# STATE OF INFRASTRUCTURE SECURITY

## CISA CYBER ASSESSMENTS

**Jason Hill**
September 23, 2021

# Introduction: Jason Hill

- Chief of CISA Cybersecurity Assessments
- Former head of DHS Red Team
- 20 years Army National Guard Cyber

# CISA and VM Overview

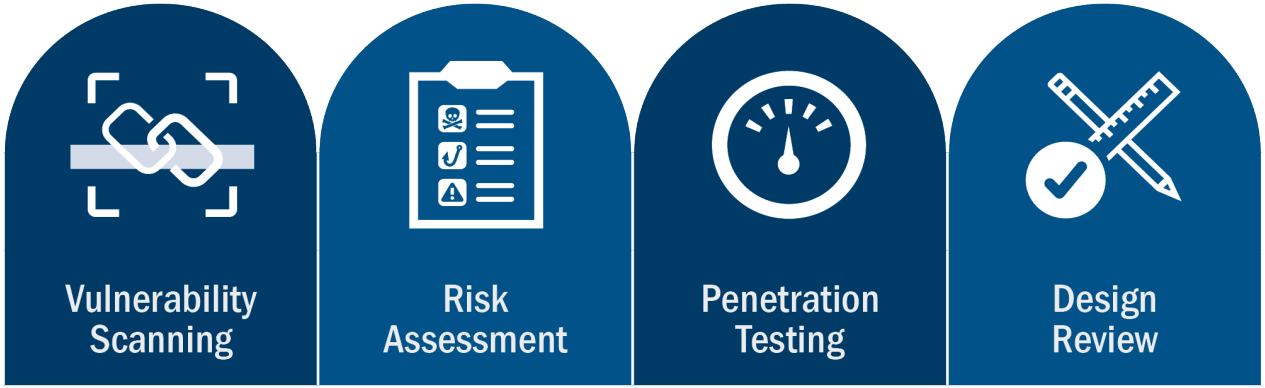
- **CISA** builds the national capacity to defend against cyber attacks and works with the federal government to provide cybersecurity tools, incident response services and assessment capabilities

- **Vulnerability Management** aims to reduce risks and gain insights on vulnerabilities in Federal, State, Local, Tribal, Territorial, and Private Critical Infrastructure customers.

# Cyber Assessments Overview

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

- Proactive services to government and critical infrastructure clients to assess and improve cybersecurity posture, understand risk, and identify operational strengths and weaknesses
- The team also provides an objective third-party perspective of stakeholder operational cybersecurity posture




## Core Capabilities

*Services are provided at "no cost" to our customers*

*Our "payment" is authorization to use anonymized, non attributable, data to enhance national situation awareness and enable our stakeholders to make data driven decisions*

# Goals

## IDENTIFY AND ELIMINATE

Identify and eliminate remote attack paths prior to their exploitation

## CHAMPION AND PROMOTE

Champion and promote data-driven standards, policies, guidelines and capabilities

## MONITOR

Monitor secure deployment and implementation of infrastructure components

## DRIVE

Drive implementation and adoption of mature operational capabilities and behaviors

## ENSURE

Ensure that no single customer receives a disproportionate amount of resources and that all 16 critical infrastructure sectors receive CISA services

# Service Catalogue

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

# Risk and Vulnerability Assessment

- **One-on-one engagements** with customers that combine national threat and vulnerability information with data collected and discovered through onsite assessment activities.
- Service components include **scenario-based network penetration testing, web application scanning, social engineering** in the form of a phishing email, wireless testing, database scanning, and internal threat emulation.
- **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.
- **Provides customers risk analysis reports** with actionable remediation recommendations prioritized by risk.
- **2-week engagement** – one week from Arlington, VA lab. One week onsite at customer location.

# Validated Architecture Design Review

- Assessment based on federal and industry standards, guidelines, and best practices conducted on **Information Technology (IT) or Operational Technology (OT) Infrastructures**.
- **Includes an in-depth Architecture Design Review** and a review of interconnectivity to internal and external systems with a focus 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** to identify anomalous communications, indicative of vulnerabilities.

# RVA/VADR 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.
- Creates sector and mission reporting and analytics.

# RVA/VADR Assessments Conducted

- Fiscal Year 2020 - Present

| Sector | RVA Assessments | VADR Assessments |
|---|---|---|
| Energy | 6 | 41 |
| Agriculture | 1 | 1 |
| Government Facilities | 69 | 10 |
| Health | 22 | 7 |
| IT | 17 | 2 |
| Manufacturing | 2 | 1 |
| Transportation | 3 | 16 |
| Water | 14 | 5 |

# RVA/VADR Trends and Findings

VADR findings across all sectors, 2021

| Finding | Occurrences |
|---|---|
| Boundary Protection | 70 |
| Least Functionality | 31 |
| Information Systems Partitioning | 24 |
| Allocation of Resources | 20 |
| Information System Backup | 19 |
| Identification and Authentication (organizational users) | 17 |
| Monitoring Physical Access | 14 |
| Access Control for Mobile Devices | 11 |
| Authenticator Management | 11 |
| Physical Access Control | 11 |

# Ransomware

- Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable.
- In recent years, ransomware incidents have become increasingly prevalent.
- Ultimately, ransomware is *not a vulnerability*, it is instead an outcome of existing attack vectors.

# Current Ransomware Examples

- The May 2021 Colonial Pipeline Attack:

  A ransomware attack resulted in the halting of pipeline operations. Colonial paid out $4.4 million to the hackers. $2.3 million was eventually recovered. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

- The December 2020 San Diego Family Care Attack:

  Hackers stole and locked hospital records, compromising the care of over 100,000 patients. The healthcare company paid out $2.3 million to regain access. Similar attacks continue to occur at other healthcare institutions across the US. https://www.hipaajournal.com/4-more-healthcare-organizations-announce-patients-affected-by-recent-ransomware-attacks/

New Services can be requested from: vulnerability@cisa.dhs.gov

Questions?


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY