDATED ARCHITECTURE DESIGN REVIEW

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

CISA Assessments' 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

Pre-Planning

- Request VADR
- Sign and return documents
- Schedule Execution Activities
- Confirm Schedule

Planning

- Submit VADR specific documents and network diagram
- Schedule assessment planning meeting
- Submit network configurations, logs, and packet captures
- Interviews with key personnel

Execution

- Review submitted architecture
- Analyze packet captures

Post-Execution
- Out-brief – provides initial findings
- Final report (approximately 4 weeks)
- Follow-up on remediation actions – 180 days

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.

RISK AND VULNERABILITY ASSESSMENT

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

CISA Assessments' 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 Assessments 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 Assessments 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

ASSESMENT 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 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.

REMOTE PENETRATION TESTING

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

CISA Assessments' 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 less costly and more scalable than on-site offerings; however, it is more limited in organizational insight and context.

SCENARIOS

External Penetration Test: Verifying 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; the test can include automated scanning, manual testing, or a combination of both methods.

Phishing Assessment: Testing through carefully crafted phishing emails containing a variety of malicious payloads to the trusted point of contact.

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's mission, operation, and network infrastructure.

ASSESMENT TIMELINE

Pre-Planning

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

Planning

- Confirm schedule
- Establish trusted points of contact

- Determine RPT services, scope, and logistics during pre-assessment call(s)

Execution (Up to Six Weeks)

- Dependent on resource availability
- Critical findings are immediately disclosed

Reporting

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

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.

RED TEAM ASSESSMENT

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

CISA Assessments' Red Team Assessment (RTA) is a comprehensive evaluation of an information technology (IT) environment. Simulation of advanced persistent threats (APTs) can assist stakeholders in determining their security posture by testing the effectiveness of response capabilities to a determined adversarial presence. RTAs are crafted specifically to test the people, processes, and technologies defending a network.

ASSESSMENT PHASES

Threat Simulation: CISA Assessments simulate APT tactics, techniques, and procedures using publicly available tools and data to access, navigate, and persist in a stakeholder's environment.

Measureable 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 stakeholder's network is determined by observable response-driven metrics.

ASSESSMENT OBJECTIVES

- Evaluate people, processes, and technologies responsible for defending the stakeholder's network.
- Provide stakeholder executives actionable insight to their cybersecurity posture and practical training for technical personnel.

ASSESMENT TIMELINE

Pre-Planning

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

Planning

- Confirm schedule
- Define scope
- Establish trusted points of contact

Execution (90 Days)

- Open-source intelligence
- Simulate APT
- Security response testing through activation of measurable Events

Post-Execution

- On-site out-brief and training

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.

CRITICAL PRODUCT EVALUATION

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

CISA Assessments' Critical Product Evaluation (CPE) is a multi-week, comprehensive evaluation of a vendor's solution or appliance that ubiquitously supports critical infrastructure operations or other national endeavors to improve the "out of the box" and recommended security implementation of the product, ultimately improving our national resiliency.

ASSESSMENT OBJECTIVES

- Enumerate the vulnerabilities associated with the product's in-scope software, firmware, hardware
- Attempt exploitation of vulnerabilities that present the greatest risk using known exploits, or, if practical, develop new code or technique
- Capture indicators-of-compromise information to help incident responders determine the existence or extent of an incident
- Capture assessment methods
- Assist in developing remediation or mitigation strategies.

ASSESSMENT PHASES AND TIMELINE

Pre-Planning
- Request assessment
- Receive CPE brief
- Sign and return documents

Planning
- Define scope and confirm schedule
- Coordinate delivery of the system(s)-under-test (SUT)

Execution (Tailored*)
- Check-in and Configuration: setup and configure for normal operation

- Enumeration: list software and hardware interfaces
- Deconstructive Testing: mapping the attack surface and developing threat scenarios
- Target Analysis: execute attack vector testing and attempt exploitation

Post-Execution
- Coordinate SUT return**
- Report generation
- Out-brief with evaluation team

* Length of time for a CPE is based on the complexity of the SUT. Generally, eight-weeks is the starting point, however, this time can be amended during the scoping meetings or during the course of the evaluation.

** Equipment may become damaged during the course of testing.

ABOUT CISA ASSESSMENTS

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.

Hunt and Incident Response Team (HIRT)

THE NATIONAL CYBERSECURITY & COMMUNICATIONS INTEGRATION CENTER (NCCIC) OPERATES AT THE INTERSECTION OF THE PRIVATE SECTOR, CIVILIAN, LAW ENFORCEMENT, INTELLIGENCE, AND DEFENSE COMMUNITIES, APPLYING UNIQUE ANALYTIC PERSPECTIVES, ENSURING SHARED SITUATIONAL AWARENESS, AND ORCHESTRATING SYNCHRONIZED RESPONSE EFFORTS WHILE PROTECTING THE CONSTITUTIONAL AND PRIVACY RIGHTS OF AMERICANS IN BOTH THE CYBERSECURITY AND COMMUNICATIONS DOMAINS.

The NCCIC HIRT provides expert intrusion analysis and mitigation guidance to clients who lack in-house capability or require additional assistance with responding to a cyber incident. HIRT supports federal departments and agencies, state and local governments, the private sector (industry and critical infrastructure asset owners and operators), academia, and international organizations.

NCCIC HIRT performs both on-site and remote cybersecurity incident response. A typical engagement includes log, network traffic, and host analysis. The goal is to discover malicious actors, acquire, and analyze the malicious tools, and provide mitigation guidance.

NCCIC HIRT is uniquely positioned with knowledge of both unclassified and classified actor tactics, techniques, and procedures compiled from public and private sector partners. HIRT works closely with law enforcement, the intelligence community, and international partners to provide a coordinated and comprehensive response. The NCCIC HIRT provides on-site support for numerous large-scale engagements each year, covering a wide variety of organizations.

HUNT

The goal of a hunt is to use tools and techniques to proactively check for and mitigate against malicious actor activity. More specifically, it will be charged to search for exploitation tools, tactics, procedures and their associated artifacts. Performed from within the customer environment on internal networks and hosts, it will encompass any systems that were identified by a Risk Review. Hunts are scoped to those systems that are part of a risk vetting process. The initial hunt will be targeted and precise, but results of an initial analysis may warrant the expansion of its scope to include additional systems, segments or environments. Ultimately, the analysis will further measure potential risks to the integrity, confidentiality, and availability of systems that need immediate attention. If evidence of a potential compromise is recognized, the Incident Response Team (IRT) will review agency materials and conduct interviews with technical staff, management, and senior leadership to further understand possible security gaps, thus allowing for more effective mitigation. As part of this mitigation response, a document incorporating actionable guidance will be provided.

INCIDENT RESPONSE

If evidence of a potential compromise is recognized, the Incident Response Team (IRT) will review agency materials and conduct interviews with technical staff, management, and senior leadership to further understand possible security gaps, thus allowing for more effective mitigation. As part of this mitigation response, a document incorporating actionable guidance will be provided.

TOOLS, TECHNIQUES, AND ARTIFACTS

A hunt and incident response will utilize tools, techniques, and artifacts to determine where a system has been compromised. They are listed as follows:

- Existing documentation to include policies, procedures and processes
- System owner interviews

- Existing customer documentation
- Host-based analysis
- Review of existing customer logs

- Network traffic analysis
- Network infrastructure analysis
- Data mappings and other diagrams

ADVANTAGES

- HIRT improves in-house lab capabilities and onsite processes
- HIRT utilizes defined, repeatable processes

- HIRT leverages total HIRT, US-CERT, ICS-CERT, and NCCIC capabilities to assist the client
- HIRT is able to create customized mitigation plan for the client

SERVICE OFFERINGS

The HIRT works onsite and remotely to provide services to eligible clients. All of the following are offered on a voluntary basis:

Incident Triage: Process taken to scope the severity of an incident and determine required resources for action

Network Topology Review: Assessment of network ingress, egress, remote access, segmentation, and interconnectivity, with resulting recommendations for security enhancements

Infrastructure Configuration Review: Analysis of core devices on the network which are or can be used for network security (e.g., prevention, monitoring, or enforcement functions)

Log Analysis: Examination of logs from network and security devices to illuminate possible malicious activity

Incident Specific Risk Overview: Materials and in-person briefings for technical, program manager, or senior leadership audience; cover current cyber risk landscape, including classified briefings to cleared staff when appropriate

Hunt Analysis: Deployment of network hunting tools to proactively detect indicators of compromise (IOC)

Security Program Review: A review of the client's existing security roles, responsibilities, and policies to identify possible organizational or information-sharing gaps

Malware Analysis: Reverse engineering of malware artifacts to determine functionality and build indicators

Mitigation: Actionable guidance to improve the organization's security posture, including incident-specific recommendations, security best practices, and recommended tactical measures

Digital Media Analysis: Technical forensic examination of digital artifacts to detect malicious activity and develop further indicators

Control Systems Incident Analysis: Analysis of supervisory control and data acquisition devices, process control, distributed control, and any other systems that control, monitor, and manage critical infrastructure

SEND REPORTS TO NCCIC

HIRT encourages reports of cybersecurity incidents, possible malicious code, vulnerabilities, and phishing attacks. Submit a report via phone: 1-888-282-0870 or email: *NCCICCustomerService@hq.dhs.gov*.

CYBERSECURITY ASSESSMENTS SUMMARY

Name	Validated Architecture Design Review (VADR)	Phishing Campaign Assessment (PCA)	Vulnerability Scanning (Formally Cyber Hygiene)	Remote Penetration Test (RPT)	Network Risk and Vulnerability Assessment (RVA)
Purpose	Provide analysis and representation of asset owner's network traffic, data flows, and device relationships and identifies anomalous communications flows.	Measure the susceptibility of an organization's personnel to social engineering attacks, specifically email phishing attacks.	Identify public-facing Internet security risks, through service enumeration and vulnerability scanning	Perform external penetration testing and security services to identify risks and externally exploitable pathways into systems, networks and applications.	Perform penetration testing and security services to identify risks and vulnerabilities within IT systems, networks and applications
Scope	Industrial Control Systems / Network Architecture/ Network Traffic	Organization / Business Unit / Email Service	Public-Facing, Network-Based IT Service	Organization / Business Unit / Network-Based IT Service	Organization / Business Unit / Network-Based IT Service
Time to Execute	Variable (Hours to Days)	Approximately 6 Weeks	Continuous	Up to 6 weeks	Two weeks of testing
Information Sought	Network design, system configurations, log files, interdependencies, and its applications	Phishing "click rate" metrics compared to attack sophistication	Network service and vulnerability information	Network, Database, Application scope and/or access to be tested with various security tools	Network, Database, Application scope and/or access to be tested with various security tools
Preparation	Coordinated via Email. Planning calls	Formal rules of engagement and pre-planning	Signed agreement letter and IP address scope to be tested	Formal rules of engagement and extensive pre-planning	Formal rules of engagement and extensive pre-planning
Participants	Control system operators/ engineers, IT personnel, and OT personnel	IT/Security Manager, Network Administrators, end users	IT/Security Manager and Network Administrators	Management stakeholders, IT/Security Manager, Network Administrators & System Owners.	Management stakeholders, IT/Security Manager, Network Administrators, and System Owners.
Delivered By	Contact the Cybersecurity Advisor mailbox at cyberadvisor@hq.dhs.gov for more information or to request services				