CISA

CYBERSECURITY SERVICES AND RESOURCES FOR YOU

Mark Robinson, Federal Lead
Vulnerability Management

CISA Defends against today's threats & collaborates to build a more secure tomorrow

VISION

Secure and resilient infrastructure for the American people.

MISSION

Lead the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure.

GOAL 1

CYBER DEFENSE

Spearhead the national effort to ensure defense and resilience of cyberspace

GOAL 2

RISK REDUCTION AND RESILIENCE

Reduce risks to, and strengthen resilience of, America's critical infrastructure

GOAL 3

OPERATIONAL COLLABORATION

Strengthen whole-of-nation operational collaboration and information sharing

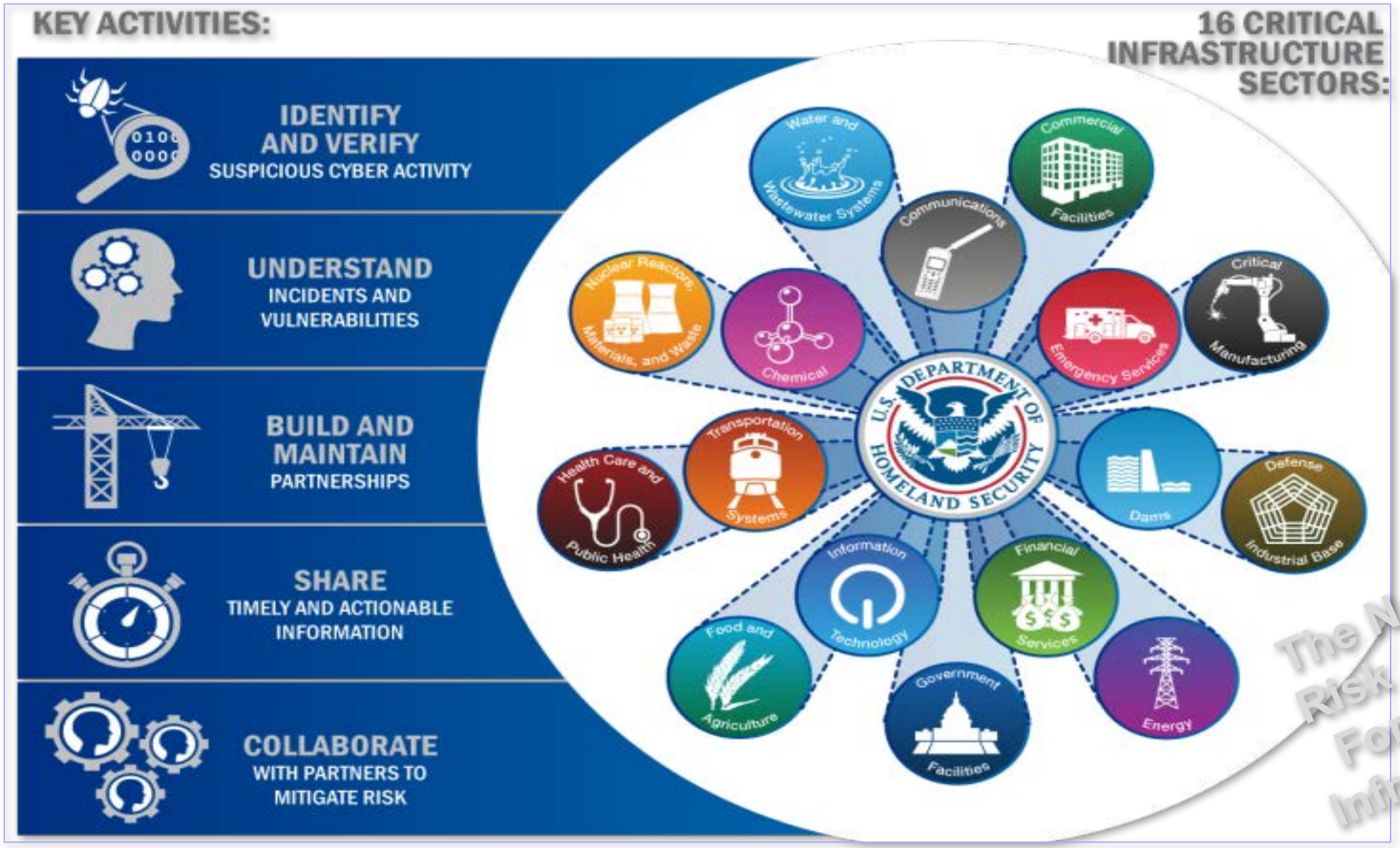
GOAL 4

AGENCY UNIFICATION

Unify as One CISA through integrated functions, capabilities, and workforce

Core Principles & Values

Serving Critical Infrastructure

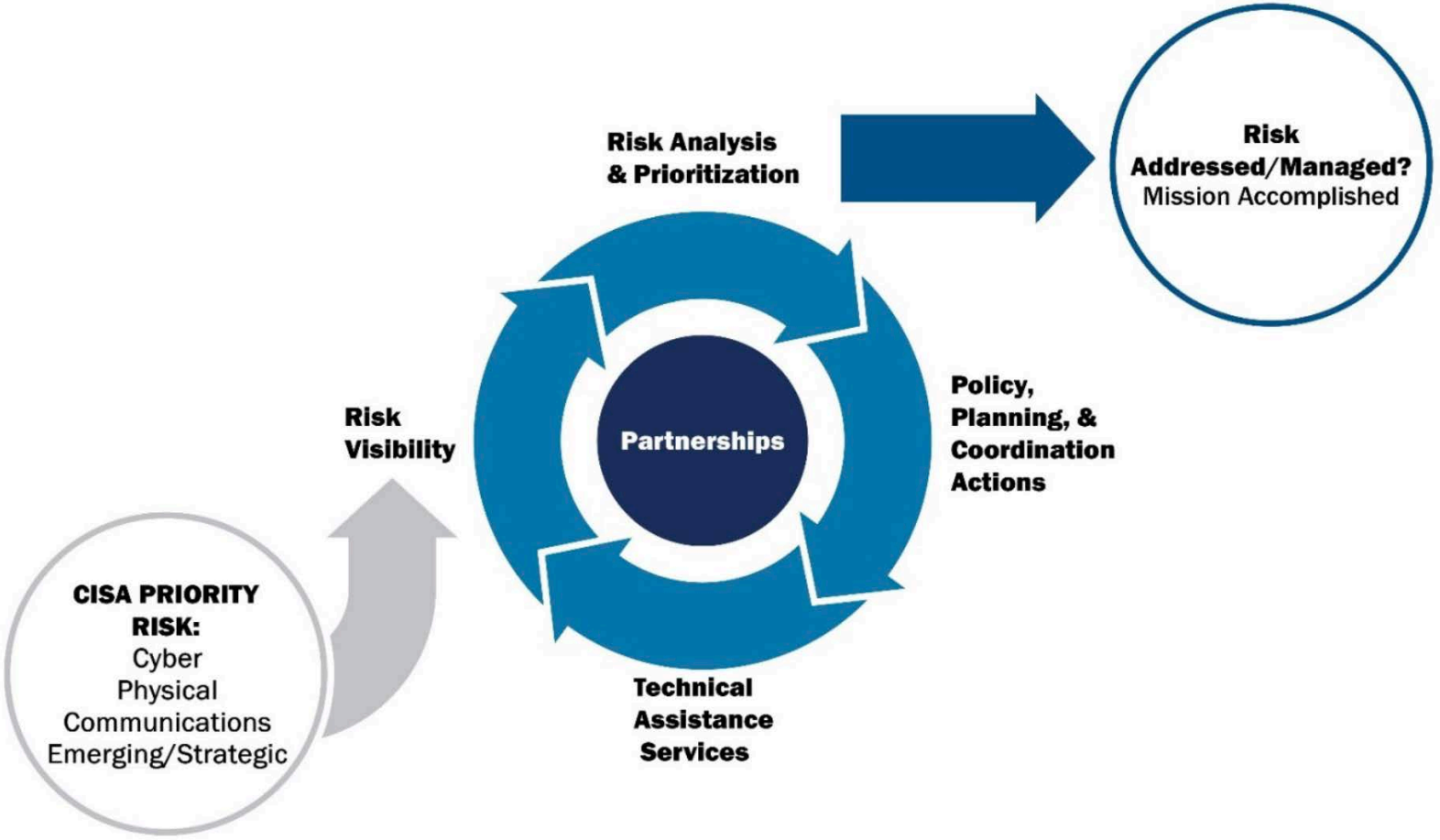


The Nation's Risk Advisor For Critical Infrastructure

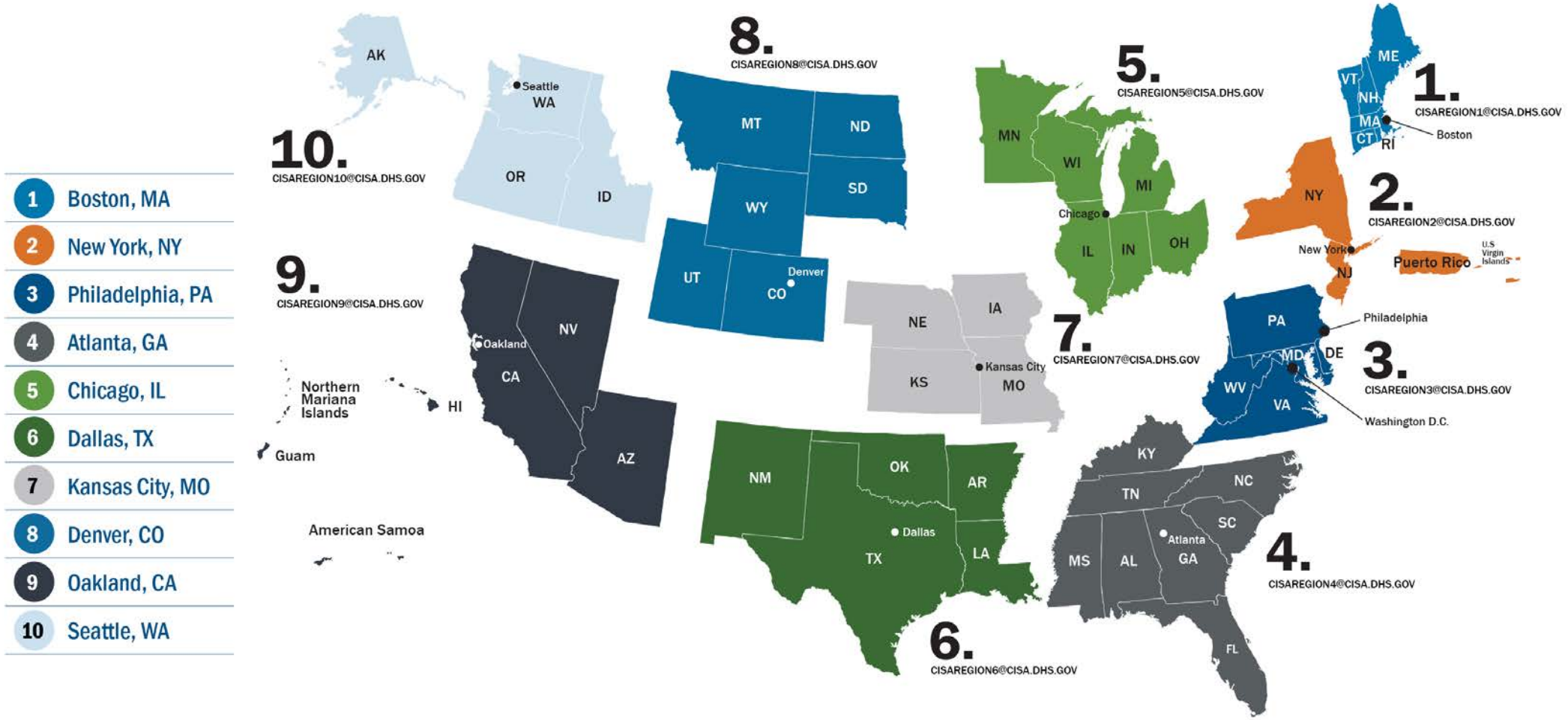
Shared Mission Space

Operating Model

Manage priority risks to critical infrastructure



Field Regions

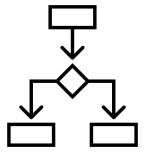


Cybersecurity Responsibilities

Information sharing and collaboration

Technical Assistance

Protecting federal civilian executive-branch information and information systems

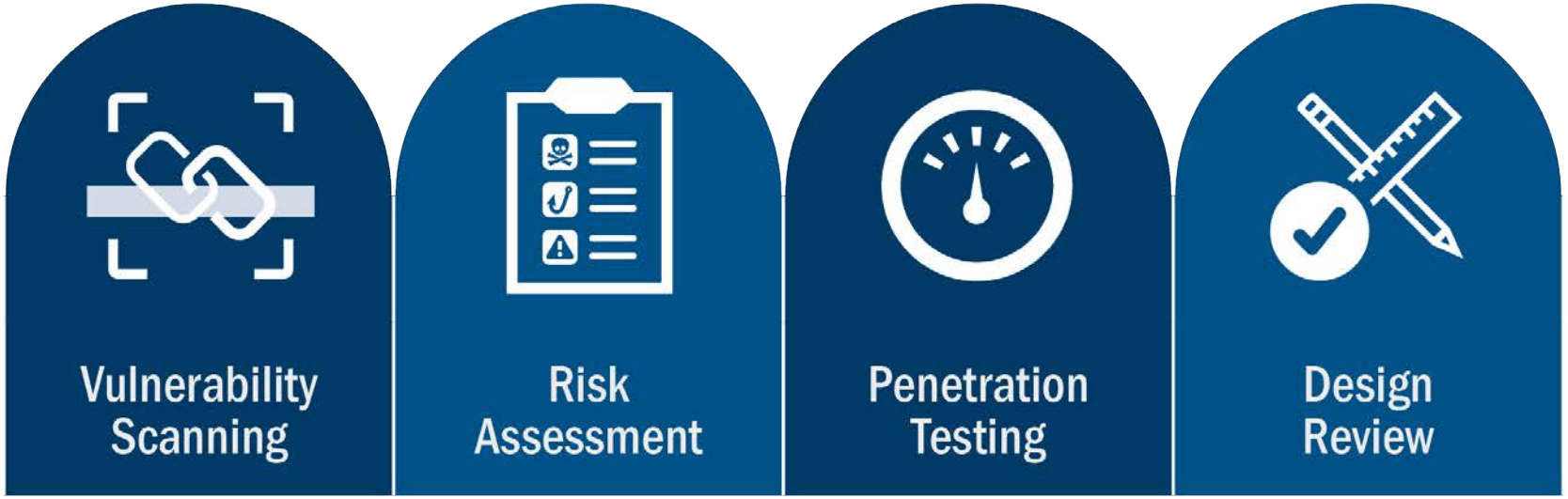


Cyber incident response coordination; planning

Cyber workforce development and education

Cyber Assessment Services

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



Core Capabilities

Service Catalog

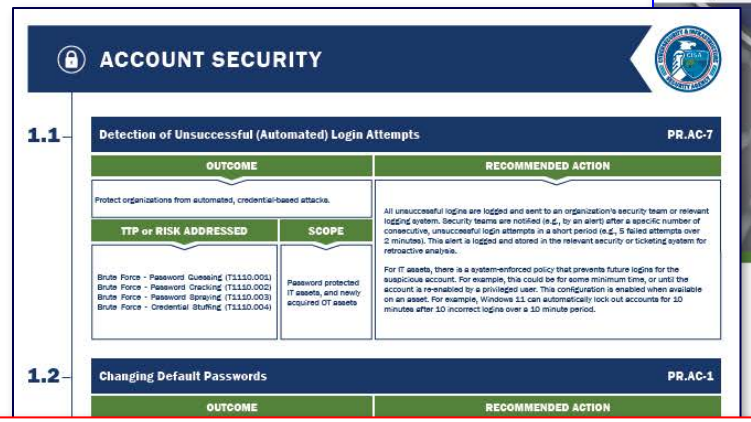
- Vulnerability Scanning (Cyber Hygiene)
- Phishing Campaign Assessments
- Posture and Exposure Monitoring
- Risk and Vulnerability Assessments
- Web Application Scanning
- Remote Penetration Testing
- Red Team Assessments
- Validated Architecture Design Review
- Security Architecture Review
- Critical Product Evaluation

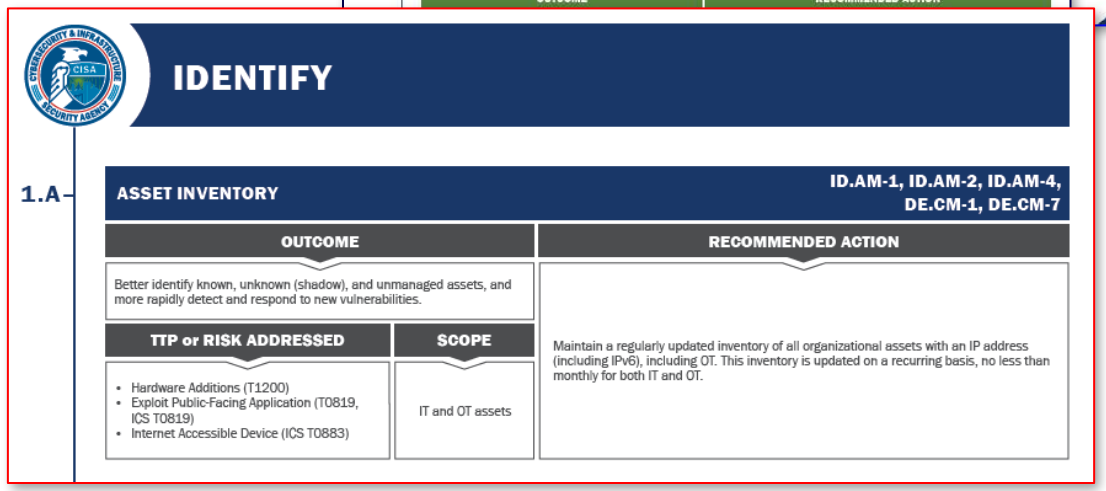
CISA CYBER PERFORMANCE GOALS (CPG)

CISA Cybersecurity Performance Goals (CPG)

A baseline set of cybersecurity practices broadly applicable across critical infrastructure with **known risk-reduction value**.

- 38 topic areas
- Takes about an hour to complete
- Completely **voluntary**
- To help **establish** a common set of **fundamental cybersecurity practices** for critical infrastructure, or anyone
- Help organizations **kickstart their cybersecurity efforts**
- Resides within the CSET





Voluntary
Not Comprehensive
Known risk-reduction

cisa.gov/cpg

CISA

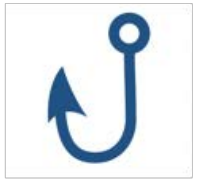
CYBER HYGIENE (CYHY)

What is Cyber Hygiene?

Our Mission: Enhance situational awareness and enable efforts to reduce risk and increase national resilience

- Reduce stakeholder risk by helping organizations understand their exposure
- Support national resilience through the proactive identification of vulnerabilities
- Inform national risk management efforts and policy decisions
- Enable data driven decisions across the government and industry alike

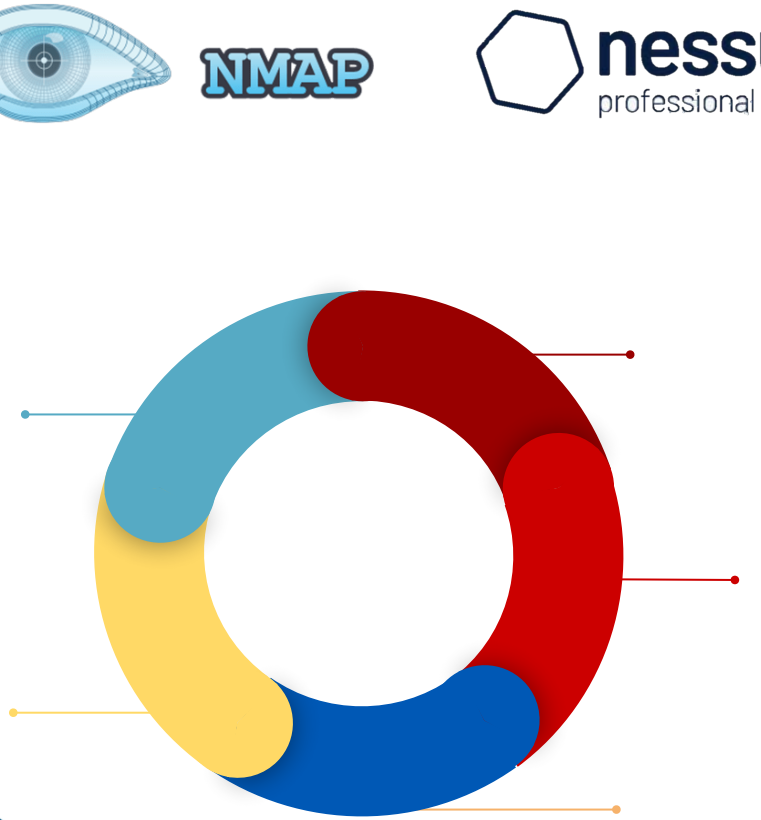
- Cost free! No charge! Yes, really!



A CyHy VS Overview

- Proactive identification of weaknesses directly accessible for exploitation by an external party from the Internet
  - Continuous scanning to monitor external network
  - Scope currently targets public, static IP addresses
  - Discover how your organization looks from the perspective of an attacker
- Key takeaways:
  - Internet-accessible vulnerabilities
  - Potentially risky services
  - Unsupported software

The CyHy VS Methodology



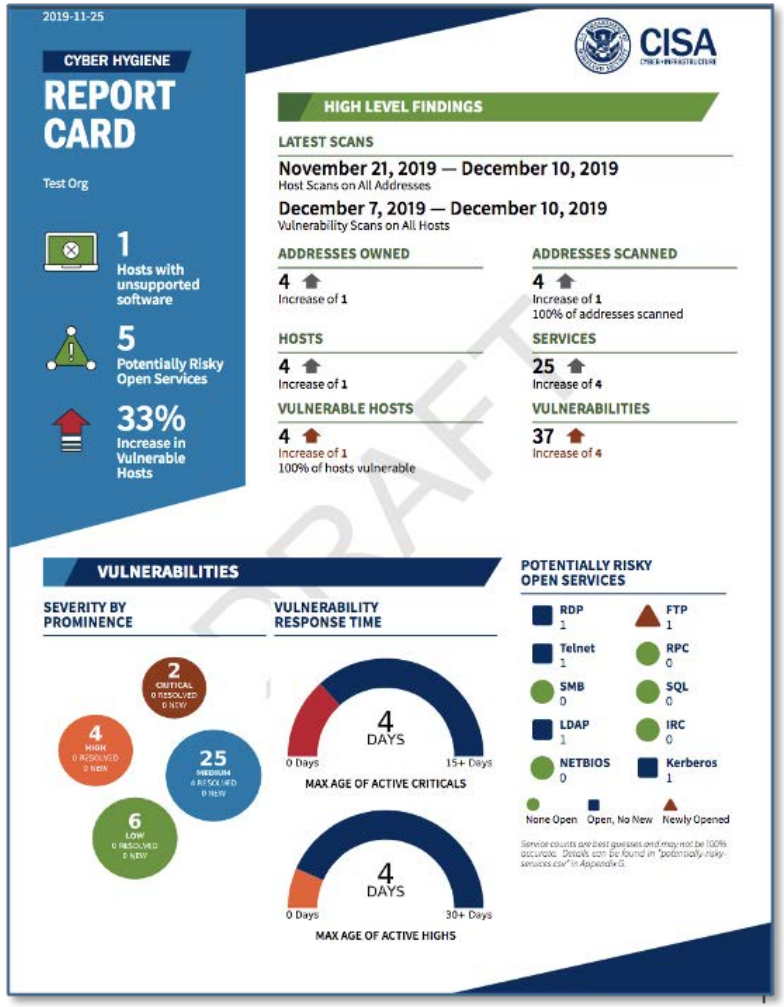
- (Nmap) – Port scanning to find open ports and listening services
- (Nessus) – Vulnerability scanning to check identified systems against a library of vulnerabilities that an Internet-based actor could exploit

Note: IPs with no open ports/ listening services are port scanned only every 90 days to check for changes in host status

CyHy VS Reports

- Weekly Reports
  - Password-protected PDF
  - High-level summary “Report Card”
  - Filterable/ingestible CSV attachments
  - Sub-organization breakdown (if requested)
- Ad-Hoc Alerts within 24 hours of detecting:
  - New critical/high vulnerabilities
  - New known exploited vulnerabilities
  - Newly available potentially risky services

We recommend creating a distribution list to receive reports so that you can control who receives them.



CISA

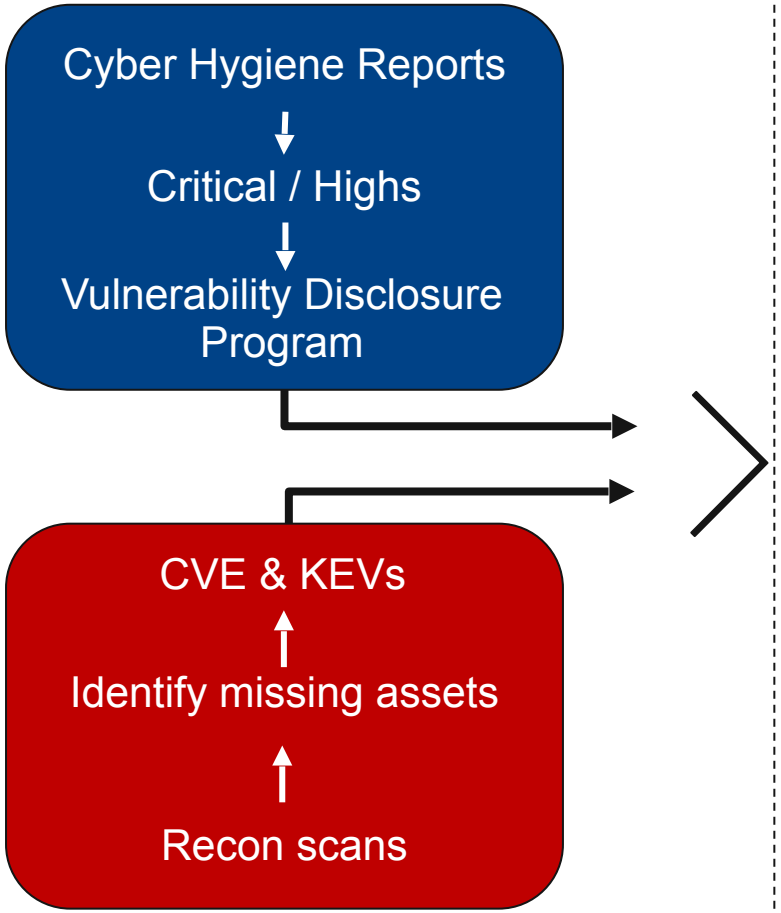
FEDERAL ATTACK SURFACE TESTING (FAST)

Overview

- Attack surface management through continuous hands-on testing of internet-facing Federal assets
- Identify web application misconfigurations missed by vulnerability scanners and automated web-application testing
- Re-testing to validate remediation

Assessment Model

TLP:WHITE



- Full verified footprint in scope
- Emphasis on Critical / High findings
- Emphasis on Known Exploited Vulnerabilities (KEVs)
- Validation of previous findings

Methodology

- Scans are rate-limited, not as “low and slow” as a red team
  - Alerts may be generated
  - Overnight
- Don’t solely rely on automated scans
  - Burp’s Active Scanner
  - Directory Enumeration (feroxbuster, wfuzz, gobuster, etc.)
  - Subdomain enumeration (amass, cert.sh, etc.)
  - Custom scripts
- Manual testing and analysis of web applications
  - Create accounts the public can

CISA

REMOTE PENETRATION TEST (RPT)

Services

- Open-Source Information Gathering
- Network Penetration Test
- Web Application Assessment
- Phishing Assessment (Infrastructure Only)

Services – Open-Source Information Gathering

- Network Presence (size and location)
- Email Addresses
- Breach Information
- Credentials (email address and password)
- Validation

Services – Network Penetration Test

- System Identification
- Network Service Identification
- Broad-based Vulnerability Scanning
- Specialized Tools
- Analysis and Manual Testing

- Targeting underlying operating system (no internal operations)

Services – Web Application Assessment

- Web Servers and Web Applications
- Web applications typical have:
  - Authentication mechanism (ie Login Page)
  - Underlying Database
  - Used by Non-Administrators (ie Portals, not CMS)
  - Not COTS products (ie VPN, OWA, Citrix, etc)
- 2 sets of credentials (per non-administrative role per web application)
- Third party web sites can be included

- Targeting underlying database (and sensitive information)

Services – Phishing Assessment (Infrastructure Only)

- NOT a Social Engineering Exercise
- Testing Criteria
  - Introduce malicious code to the environment/workstation
  - Successfully execute malicious code
  - No changes will be made to the workstation/environment

CISA

RED TEAM ASSESSMENT (RTA)

Red Team Methodology

RED TEAM ASSESSMENT

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

CISA Cyber 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.

Red Team Tactics

ASSESSMENT PHASES

Threat Emulation: CISA Assessments emulate APT tactics, techniques, and procedures using publicly available tools and data to access, navigate, and persist in a stakeholder'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 stakeholder's network is determined by observable response-driven metrics.

ASSESSMENT OBJECTIVES

- Evaluate an organization's defensive team on how they utilize people, processes, and technologies to protect, detect, and respond to cyber threats.
- Provide organizational leadership with actionable insight to their cybersecurity posture and practical training for technical personnel.

Red Team Timeline

ASSESSMENT TIMELINE

Planning

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

CISA
VALIDATION AND ARCHITECTURE REVIEW (VADR)

VADR Assessment Overview

- A collaborative proactive assessment to evaluate the cyber risks associated with the system(s) being assessed.
- An unbiased, third-party review of the operational technology (OT) environment cybersecurity posture.
- Aims to determine whether the system owner has adequately identified, evaluated, and managed the risks to the OT environment.
- Verifies that the customer fully understands the risks that are inherent in their cybersecurity solution.

VADR Activities

- CISA analyzes the following documents to gain an understanding of the network architecture and tailor the technical discussions:
  - Network Architecture Diagram(s)
  - HW/SW Asset Inventory
  - Network System Configuration(s)
  - Packet Capture (PCAP) Data
- Conduct open-source intelligence research
- Conduct technical interviews to provide CISA with a complete operational picture of the cybersecurity program

VADR Process

Planning

~30 days

- ❑ Assessment Planning Meeting ~2-3 hours
  - Review Network Diagrams
  - Confirm Assessment Scope
  - Discuss Packet Capture locations
  - Identify Configurations Required
- ❑ Data Collection/Submission
  - Packet Captures
  - Network Device Configurations
  - Asset Inventory
  - Other artifacts as agreed upon with CISA Assessment Team

Execution

~3-4 days

- ❑ Overview of Systems
- ❑ Review Network Architecture Validation
- ❑ Review Open-Source Information
- ❑ Interviews with Key Personnel
- ❑ Out-Brief

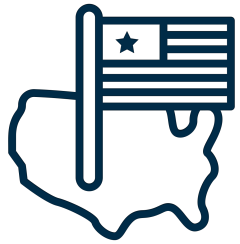
Post Execution

Incremental

- ❑ After 1-Month
  - Final Report Delivery
  - Customer Satisfaction Survey I (10-20 min)
- ❑ After 6-Months
  - Remediation Follow-up Meeting/Discussion (2-3 hours)
  - Customer Satisfaction Survey II (10-20 min)

CISA RISK AND VULNERABILITY ASSESSMENT (RVA)

What it is



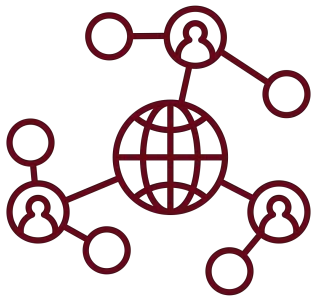
- Flagship assessment service for CISA
- Holistic penetration test scoped to the entire organization
- Informs organizations on the effect of their assumed risk
- RVA is significantly more advanced than vulnerability scans, but doesn't evade security products like a Red Team
- Serves the entire Nation (private and public sectors)
- 90-day follow up

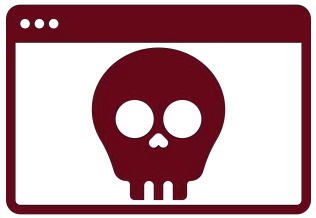
RVA vs Vulnerability Scan

- RVAs utilize vulnerability scans to assist in what to target
- Vulnerability scans assign risk without consideration to whether exploits exist
- RVA must demonstrate an effect of the vulnerability to assign risk
- Vulnerability scans cannot easily assess complex risk stemming from weak network protocols, files on shares, or Active Directory
- RVAs result in zero false positives

Methodology

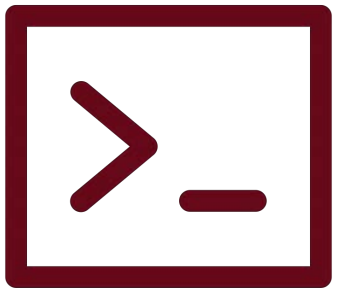
- Two (2) week penetration test (non-negotiable)
  - One (1) week external
  - One (1) week internal
- **External**: Publicly-accessible endpoints; web applications; phishing
- **Internal**: Network protocol analysis; password analysis; endpoint analysis; Active Directory analysis; role-based permission analysis; data exfiltration analysis; ransomware susceptibility, wireless analysis and much more!
- Discover and demonstrate the effects of as many vulnerabilities as possible within the timeframe

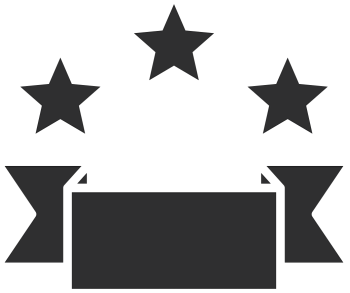


RVA Phishing

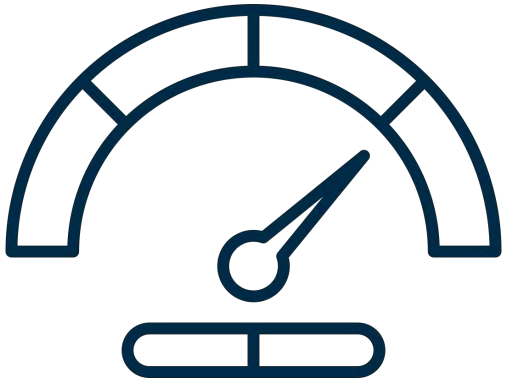
- Demonstrable risk! Not click rate…
- Click rate phishing doesn't educate organizations of their true risk.
- Minimum number of clicks to phish a user: THREE (3)
- RVA creates realistic, customized payloads for each organization
- When users fall victim to RVA phishing, RVA team gains remote access (real risk)
- RVA team demonstrates weakness and affect of the weakness



Risk Score



- Curious how your organization compares to your peers?
- Tired of subjective risk?
- New in FY24, RVAs are utilizing a proprietary risk score to quantify risk
- Risks are scored individually, but the organization also receives a risk score
- Allows RVA to compare customers across the Nation
- Vulnerabilities are scored based upon:
  - What adversaries stand to gain from the vulnerability
  - Known adversary targeting of the vulnerability
  - Occurrence of the vulnerability within the organization



CISA FREE RESOURCES ON CISA.GOV

Shields Up

Shields Up: Guidance for Families

Every individual can take simple steps to improve their cyber hygiene and protect themselves online. Here are 4 things you can do to keep yourself cyber safe.

Shields Up: Guidance for Organizations

CISA recommends all organizations—regardless of size—adopt a heightened posture when it comes to cybersecurity and protecting their most critical assets. Take these recommended actions.

Shields Up: Guidance for Corporate Leaders and CEOs

Corporate leaders have an important role to play in ensuring that their organization adopts a heightened security posture. CISA urges all senior leaders, including CEOs, to take these steps.

Services

Access Control Policies/Procedures Consultation & Documentation

Design and document system access control processes and procedures that comply with federal guidelines.

INCREASE YOUR RESILIENCE | FOUNDATIONAL

Account Management

Ensure that a concept of separation of duties is implemented and logical access controls and account lockout/disabling controls are in place.

ASSESS YOUR RISK LEVEL | INTERMEDIATE

Analysis & Detection

Ensure your agency's or division's information security program is fully implemented and maintained with Analysis and Detection services.

INCREASE YOUR RESILIENCE | FOUNDATIONAL

Anti-Phishing Training Program Support

Comprehensive support to establish and operate an anti-phishing program, which includes employee awareness and training, simulated attacks, and results analysis to inform training modifications and mitigate the risk of phishing attacks against an enterprise.

INCREASE YOUR RESILIENCE, ASSESS YOUR RISK LEVEL | FOUNDATIONAL

Assist Visits

CISA Assist Visits help critical infrastructure owners and operators understand the importance of their facility, how their service fits into a critical infrastructure sector, and the CISA resources available to enhance their security and resilience.

Cyber Resource Hub

Cyber Resource Hub

The Cybersecurity and Infrastructure Security Agency offers a range of cybersecurity assessments that evaluate operational resilience, cybersecurity practices, organizational management of external dependencies, and other key elements of a robust and resilient cyber framework. These professional, no-cost assessments are provided upon request on a voluntary basis and can help any organization with managing risk and strengthening the cybersecurity of our Nation's critical infrastructure.

Assessment Evaluation and Standardization

The Cybersecurity and Infrastructure Security Agency (CISA) Vulnerability Management team offers the Assessment Evaluation and Standardization (AES) program that is available to federal, state, local, tribal and territorial governments, critical infrastructure, and federal agency partners. The program is designed to enable organizations to have a trained individual that can perform several cybersecurity assessments and reviews in accordance with industry and/or federal information security standards.

For more information on the AES program, visit cisa.gov/aes

Vulnerability Scanning

Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPv4s for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts.

For more information on this service and how to sign up, visit the Cyber Hygiene Services page.

Cyber Resilience Review

The Cyber Resilience Review (CRR) is an interview-based assessment that evaluates an organization's operational resilience and cybersecurity practices. This assessment is derived from the CERT Resilience Management Model (CERT-RMM), a process improvement model developed by Carnegie Mellon University's Software Engineering Institute for managing operational resilience. The Cyber Resilience Review evaluates that maturity of an organization's capacities and capabilities in performing, planning, managing, measuring, and defining cybersecurity capabilities across the following 10 domains:

Reducing the Likelihood of a Damaging Cyber Incident

Service	Skill Level	Owner	Description	Link
FortifyData	Basic	FortifyData	Quarterly vulnerability assessments that include automated attack surface assessments with asset classification, risk-based vulnerability management and security rating. The FortifyData all-in-one cyber risk management platform also offers third party cyber risk management.	Free Plan - FortifyData
OpenVAS	Basic	Greenbone	This is a vulnerability scanner and capabilities include unauthenticated and authenticated testing, various high-level and low-level internet and industrial protocols, performance tuning for large-scale scans and a powerful internal programming language to implement any type of vulnerability test.	OpenVAS - Open Vulnerability Assessment Scanner
Network Reporting	Basic	ShadowServer	A subscription service that sends custom remediation reports to inform organizations about the state of its networks and security exposures.	Network Reporting | The Shadowserver Foundation
Vulcan Cyber	Basic	Remedy Cloud	A searchable database of remedies and fixes for thousands of known vulnerabilities. It also provides	https://vulcan.io/remedy-cloud/

Free Cybersecurity Services & Tools

Reducing the Likelihood of a Damaging Cyber Incident

Service	Skill Level	Owner	Description	Link
FortifyData	Basic	FortifyData	Quarterly vulnerability assessments that include automated attack surface assessments with asset classification, risk-based vulnerability management and security rating. The FortifyData all-in-one cyber risk management platform also offers third party cyber risk management.	Free Plan - FortifyData
OpenVAS	Basic	Greenbone	This is a vulnerability scanner and capabilities include unauthenticated and authenticated testing, various high-level and low-level internet and industrial protocols, performance tuning for large-scale scans and a powerful internal programming language to implement any type of vulnerability test.	OpenVAS - Open Vulnerability Assessment Scanner
Network Reporting	Basic	ShadowServer	A subscription service that sends custom remediation reports to inform organizations about the state of its networks and security exposures.	Network Reporting | The Shadowserver Foundation
Vulcan Cyber	Basic	Remedy Cloud	A searchable database of remedies and fixes for thousands of known vulnerabilities. It also provides highlight trend analytics such	https://vulcan.io/remedy-cloud/

CISA

CYBER+INFRASTRUCTURE

Questions?

For more information:

vulnerability@cisa.dhs.gov


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY