CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Cybersecurity Services For Building Cyber Resilience

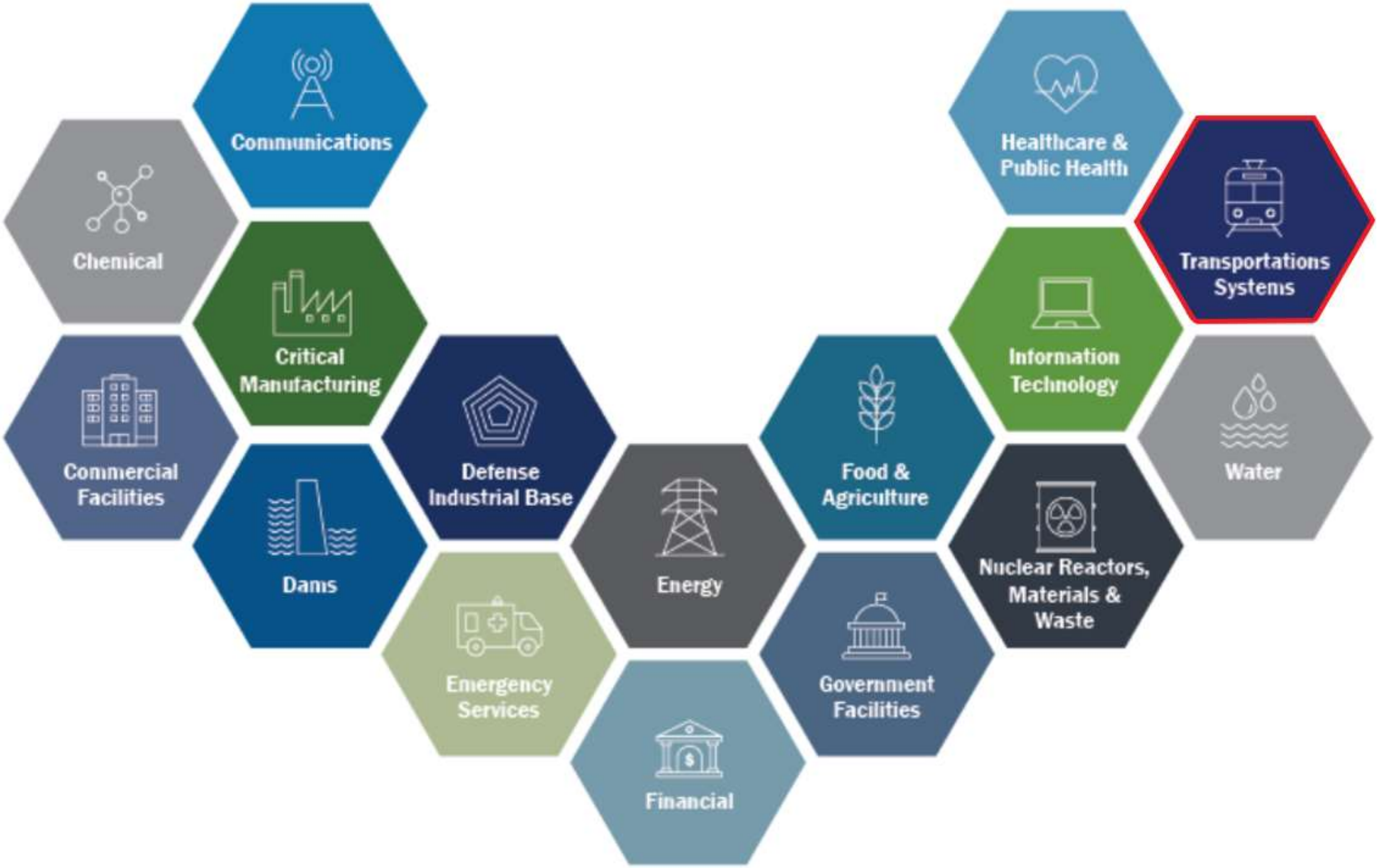
aka *Don’t Divide and Conquer – Partner and Prevail*

R. S. Richard Jr., CISM, CCISO
Cybersecurity Advisor, Region II (NY, NJ, PR, VI)
Cybersecurity Advisor Program
Cybersecurity and Infrastructure Security Agency

Westchester Project Management Institute
21 May 2021

Critical Infrastructure Sectors

CISA assists the public and private sectors secure its networks and focuses on organizations in the following 16 critical infrastructure sectors.



Cybersecurity Advisor Program

CISA mission: Lead the collaborative national effort to strengthen the security and resilience of America’s critical infrastructure

In support of that mission: Cybersecurity Advisors (CSAs):

- **Assess**: Evaluate critical infrastructure cyber risk.
- **Promote**: Encourage best practices and risk mitigation strategies.
- **Build**: Initiate, develop capacity, and support cyber communities-of-interest and working groups.
- **Educate**: Inform and raise awareness.
- **Listen**: Collect stakeholder requirements.
- **Coordinate**: Bring together incident support and lessons learned.

Cyber Threats

735771
979389
33679
380444
1542878
17931
782887
205

Mechanics of a Cyber Attack

Who is the Target?

Staging Targets

- **Smaller organizations** with less sophisticated networks
- **Pre-existing relationships** with intended targets
- **Deliberately selected**, not targets of opportunity
- Examples: **vendors, integrators, suppliers,** and **strategic R&D partners**
- Used for **staging tools** and **capabilities**

Intended Targets

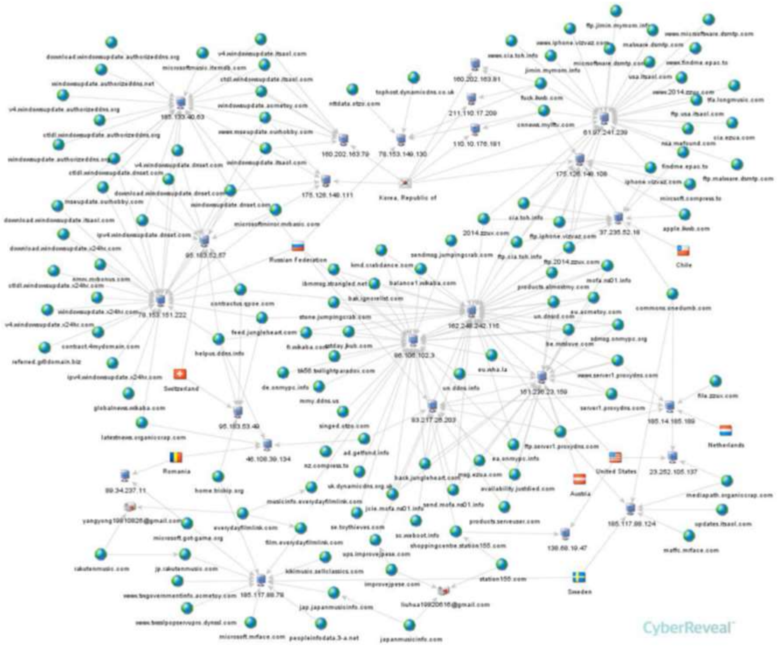
- **Small, medium,** and **large organizations**
- U.S. targets focused within the **Energy Sector**, specifically power generation, transmission, and distribution
- **Sophisticated networks** with more defensive cyber tools

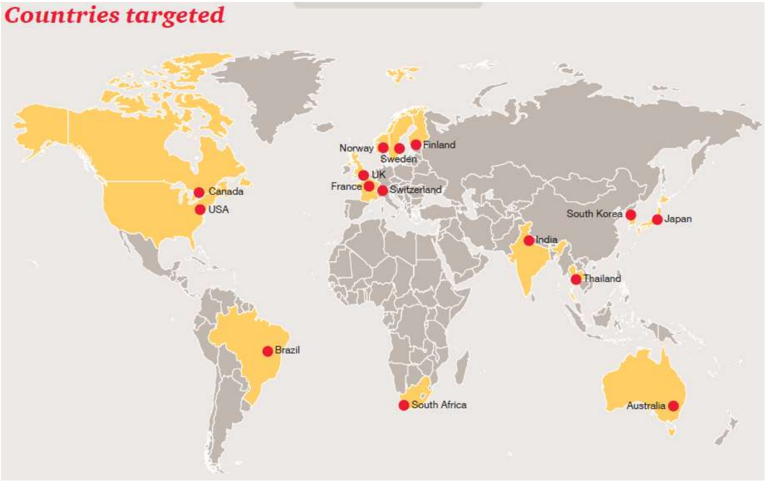
Operation Cloud Hopper

Event: Since late 2016, a threat actor known as “APT10” has targeted managed IT service providers (MSPs). The campaign is known as “Operation Cloud Hopper”.

Impact: The attack allows APT10 unprecedented potential access to the intellectual property and sensitive data of those MSPs and their clients globally.

Specifics: Exfiltrated high volume of data from multiple victims, exploiting compromised MSP networks to stealthily move the data around the world.



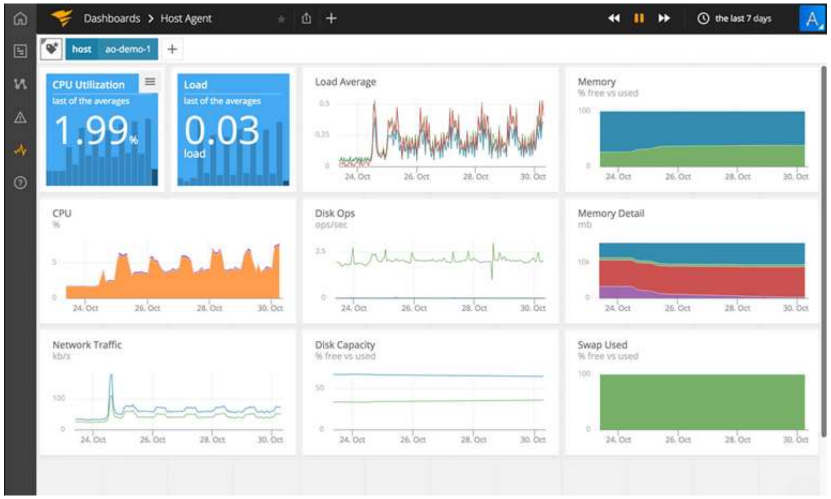


SolarWinds

Event: On December 13, 2020, a cybersecurity company announced the discovery of APT actors infiltrating the supply chain of SolarWinds by inserting a backdoor into their Orion platform.

Impact: As customers downloaded the Trojan Horse installation packages from SolarWinds, attackers were able to access the compromised systems.

Specifics: CISA issued Emergency Directive 21-01 and Alert AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations.

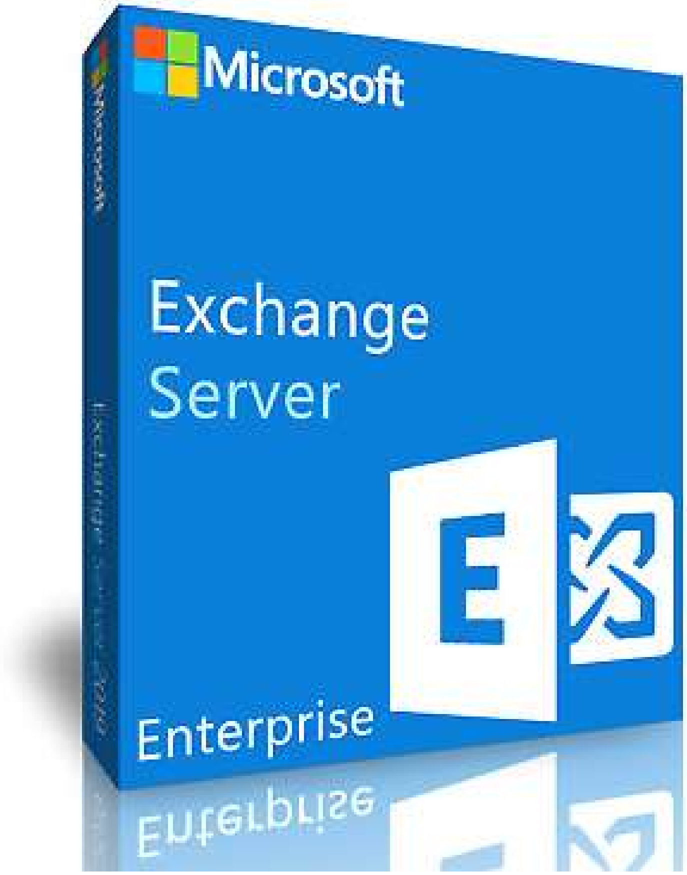


Microsoft Exchange

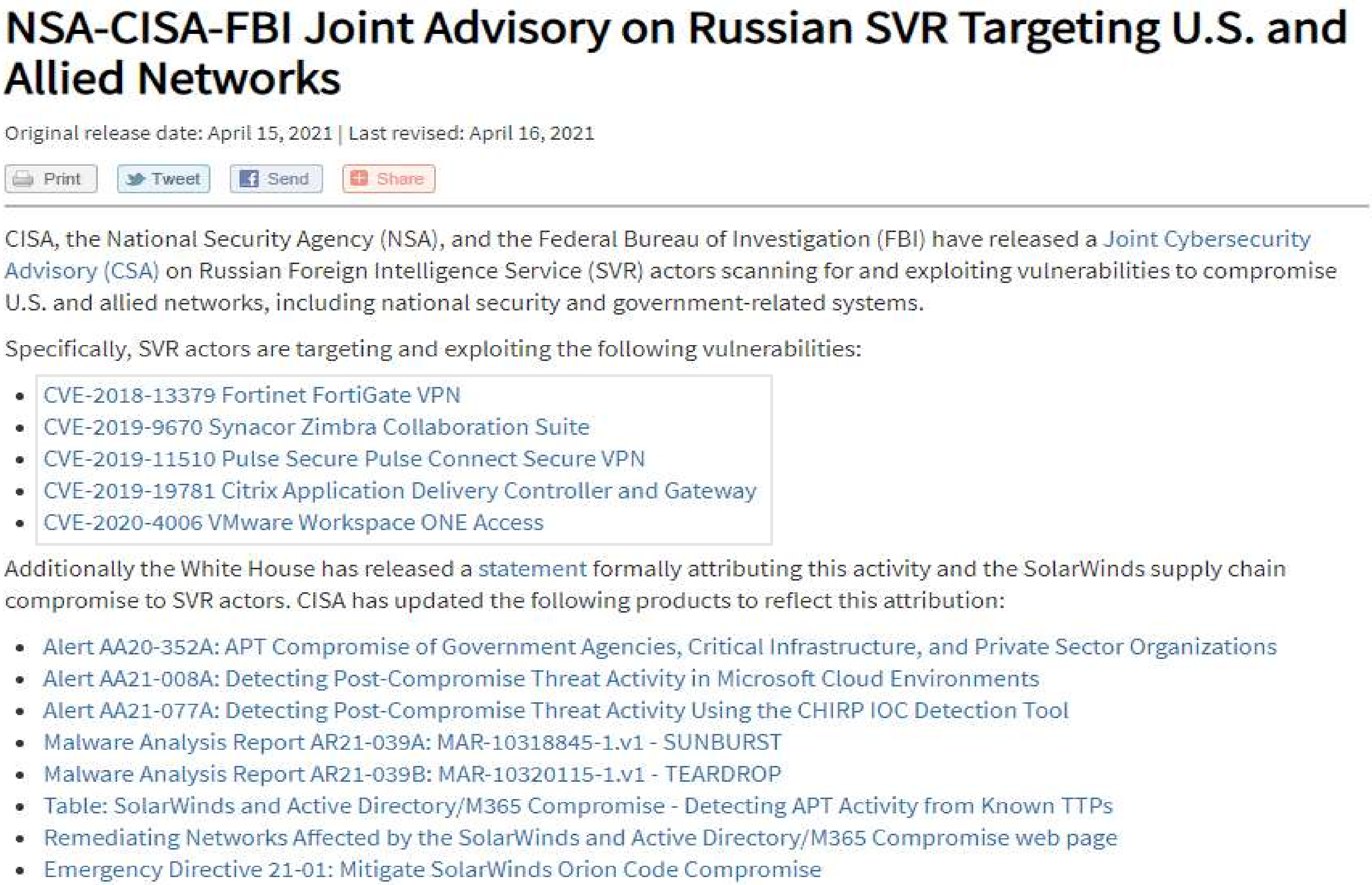
Event: On March 2, 2021, Microsoft disclosed four critical zero-day vulnerabilities in Microsoft Exchange on-premises products which permit an attacker to gain persistent access and control of an enterprise network.

Impact: Impacted multiple versions of Microsoft Exchange Server (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 and CVE-2021-27065).

Specifics: CISA issued Emergency Directive 21-02 and Alert AA21-062A: Mitigate Microsoft Exchange Server Vulnerabilities.



Joint Advisory on Russian SVR Targeting



NSA-CISA-FBI Joint Advisory on Russian SVR Targeting U.S. and Allied Networks

Original release date: April 15, 2021 | Last revised: April 16, 2021

CISA, the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) have released a Joint Cybersecurity Advisory (CSA) on Russian Foreign Intelligence Service (SVR) actors scanning for and exploiting vulnerabilities to compromise U.S. and allied networks, including national security and government-related systems.

Specifically, SVR actors are targeting and exploiting the following vulnerabilities:

- CVE-2018-13379 Fortinet FortiGate VPN
- CVE-2019-9670 Synacor Zimbra Collaboration Suite
- CVE-2019-11510 Pulse Secure Pulse Connect Secure VPN
- CVE-2019-19781 Citrix Application Delivery Controller and Gateway
- CVE-2020-4006 VMware Workspace ONE Access

Additionally the White House has released a statement formally attributing this activity and the SolarWinds supply chain compromise to SVR actors. CISA has updated the following products to reflect this attribution:

- Alert AA20-352A: APT Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations
- Alert AA21-008A: Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments
- Alert AA21-077A: Detecting Post-Compromise Threat Activity Using the CHIRP IOC Detection Tool
- Malware Analysis Report AR21-039A: MAR-10318845-1.v1 - SUNBURST
- Malware Analysis Report AR21-039B: MAR-10320115-1.v1 - TEARDROP
- Table: SolarWinds and Active Directory/M365 Compromise - Detecting APT Activity from Known TTPs
- Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise web page
- Emergency Directive 21-01: Mitigate SolarWinds Orion Code Compromise

Project Management vs Cyber Security

Some Important Considerations:

- Planning is critical
- Data Security is essential
- Integrate security at every stage
- Evaluation of risks & costs is imperative
- Secure and effective communications is vital
- Employee training is quintessential

Criticality of Periodic Assessments

- Periodic assessments are essential for resilience
- Can’t protect if you don’t know what needs protection
- Can’t fix what needs if you don’t know what’s wrong

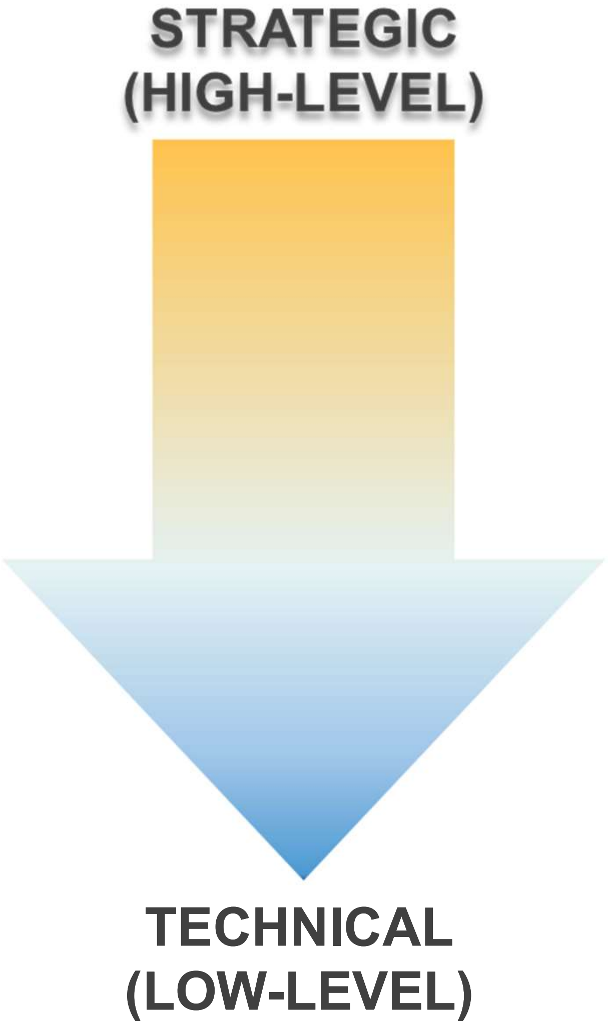
Cybersecurity Resources and Assessments

Regional Resources:

- Cyber Resilience Review (CRR)
- External Dependencies Management (EDM)
- Cyber Infrastructure Survey (CIS)
- Workshops (Incident Mgmt, Cyber Resilience)

National Resources:

- Phishing Campaign Assessment (PCA)
- Cyber Tabletop Exercises (CTTX)
- Vulnerability Scanning Service (CyHy)
  - Web Application Scanning (WAS)
- Validated Architecture Design Review (VADR)
- Red Team Assessment (RTA)
- Remote Penetration Test (RPT)
- Risk & Vulnerability Assessment (RVA)



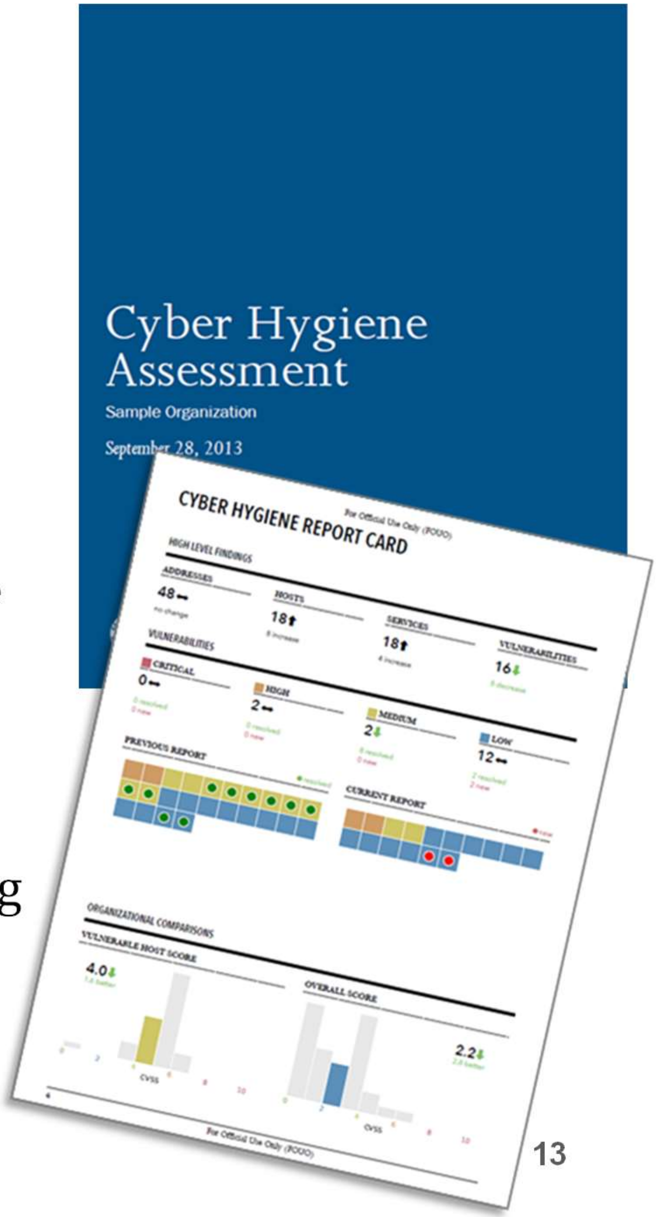
Vulnerability Scanning Service (CyHy)

Assess Internet accessible systems for known vulnerabilities and configuration errors

Work with organization to proactively mitigate threats and risks to systems

Activities include:

- Network Mapping
  - ➢ Identify public IP address space
  - ➢ Identify hosts that are active on IP address space
  - ➢ Determine the O/S and Services running
  - ➢ Re-run scans to determine any changes
  - ➢ Graphically represent address space on a map
- Network Vulnerability & Configuration Scanning
  - ➢ Identify network vulnerabilities and weakness



Cyber Hygiene Assessment

Sample Organization

September 28, 2013

CYBER HYGIENE REPORT CARD

For Official Use Only (FOUO)

HIGH LEVEL FINDINGS

ADDRESSES	HOSTS	SERVICES	VULNERABILITIES
48 ⟷ no change	18 ↑ 8 increase	18 ↑ 4 increase	16 ↓ decrease

VULNERABILITIES

CRITICAL	HIGH	MEDIUM	LOW
0 ⟷ 0 resolved 0 new	2 ⟷ 0 resolved 0 new	2 ↓ resolved 0 new	12 ⟷ 2 resolved 2 new

PREVIOUS REPORT

● resolved

CURRENT REPORT

● new

ORGANIZATIONAL COMPARISONS

VULNERABLE HOST SCORE

4.0 ↓

better

OVERALL SCORE

2.2 ↓

better

For Official Use Only (FOUO)

Web Application Scanning (WAS)

An Internet based scanning service to assess the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations.

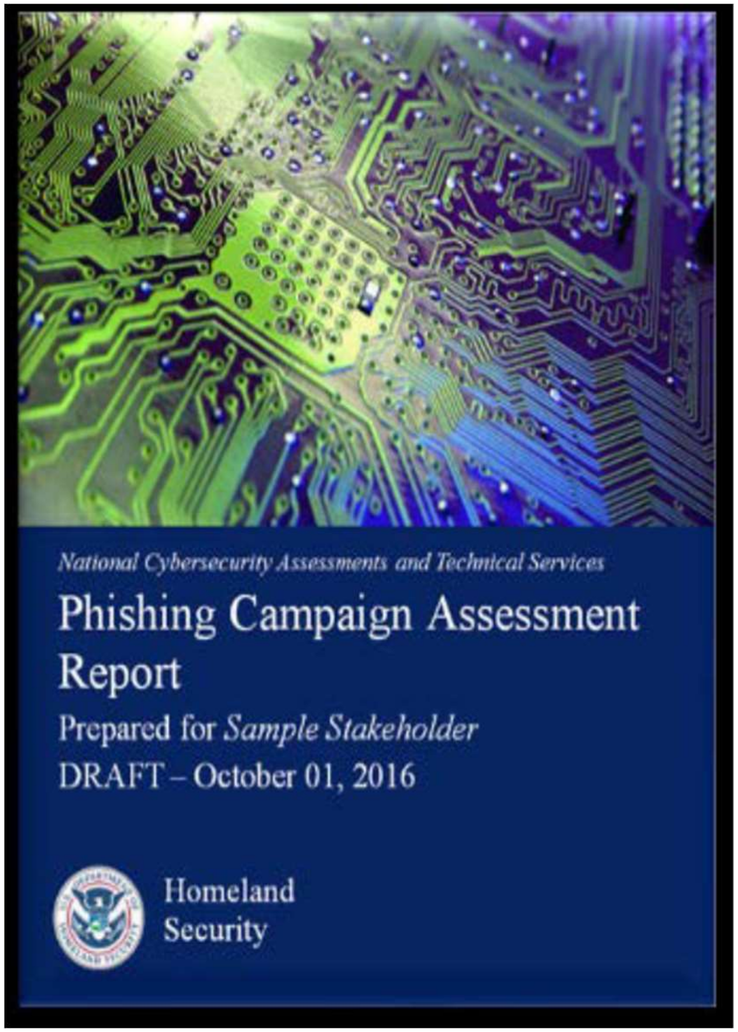
SCANNING OBJECTIVES

- 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

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

Phishing Campaign Assessment (PCA)



National Cybersecurity Assessments and Technical Services

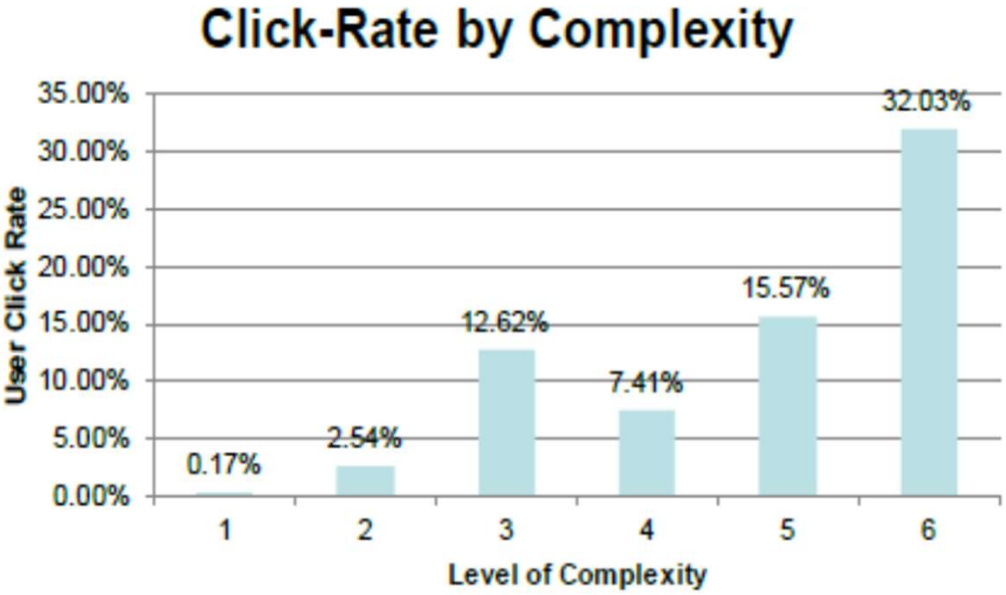
Phishing Campaign Assessment Report

Prepared for *Sample Stakeholder*

DRAFT – October 01, 2016

Homeland Security

Week	Campaign	Date Sent	Complexity Level	User Click Rate	# Emails Sent
1	Please Help!	3/18/16	1	0.17%	401
2	Reveal Your Past	3/31/16	2	2.54%	402
3	Password Expire Alert	4/6/16	3	12.62%	401
4	Severe Weather Checklist	4/15/16	4	7.41%	402
5	Federal Employee Survey	4/20/16	5	15.57%	401
6	Salary Guidelines	4/27/16	6	32.03%	402



Risk and Vulnerability Assessment (RVA)

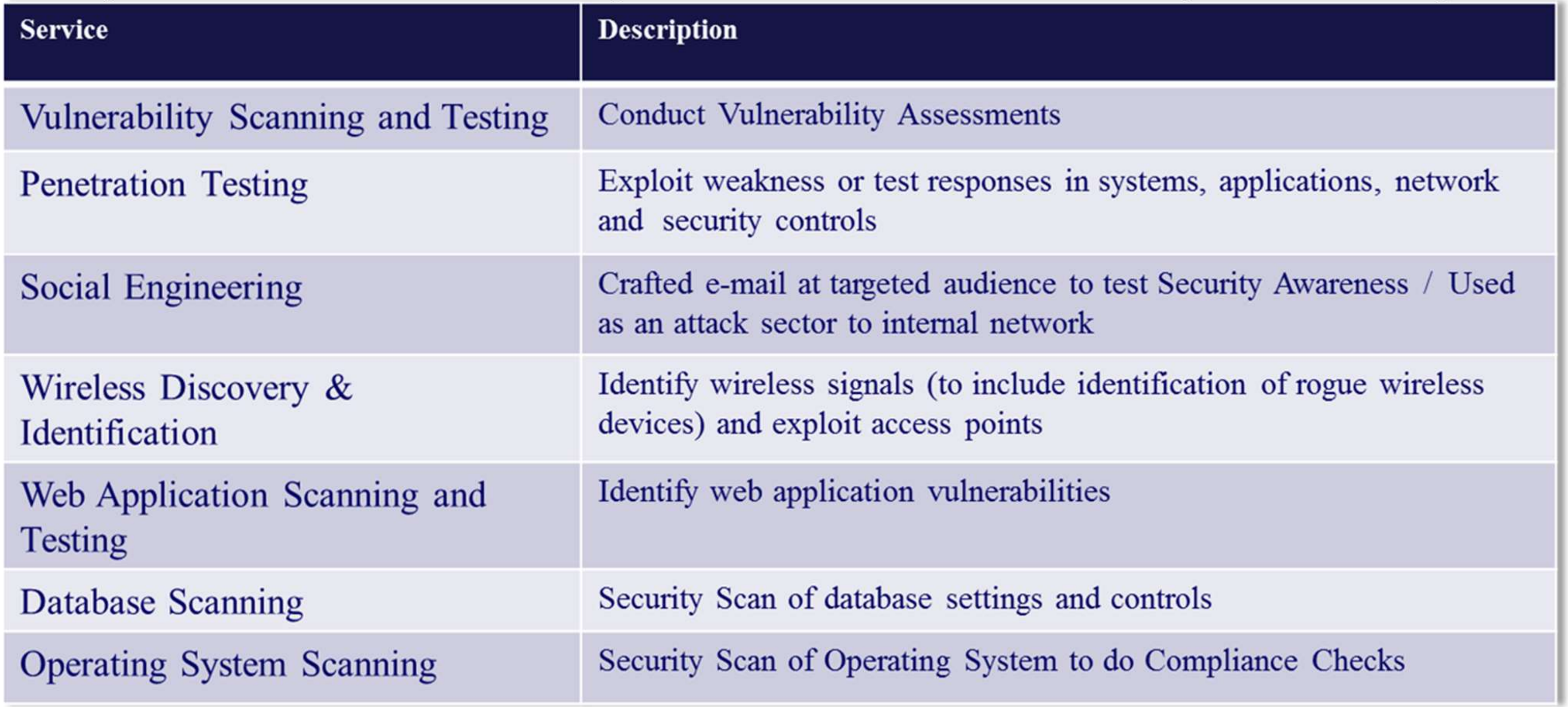
A penetration test, or the short form pen-test, is an attack on a computer system with the intention of finding security weaknesses, potentially gaining access to it, its functionality and data.

- Involves identifying the target systems and the goal, then reviewing the information available and undertaking available means to attain the goal
- A penetration test target may be a white box (where all background and system information is provided) or black box (where only basic or no information is provided except the company name)
- A penetration test will advise if a system is vulnerable to attack, if the defenses were sufficient and which defenses (if any) were defeated in the penetration test

Risk and Vulnerability Assessment (RVA)

Conducts red-team assessments and provides remediation recommendations.

- Identify risks, and provide risk mitigation and remediation strategies
- Improves an agency’s cybersecurity posture, limits exposure, reduces rates of exploitation, and increases the speed and effectiveness of future cyber attack responses.



Service	Description
Vulnerability Scanning and Testing	Conduct Vulnerability Assessments
Penetration Testing	Exploit weakness or test responses in systems, applications, network and security controls
Social Engineering	Crafted e-mail at targeted audience to test Security Awareness / Used as an attack sector to internal network
Wireless Discovery & Identification	Identify wireless signals (to include identification of rogue wireless devices) and exploit access points
Web Application Scanning and Testing	Identify web application vulnerabilities
Database Scanning	Security Scan of database settings and controls
Operating System Scanning	Security Scan of Operating System to do Compliance Checks

Remote Penetration Test (RPT)

Utilizes a dedicated remote team to assess and identify vulnerabilities and work with customers to eliminate exploitable pathways.

- Focuses on externally accessible systems

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.

Cyber Security Evaluation Tool (CSET)

Purpose: Provides a detailed, effective, and repeatable tool for assessing systems security against established industry standards and guidance.

Facilitated: Self-Administered, undertaken independently

Benefits:

- Immediately available for download upon request
- Understanding of operational technology and information technology network security practices
- Ability to drill down on specific areas and issues
- Helps to integrate cybersecurity into current corporate risk management strategy

Time to Execute / Availability:

- Varies greatly (min 2 Hours) / N/A (self-assessment)

Cyber Resilience Review (CRR)

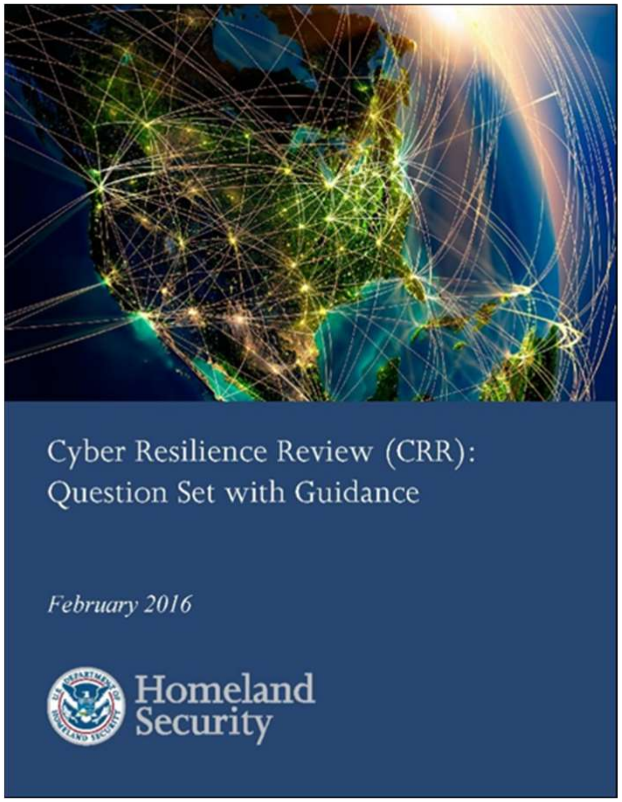
Purpose: The CRR is an assessment intended to evaluate an organization’s operational resilience and cybersecurity practices of its critical services

Delivery: The CRR can be

- Facilitated
- Self-administered

CRR Self-Assessment Package is available on the C-Cubed Voluntary Program website.

- Helps public and private sector partners understand and measure cyber security capabilities as they relate to operational resilience and cyber risk
- Based on the CERT ® Resilience Management Model (CERT® RMM)



Cyber Resilience Review (CRR): Question Set with Guidance

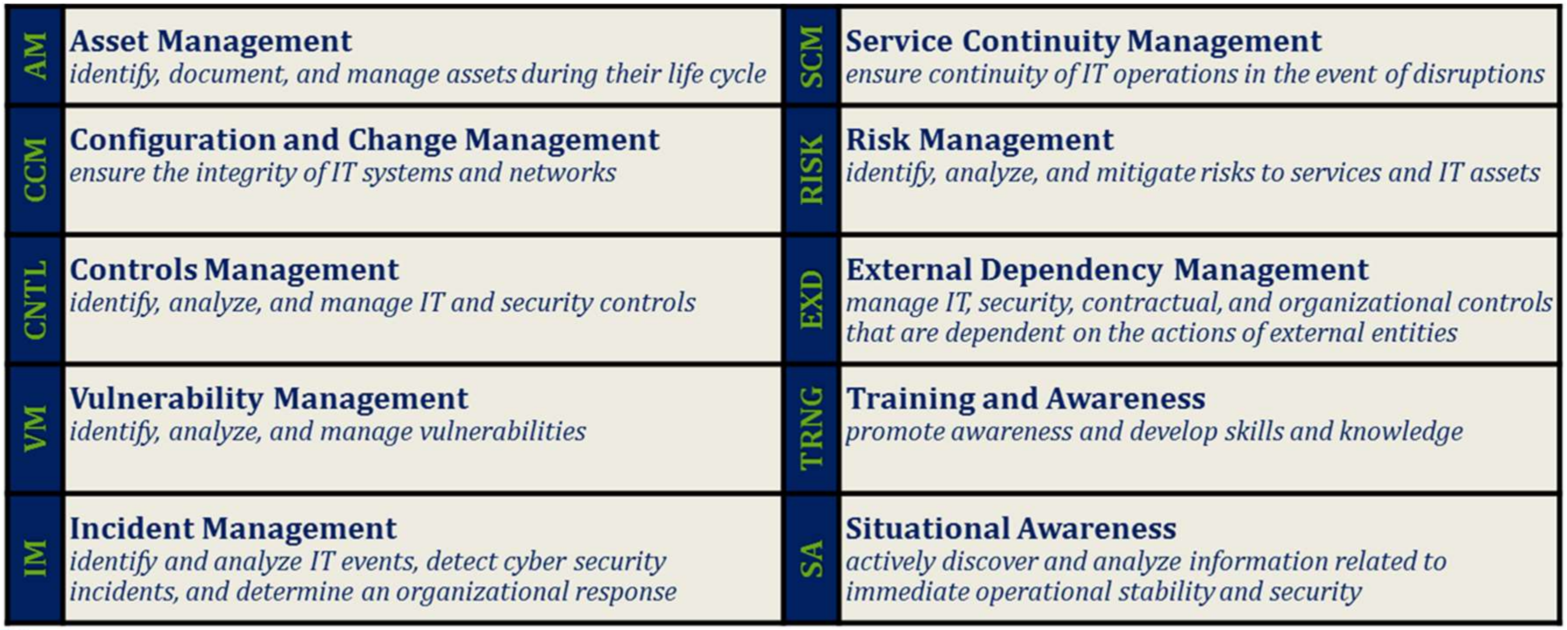
February 2016

Homeland Security

Cyber Resilience Review (CRR) | Domains

These represent key areas that typically contribute to an organization's cyber resilience— each domain focuses on:

- Documentation in place, and periodically reviewed & updated
- Communication and notification to all those who need to know
- Execution/Implementation & analysis in a consistent, repeatable manner
- Alignment of goals and practices within and across CRR domains



AM	**Asset Management** *identify, document, and manage assets during their life cycle*	SCM	**Service Continuity Management** *ensure continuity of IT operations in the event of disruptions*
CCM	**Configuration and Change Management** *ensure the integrity of IT systems and networks*	RISK	**Risk Management** *identify, analyze, and mitigate risks to services and IT assets*
CNTL	**Controls Management** *identify, analyze, and manage IT and security controls*	EXD	**External Dependency Management** *manage IT, security, contractual, and organizational controls that are dependent on the actions of external entities*
VM	**Vulnerability Management** *identify, analyze, and manage vulnerabilities*	TRNG	**Training and Awareness** *promote awareness and develop skills and knowledge*
IM	**Incident Management** *identify and analyze IT events, detect cyber security incidents, and determine an organizational response*	SA	**Situational Awareness** *actively discover and analyze information related to immediate operational stability and security*

Cybersecurity Infrastructure Survey (CIS)

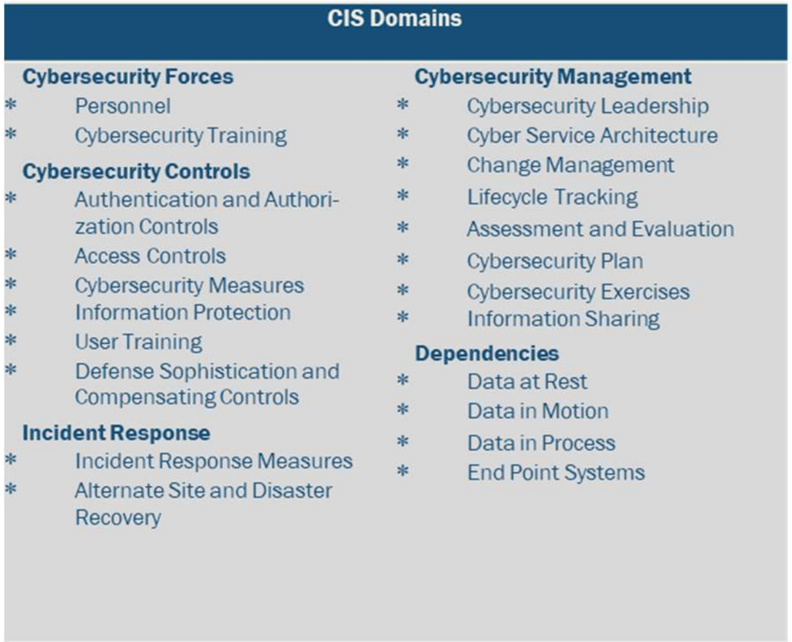
Structured, interview-based assessment (2 ½ to 4 hours) of essential cybersecurity practices and controls in-place for critical services within your organization

Identifies interdependencies, capabilities, and the emerging effects related to current cybersecurity posture

Focuses on protective measures, threat scenarios, and a service-based view of cybersecurity in context of the surveyed topics

Broadly aligns to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)

CIS Survey Question Domains



CIS Domains

Cybersecurity Forces

* Personnel
* Cybersecurity Training

Cybersecurity Controls

* Authentication and Authorization Controls
* Access Controls
* Cybersecurity Measures
* Information Protection
* User Training
* Defense Sophistication and Compensating Controls

Incident Response

* Incident Response Measures
* Alternate Site and Disaster Recovery

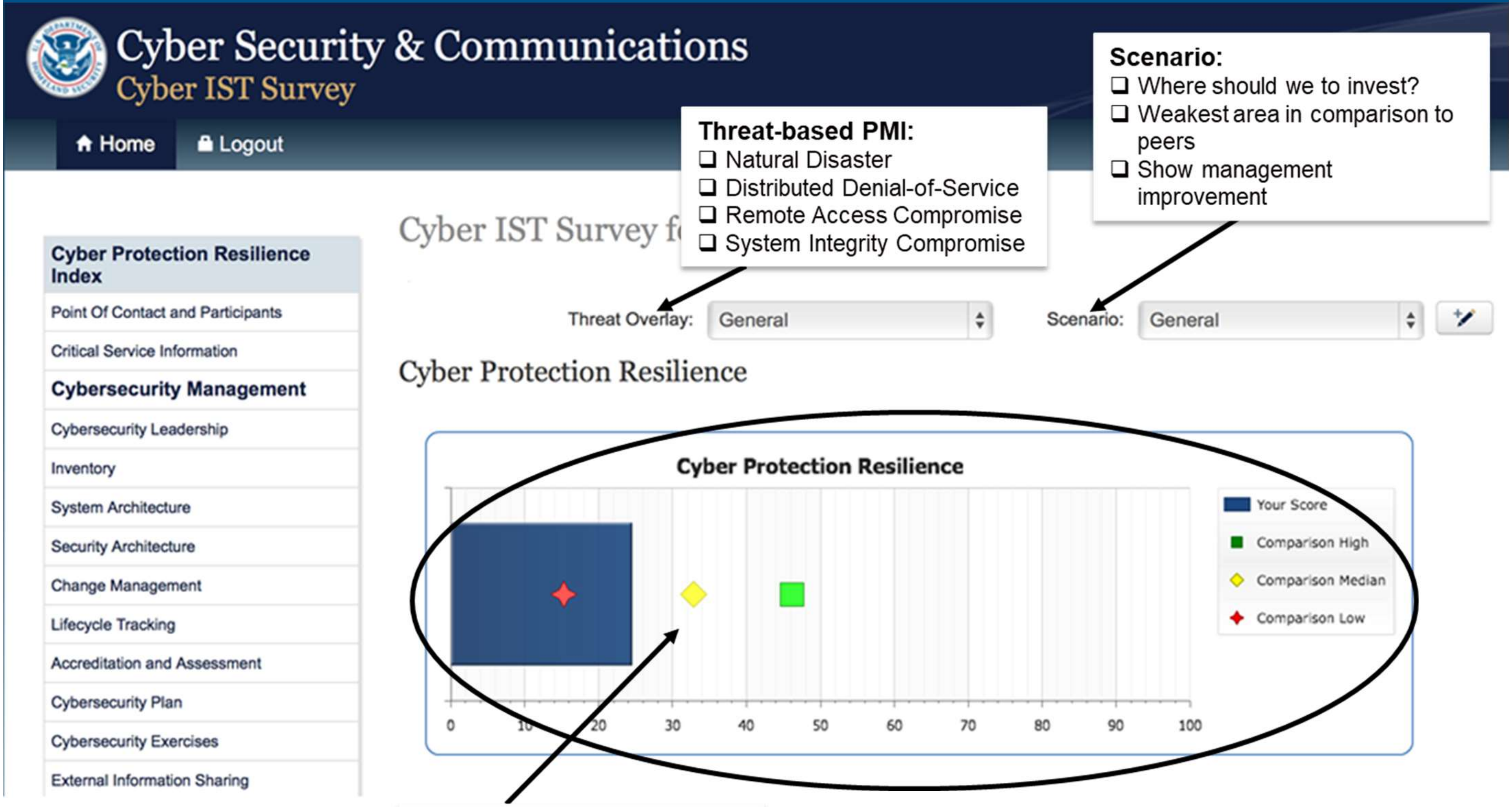
Cybersecurity Management

* Cybersecurity Leadership
* Cyber Service Architecture
* Change Management
* Lifecycle Tracking
* Assessment and Evaluation
* Cybersecurity Plan
* Cybersecurity Exercises
* Information Sharing

Dependencies

* Data at Rest
* Data in Motion
* Data in Process
* End Point Systems

Example CIS Dashboard



Cyber Security & Communications

Cyber IST Survey

Home

Logout

Cyber IST Survey f

Cyber Protection Resilience Index

- Point Of Contact and Participants
- Critical Service Information
- **Cybersecurity Management**
- Cybersecurity Leadership
- Inventory
- System Architecture
- Security Architecture
- Change Management
- Lifecycle Tracking
- Accreditation and Assessment
- Cybersecurity Plan
- Cybersecurity Exercises
- External Information Sharing

Threat Overlay: General

Scenario: General

Cyber Protection Resilience

Threat-based PMI:

- ❑ Natural Disaster
- ❑ Distributed Denial-of-Service
- ❑ Remote Access Compromise
- ❑ System Integrity Compromise

Scenario:

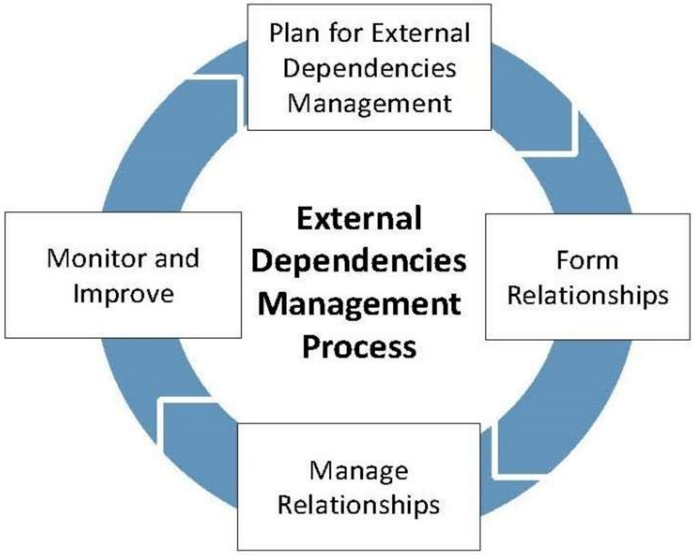
- ❑ Where should we to invest?
- ❑ Weakest area in comparison to peers
- ❑ Show management improvement

Comparison:

- ❑ Low Performers
- ❑ Median Performers
- ❑ High Performers

External Dependencies Management Assessment

- **Purpose:** Evaluate an entity's management of their dependencies on third-party entities
- **Delivery:** CSA-facilitated
- **Benefits**:
  - Better understanding of the entity's cyber posture relating to external dependencies
  - Identification of improvement areas for managing third parties that support the organization


Plan for External Dependencies Management
External Dependencies Management Process
Form Relationships
Manage Relationships
Monitor and Improve

EDM process outlined per the External Dependencies Management Resource Guide

External Dependency Management (EDM)

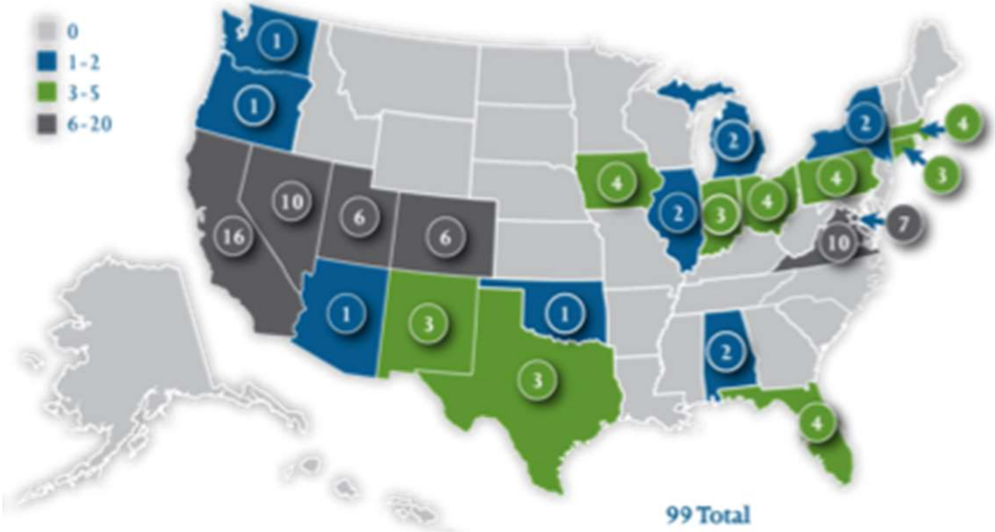
To provide the organization with an understandable and useful structure for the evaluation, the EDM Assessment is divided into three distinct areas (domains):

1. **RELATIONSHIP FORMATION** – how the organization considers third party risks, selects external entities, and forms relationships with them so that risk is managed from the start
2. **RELATIONSHIP MANAGEMENT AND GOVERNANCE** – how the organization manages ongoing relationships with external entities to support and strengthen its critical services at a managed level of risk and cost
3. **SERVICE PROTECTION AND SUSTAINMENT** – how the organization plans for, anticipates, and manages disruption or incidents related to external entities

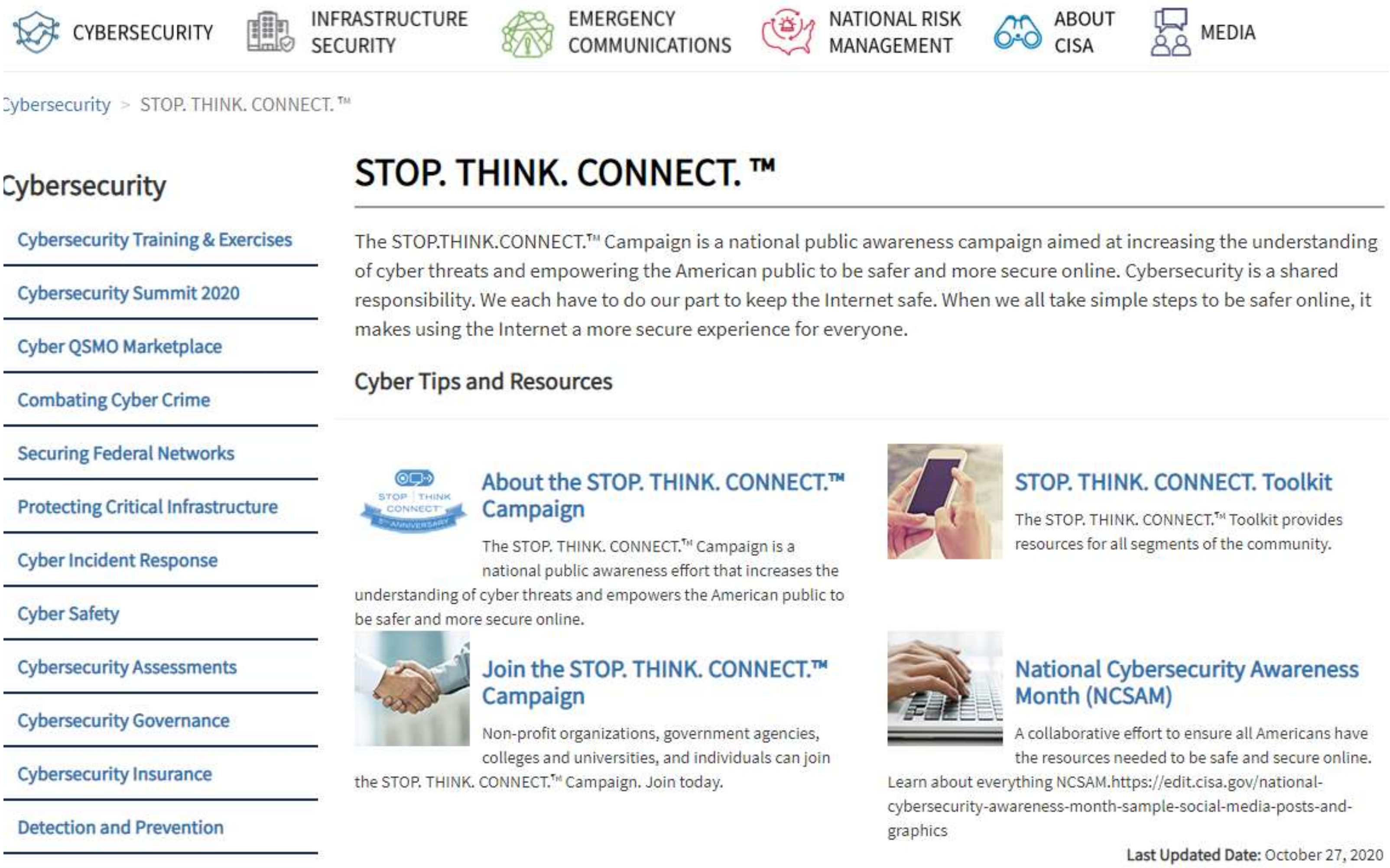
Cyber Exercises and Planning

CISA's National Cyber Exercise and Planning Program develops, conducts, and evaluates cyber exercises and planning activities for state, local, tribal and territorial governments and public and private sector critical infrastructure organizations.

- Cyber Storm Exercise – DHS's flagship national-level biennial exercise
- Exercise Planning and Conduct
- Cyber Exercise Consulting and Subject Expertise Support
- Cyber Planning Support
- Off-the-Shelf /
  Exercise-In-A-Box Resources



STOP. THINK. CONNECT.



STOP. THINK. CONNECT. ™

The STOP.THINK.CONNECT.™ Campaign is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. Cybersecurity is a shared responsibility. We each have to do our part to keep the Internet safe. When we all take simple steps to be safer online, it makes using the Internet a more secure experience for everyone.

Cyber Tips and Resources

About the STOP. THINK. CONNECT.™ Campaign

The STOP. THINK. CONNECT.™ Campaign is a national public awareness effort that increases the understanding of cyber threats and empowers the American public to be safer and more secure online.

STOP. THINK. CONNECT. Toolkit

The STOP. THINK. CONNECT.™ Toolkit provides resources for all segments of the community.

Join the STOP. THINK. CONNECT.™ Campaign

Non-profit organizations, government agencies, colleges and universities, and individuals can join the STOP. THINK. CONNECT.™ Campaign. Join today.

National Cybersecurity Awareness Month (NCSAM)

A collaborative effort to ensure all Americans have the resources needed to be safe and secure online. Learn about everything NCSAM.https://edit.cisa.gov/national-cybersecurity-awareness-month-sample-social-media-posts-and-graphics

Last Updated Date: October 27, 2020

https://www.cisa.gov/stopthinkconnect

Incident Reporting / Malware Analysis

24x7 contact number: 888-282-0870 | CISAServiceDesk@cisa.dhs.gov

Where/How/When to Report: https://www.us-cert.gov/forms/report

- If there is a suspected or confirmed cyber attack or incident that:
- Affects core government or critical infrastructure functions;
- Results in the loss of data, system availability; or control of systems;
- Indicates malicious software is present on critical systems

Advanced Malware Analysis Center:

- Provides 24x7 dynamic analyses of malicious code. Stakeholders submit samples via an online website and receive a technical document outlining the results of the analysis. Experts will detail recommendations for malware removal and recovery activities.
- Web Submission: https://malware.us-cert.gov

Contact / Questions

Questions?

Contact:
R. S. Richard Jr.
Cybersecurity Advisor, Region II
Cybersecurity & Infrastructure Security Agency
Email: richard.richard@hq.dhs.gov
Phone: 631-241-3662