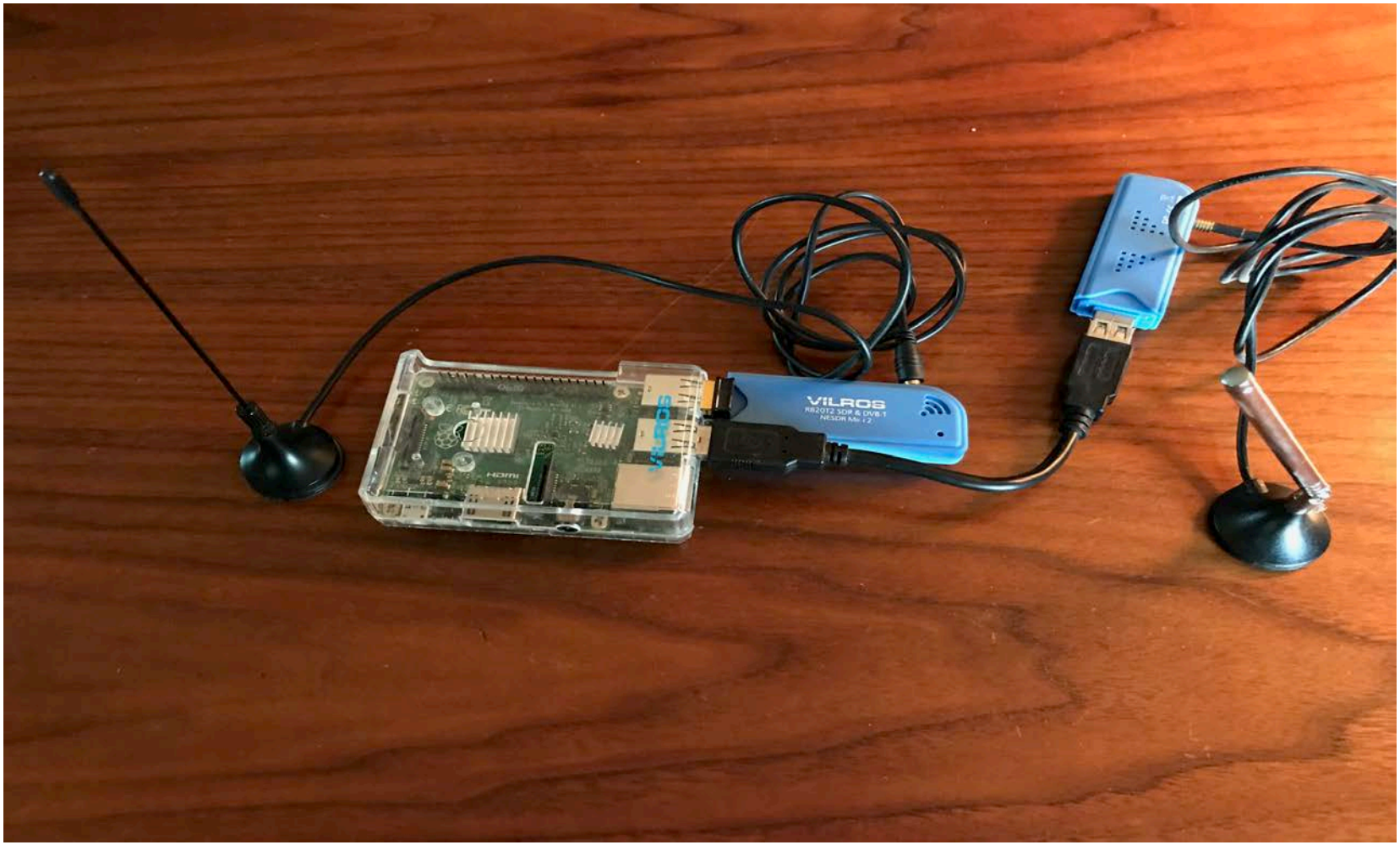
Cybersecurity Services For Building Cyber Resilience

Harley D. Rinerson
Chief of Operations – Central U.S.
Cybersecurity Advisor Program
Cybersecurity and Infrastructure Security Agency

28 March 2019

CISA
CYBER+INFRASTRUCTURE

What is this?



Free Apps

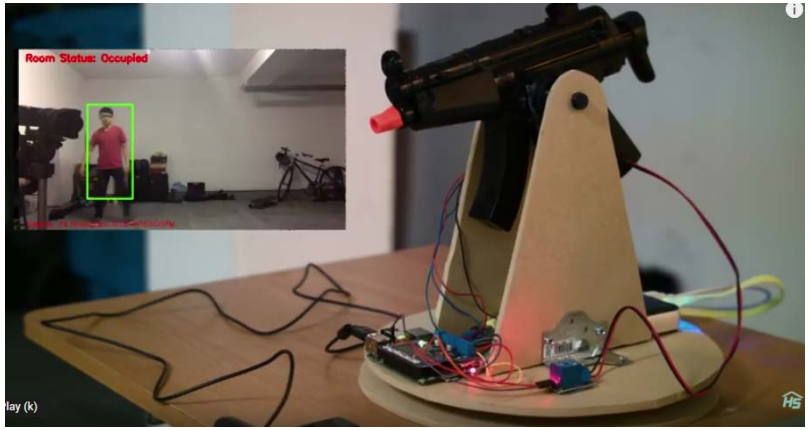

Routes
Layers
Route
Edit
METARs
Winds
SIGMETs
Weather
XM Weather™
AD
eN2653M
eDAL1732
7175ft
eAAL193
14200ft
eSWR38
11100ft
12200ft
eVRD1747
eTHY79K

Aircraft Tracking

https://www.youtube.com/watch?v=KNY7Hbl9k78

https://www.youtube.com/watch?v=6v3J6MSkTgs

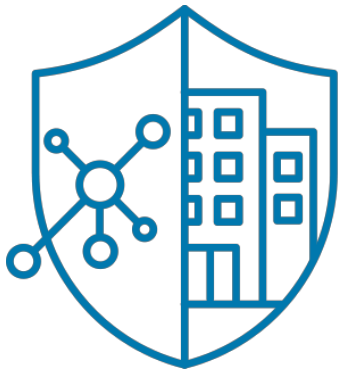
Drone camera



Nerf Gun optical tracker

CISA Mission and Vision

- Cybersecurity and Infrastructure Security Agency (CISA) mission:
  - Lead the collaborative national effort to strengthen the security and resilience of America's critical infrastructure
- CISA vision:
  - A Nation with secure, resilient, and reliable critical infrastructure upon which the American way of life can thrive



CISA
CYBER+INFRASTRUCTURE

CISA in Brief

- CISA consists of:

Cybersecurity Division

Emergency Communications Division

Infrastructure Security Division

National Risk Management Center

Federal Protective Service

CISA CYBER+INFRASTRUCTURE

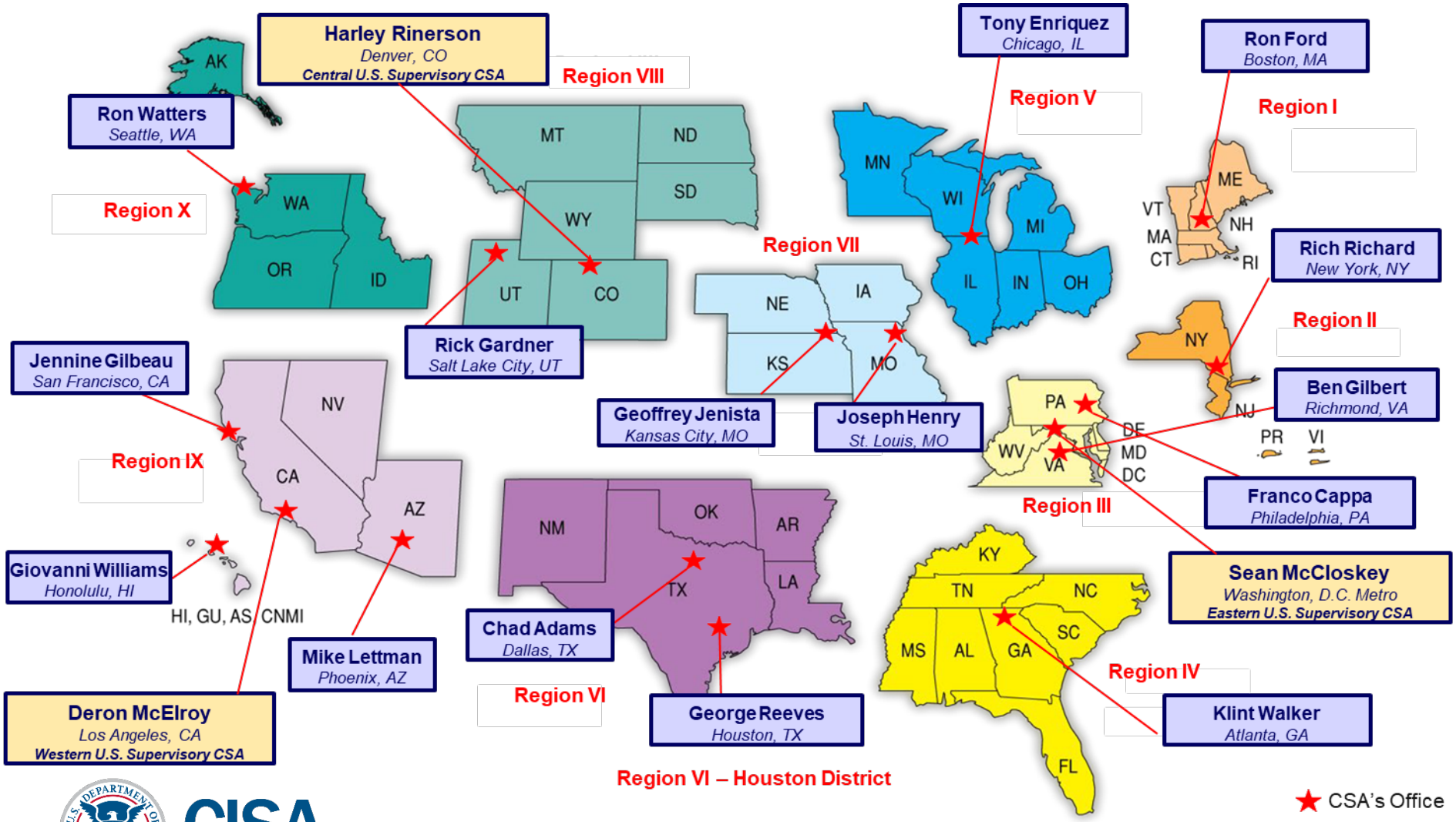
Cybersecurity Advisor Program

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.

CSA Deployed Personnel



CISA
CYBER+INFRASTRUCTURE

Resilience Defined

"… the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents…"

- Presidential Policy Directive 21
February 12, 2013

Protect (Security)	**Sustain (Continuity)**
Perform (Capability)	**Repeat (Maturity)**

CISA
CYBER+INFRASTRUCTURE

Operational Resilience in Practice

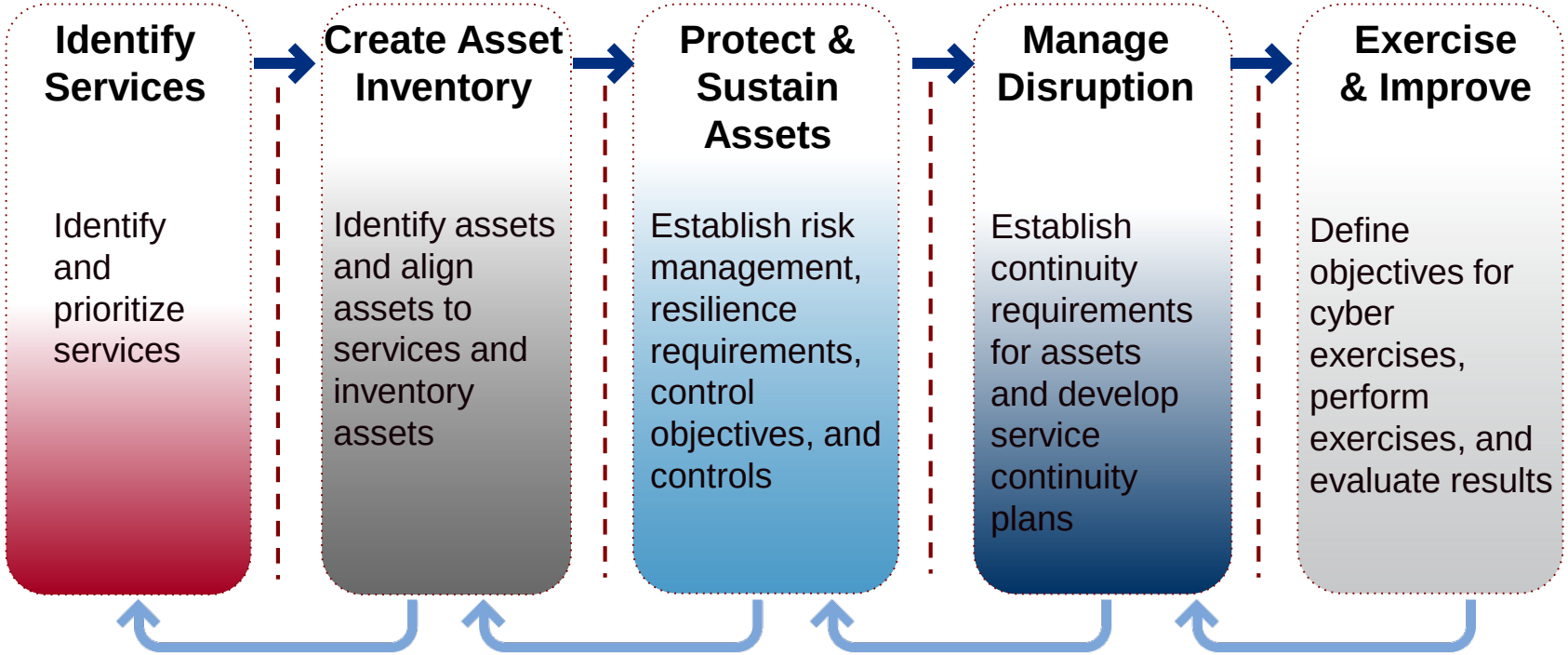
Operational resilience emerges from what we do, such as:

- Identifying and mitigating risks,
- Planning for and managing vulnerabilities and incidents,
- Performing service-continuity processes and planning,
- Managing IT operations,
- Managing, training, & deploying people,
- Protecting and securing important assets, and
- Working with external partners.

CISA
CYBER+INFRASTRUCTURE

Working toward Cyber Resilience

Follow a framework or general approach to cyber resilience.
One successful approach includes:



CISA
CYBER+INFRASTRUCTURE

NIST Cybersecurity Framework

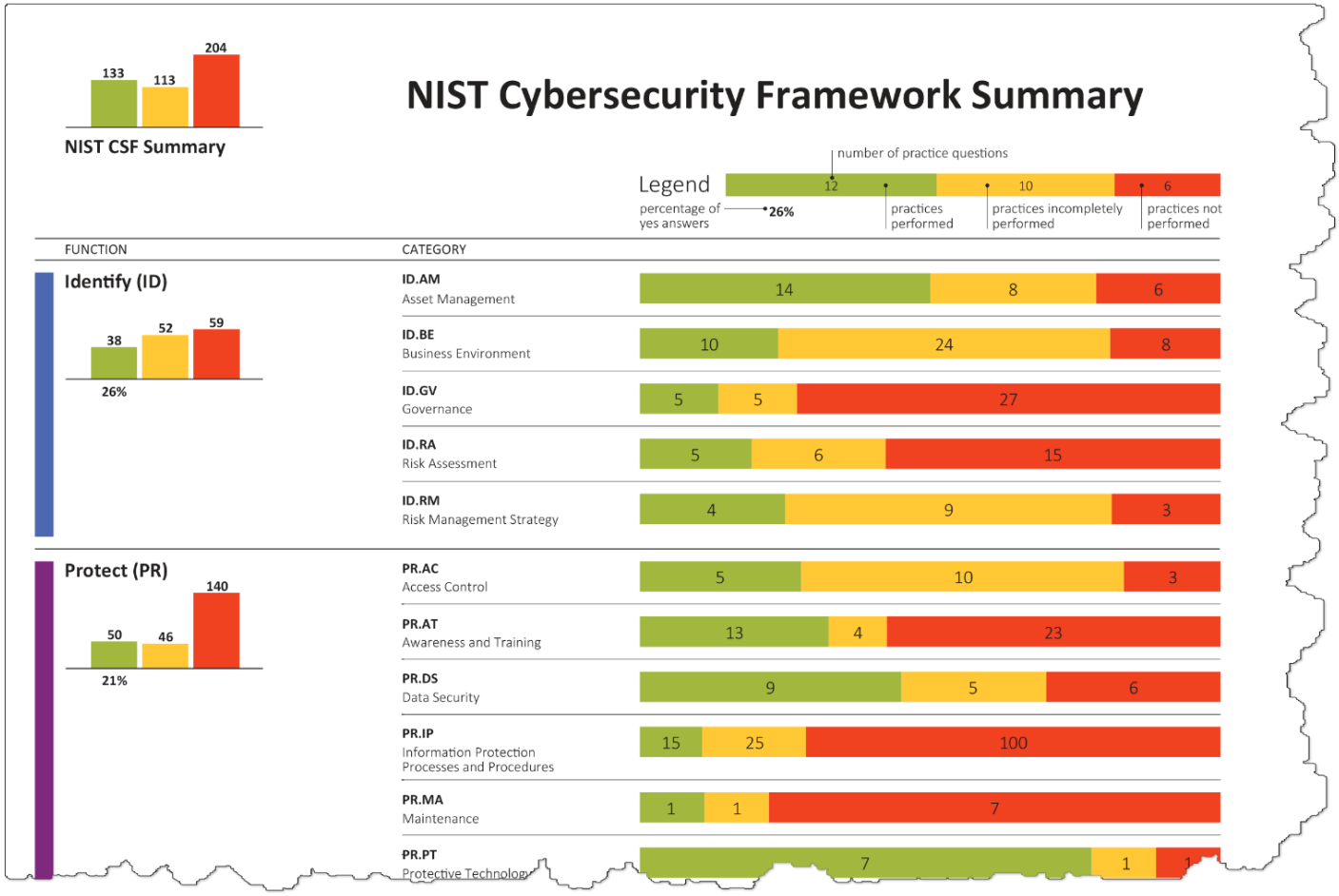
- The Cybersecurity Framework
  - Establishes a common perspective and vernacular,
  - Provides risk-based guidelines,
  - Is collaboration-oriented, and
  - Is internationally recognized.

- For more information, visit nist.gov/cyberframework

Functions	Categories
IDENTIFY (ID)	Asset Mangement (AM)
	Business Environment (BE)
	Governenace (GV)
	Risk Assessment (RA)
	Risk Management Stategy (RM)
PROTECT (PR)	Access Control (AC)
	Awareness and Training (AT)
	Data Security (DS)
	Information Protection Processess and Procedures (IP)
	Maintenance (MA)
	Protective Technology (PT)
DETECT (DE)	Anomolies and Events (AE)
	Security Continuos Monitoring (CM)
	Detection Processes (DP)
RESPOND (RS)	Incident Response Planning (RP)
	Communications (CO)
	Analysis (AN)
	Mitigation (MI)
	Improvements (IM)
RECOVER (RC)	Recovery Planning (RP)
	Improvements/Gap Remediation (IM)
	Communications (CO)

CISA CYBER+INFRASTRUCTURE

Cybersecurity Framework Summary



ASSESSMENTS

Range of Cybersecurity Assessments

STRATEGIC
(C-Suite Level)

- Cyber Resilience Review (Strategic) ----------
- External Dependencies Management (Strategic)----------
- Cyber Infrastructure Survey (Strategic)----------
- Cybersecurity Evaluations Tool Strategic/Technical)-----
- Phishing Campaign Assessment (Technical)----------
- Vulnerability Scanning / Hygiene (Technical)----------
- Validated Architecture Design Review (Technical) --------
- Risk and Vulnerability Assessment (Technical)----------

TECHNICAL
(Network-Administrator Level)

CISA
CYBER+INFRASTRUCTURE

VULNERABILITY SCANNING

Vulnerability Scanning

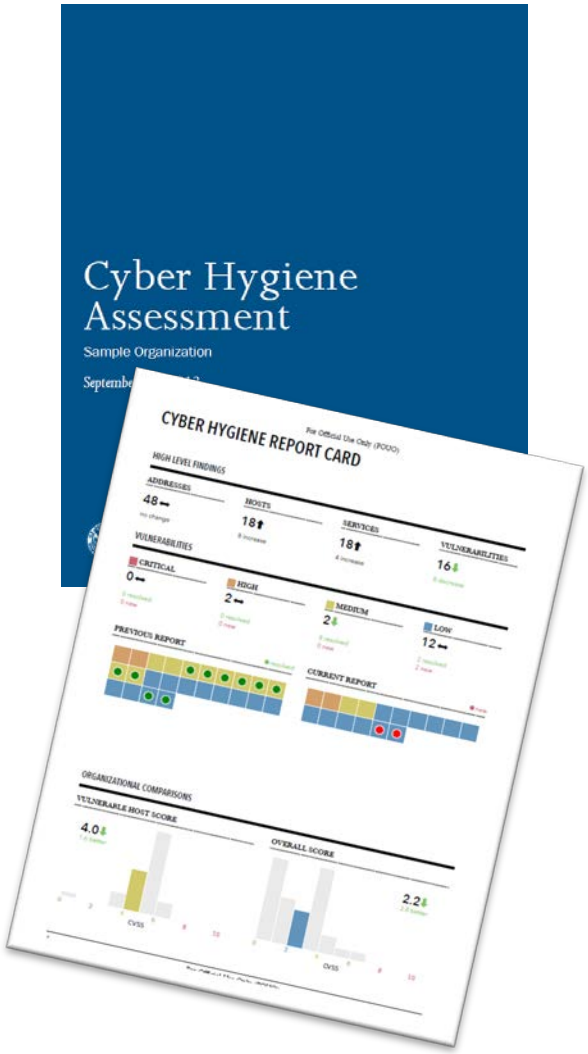
Purpose: Assess Internet-accessible systems for known vulnerabilities and configuration errors.

Delivery: Online by CISA

Benefits:

- Continual review of system to identify potential problems
- Weekly reports detailing current and previously mitigated vulnerabilities
- Recommended mitigation for identified vulnerabilities

  - **Network Vulnerability & Configuration Scanning**
    - Identify network vulnerabilities and weakness



INCIDENT MANAGEMENT

Federal Role in Cyber Incident Response,

Federal Role in Cyber Incident Response

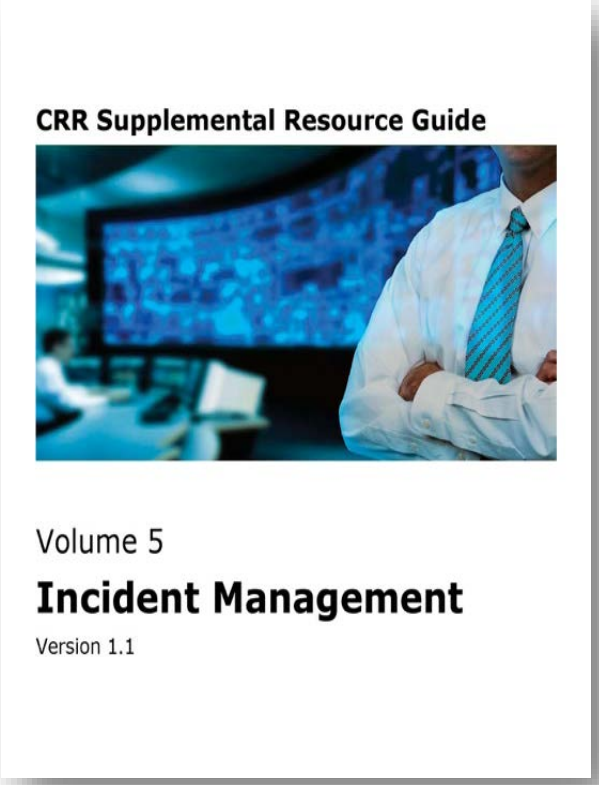
- **Threat Response:** Attributing, pursuing, and disrupting malicious cyber actors and malicious cyber activity. Conducting criminal investigations and other actions to counter the malicious cyber activity.
- **Asset Response:** Protecting assets and mitigating vulnerabilities in the face of malicious cyber activity, reducing the impact to systems and data; strengthening, recovering, and restoring services; identifying other entities at risk; and assessing potential risk to broader community.

CISA CYBER+INFRASTRUCTURE

Incident Management Planning Helps Mitigate Effects

1. Get leadership support for incident management planning.
2. Establish an event-detection process.
3. Establish a triage-and-analysis process.
4. Establish an incident-declaration process.
5. Establish an incident-response and recovery process.
6. Establish an incident-communications process.
7. Assign roles and responsibilities for incident management.
8. Establish a post-incident analysis and improvement process.

Resource: CRR Supplemental Resource Guide, Incident Management.



CISA
CYBER+INFRASTRUCTURE

National Cybersecurity and Communications Integration Center

CISA's National Cybersecurity and Communications Integration Center (NCCIC) works to reduce the risk of systemic cybersecurity and communications challenges in our role as the Nation's flagship cyber defense, incident response, and operational integration center.

Core efforts include:

- Information exchange
- Training and exercises
- Risk and vulnerability assessments
- Data synthesis and analysis
- Operational planning and coordination
- Watch operations
- Incident response and recovery

CISA
CYBER+INFRASTRUCTURE

Additional Information Sharing Opportunities

- State Fusion Centers
- Multi-State Information Sharing and Analysis Center
  - Focal point for cyber threat prevention, protection, response and recovery for state, local, tribal, and territorial governments.
  - Operates 24 x7 cyber security operations center, providing real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification and mitigation and incident response. For more information, visit www.cisecurity.org/ms-isac or email info@msisac.org

- ISACs and ISAOs
  - **Information Sharing and Analysis Centers** (ISACs) or **Organizations** (ISAOs) are communities of interest sharing cybersecurity risk, threat information, and incident management to members. For more information on ISACs, visit www.nationalisacs.org. For more on ISAOs visit www.isao.org/about.

CISA CYBER+INFRASTRUCTURE

Technical Training

Chicago Next

CISA
CYBER+INFRASTRUCTURE

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 to be fixed if you don’t know what’s wrong

Protected Critical Infrastructure Information Program

Protected Critical Infrastructure Information (PCII) Program Guards Your Information

- Sensitive critical infrastructure information voluntarily given to CISA is protected by law from
  - Public release under Freedom of Information Act requests,
  - Public release under State, local, tribal, or territorial disclosure laws,
  - Use in civil litigation and
  - Use in regulatory purposes.

CISA CYBER+INFRASTRUCTURE

Contact

General Inquiries

cyberadvisor@hq.dhs.gov

CISA Contact Information

Harley D. Rinerson **Chief of Operations – Central U.S.** **Cybersecurity Advisor Program**	**harley.rinerson@hq.dhs.gov** **202.809.3314**

Cybersecurity and Infrastructure Security Agency

CISA
CYBER+INFRASTRUCTURE

BACK-UP SLIDES

ADDITIONAL CYBERSECURITY RESOURCES

Resource Guides

- **Resource Guides:** Created to help organizations enhance their resilience in specific Cyber Resilience Review (CRR) domains.
- **CRR Tools:** Helps move organizations from initial capability to well-define capability in security management areas
- **CRR Domains**: Includes the CRR 10 “domains” each representing a capability area foundational to an organization’s cyber resilience.
- **Content**: While the guides were developed for organizations to utilize after conducting a CRR, these publications provide content useful for all organizations with cybersecurity equities.
- **Flexibility in Use**: Moreover, the guides can be utilized as a full set or as individual components, depending on organizational preference and/or need.
- For more information, visit US-CERT.gov/ccubedvp/assessments

CISA

CYBER+INFRASTRUCTURE

PHISHING CAMPAIGN ASSESSMENT

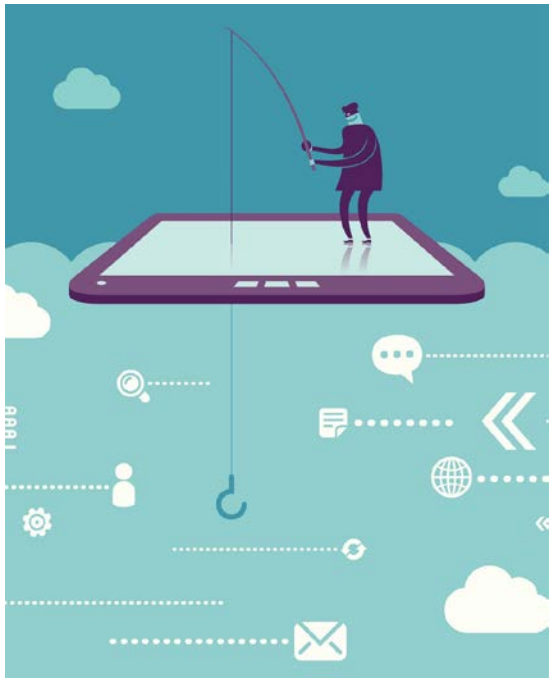
Phishing Campaign Assessment

Purpose: Test an organization's susceptibility and reaction to phishing emails.

Delivery: Online delivery by CISA

Benefits:

- Identify the risk phishing poses to your organization
- Decrease risk of successful malicious phishing attacks, limit exposure, reduce rates of exploitation
- Receive actionable metrics
- Highlight need for improved security training
- Increase cyber awareness among staff

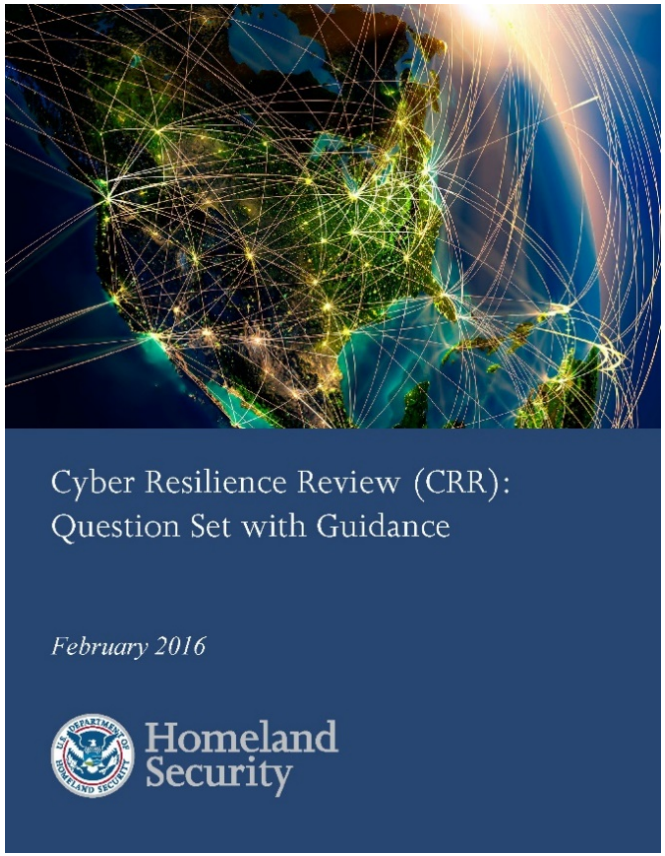


CISA CYBER+INFRASTRUCTURE

CYBERSECURITY RESILIENCE REVIEW

Cyber Resilience Review

- **Purpose:** Evaluate operational resilience and cybersecurity practices of **critical services.**
- Delivery: Either
  - CSA-facilitated, or
  - Self-administered
- Benefits include: Helps public and private sector partners understand and measure cybersecurity capabilities as they relate to operational resilience and cyber risk



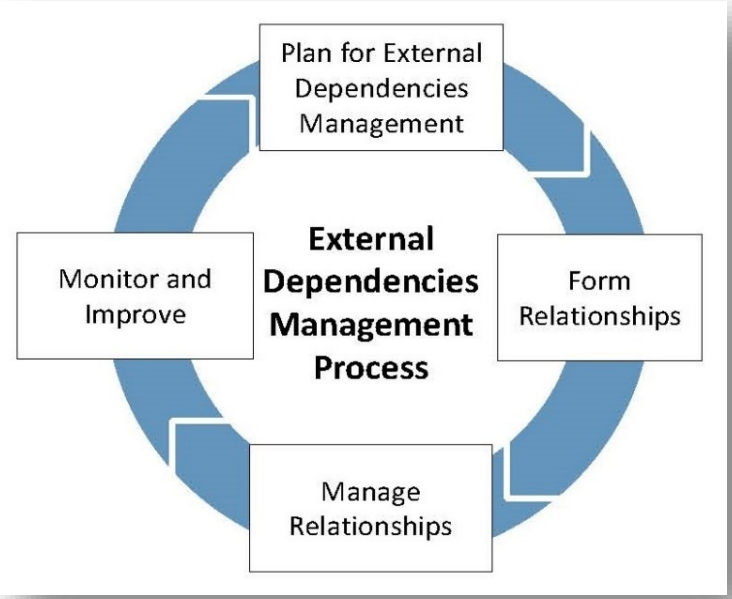
CRR Question Set & Guidance

CISA CYBER+INFRASTRUCTURE

EXTERNAL DEPENDENCIES MANAGEMENT ASSESSMENT

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



EDM process outlined per the External Dependencies Management Resource Guide

CYBER INFRASTRUCTURE SURVEY

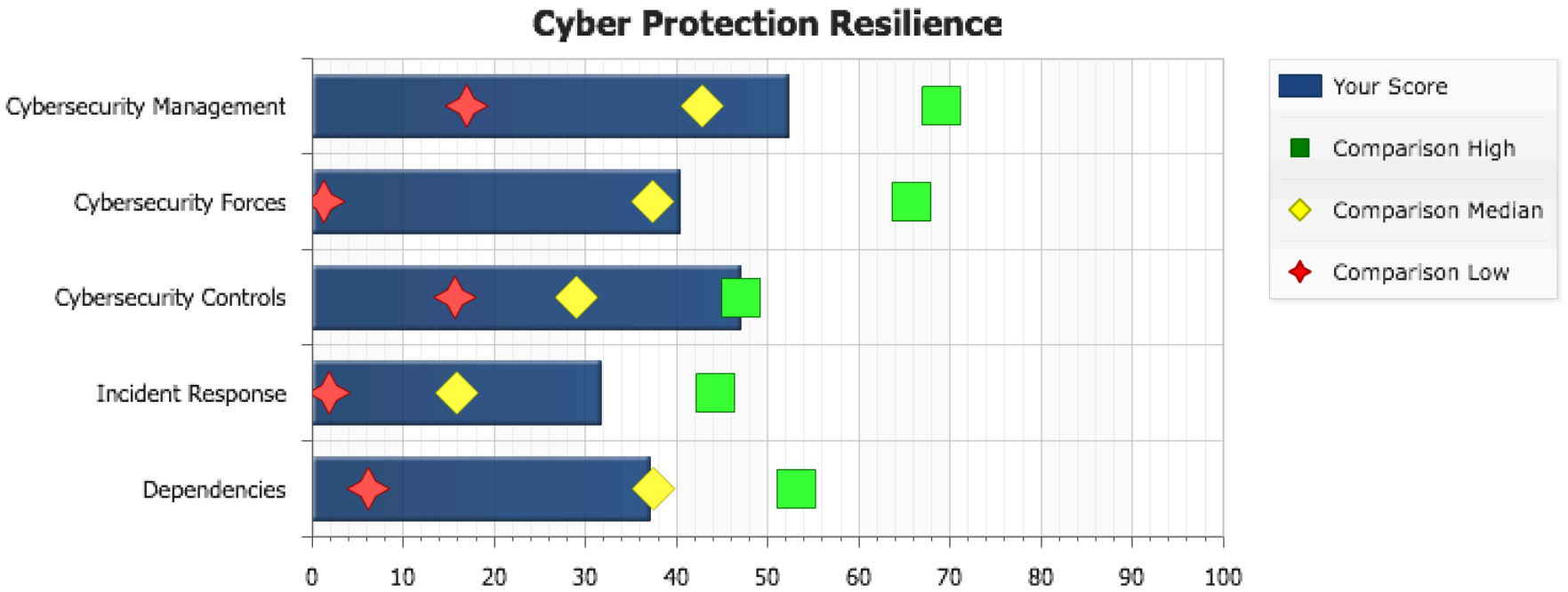
Cyber Infrastructure Survey Highlights

- Purpose: Evaluate security controls, cyber preparedness, overall resilience.
- Delivery: CSA-facilitated
- Benefits:
  - Effective assessment of cybersecurity controls in place for a critical service,
  - Easy-to-use interactive dashboard to support cybersecurity planning and resource allocation), and
  - Access to peer performance data visually depicted on the dashboard.

CISA
CYBER+INFRASTRUCTURE

CIS Dashboard - Comparison

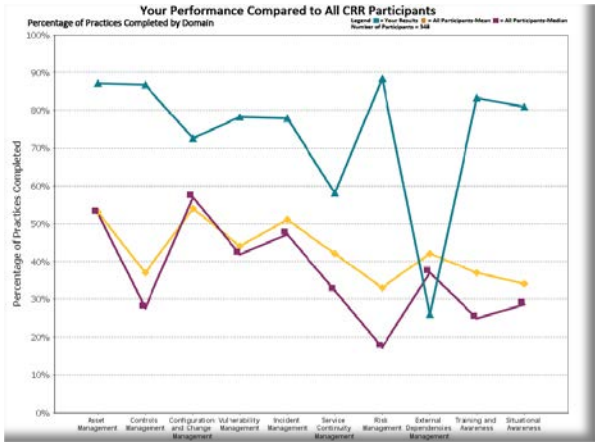
- Shows the low, median, and high performers
- Compares your organization to the aggregate



CISA CYBER+INFRASTRUCTURE

CRR Sample Report

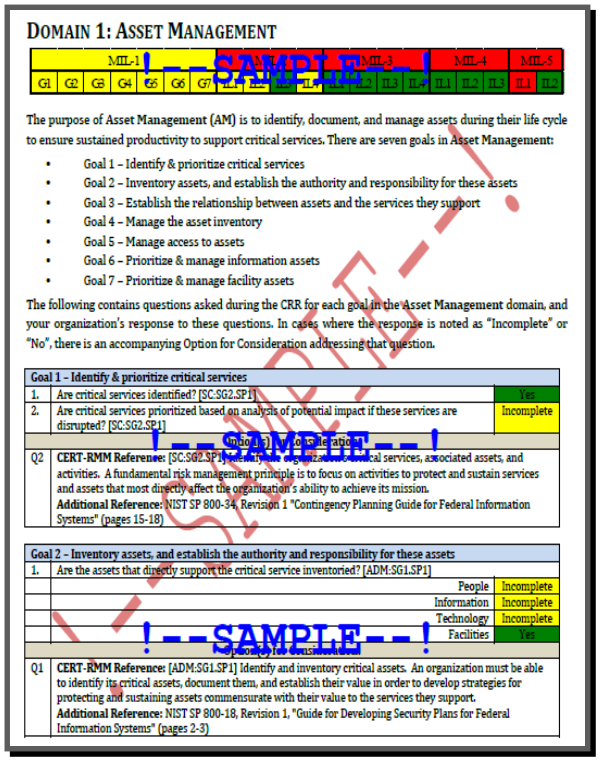
Each CRR report includes:



Comparison data with other CRR participants
**facilitated only*

A summary "snapshot" graphic, related to the **NIST Cyber Security Framework**.

Domain performance of existing cybersecurity capability and options for consideration for all responses



DOMAIN 1: ASSET MANAGEMENT

MIL-1 | MIL-2 | MIL-3 | MIL-4 | MIL-5
G1 | G2 | G3 | G4 | G5 | G6 | G7 | IL1 | IL2 | IL3 | IL4 | IL1 | IL2 | IL3 | IL1 | IL2

The purpose of Asset Management (AM) is to identify, document, and manage assets during their life cycle to ensure sustained productivity to support critical services. There are seven goals in Asset Management:

- Goal 1 – Identify & prioritize critical services
- Goal 2 – Inventory assets, and establish the authority and responsibility for these assets
- Goal 3 – Establish the relationship between assets and the services they support
- Goal 4 – Manage the asset inventory
- Goal 5 – Manage access to assets
- Goal 6 – Prioritize & manage information assets
- Goal 7 – Prioritize & manage facility assets

The following contains questions asked during the CRR for each goal in the Asset Management domain, and your organization's response to these questions. In cases where the response is noted as "Incomplete" or "No", there is an accompanying Option for Consideration addressing that question.

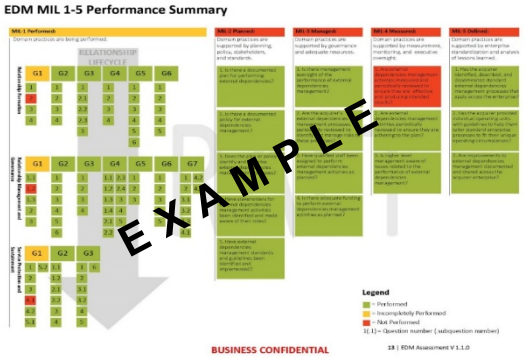
Goal 1 – Identify & prioritize critical services		
1.	Are critical services identified? [SC:SG2.SP1]	Yes
2.	Are critical services prioritized based on analysis of potential impact if these services are disrupted? [SC.SG2.SP1]	Incomplete
	Option for Consideration	
Q2	**CERT-RMM Reference:** [SC:SG2.SP1] Identify and prioritize critical services, associated assets, and activities. A fundamental risk management principle is to focus on activities to protect and sustain services and assets that most directly affect the organization's ability to achieve its mission. **Additional Reference:** NIST SP 800-34, Revision 1 "Contingency Planning Guide for Federal Information Systems" (pages 15-18)	

Goal 2 – Inventory assets, and establish the authority and responsibility for these assets		
1.	Are the assets that directly support the critical service inventoried? [ADM:SG1.SP1]	
	People	Incomplete
	Information	Incomplete
	Technology	Incomplete
	Facilities	Yes
	Option for Consideration	
Q1	**CERT-RMM Reference:** [ADM:SG1.SP1] Identify and inventory critical assets. An organization must be able to identify its critical assets, document them, and establish their value in order to develop strategies for protecting and sustaining assets commensurate with their value to the services they support. **Additional Reference:** NIST SP 800-18, Revision 1, "Guide for Developing Security Plans for Federal Information Systems" (pages 2-3)	

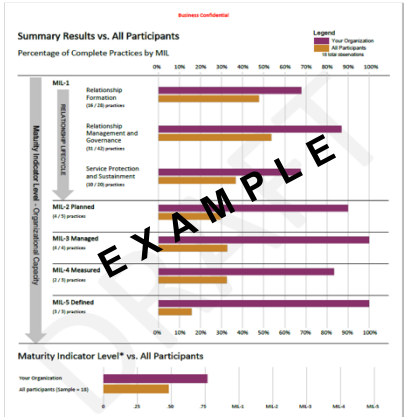
EDM Assessment Report

Each EDM report includes:

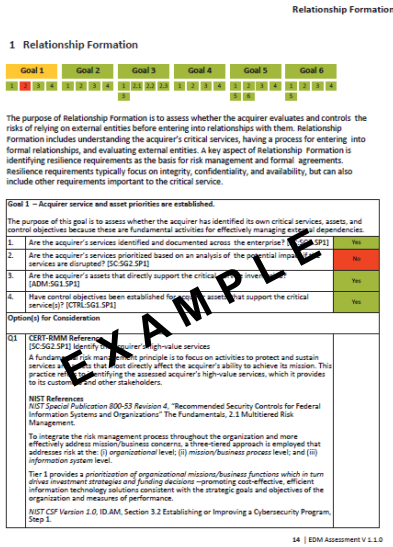
- Performance summary of existing capability managing external dependencies



- Comparison data with other EDM participants



- Sub-domain performance of existing capability managing external dependencies and options for consideration for all responses



CISA CYBER+INFRASTRUCTURE

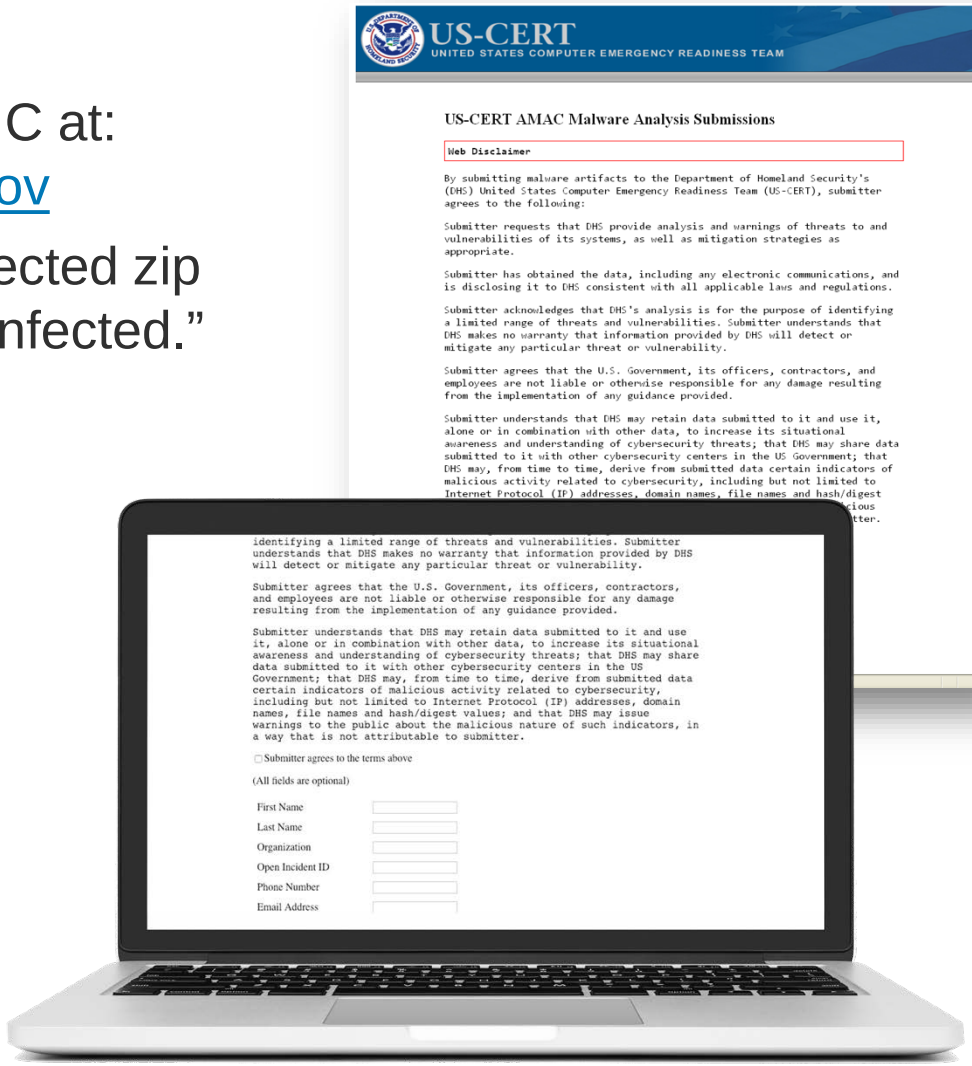
Risk Response Choises

- The choices for the risk response were:
  - Accept - No action is taken to respond to the risk based on the insignificance of the risk and/or the residual falls w/in risk tolerance
  - Avoid - Action is taken to stop the operational process or the part of the operational process causing the risk
  - Control - Action is taken to reduce the likelihood or magnitude of impact of the risk
  - Transfer - Action is taken to transfer or share risks across the entity or with external parties, such as insuring against losses
  - Pursue - action is taken to consciously seek out opportunity in light of the risk

Malware Analysis

To submit malware:

- Email submissions to NCCIC at: submit@malware.us-cert.gov
  - Send in password-protected zip file(s). Use password “infected.”
- Upload submission online: https://malware.us-cert.gov



CISA CYBER+INFRASTRUCTURE

Federal Role in Cyber Incident Response, 2 of 2

Threat Response	Asset Response
Federal Bureau of Investigation 855-292-3937 or cywatch@ic.fbi.gov	**CISA NCCIC** 888-282-0870 or NCCIC@hq.dhs.gov Report suspected or confirmed cyber incidents, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to further improve security.
U.S. Secret Service secretservice.gov/contact/field-offices	
Immigration and Customs Homeland Security Investigations 866-347-2423 or ice.gov/contact/hsi	**Report Internet Crimes**: FBI Internet Crime Complaint Center ic3.gov

CISA CYBER+INFRASTRUCTURE

Sampling of Cybersecurity Offerings

- **Preparedness Activities**
  - Information / Threat Indicator Sharing
  - Cybersecurity Training and Awareness
  - Cyber Exercises and “Playbooks”
  - National Cyber Awareness System
  - Vulnerability Notes Database
  - Information Products and Recommended Practices
  - Cybersecurity Evaluations
    - Cyber Resilience Reviews (CRR™)
    - Cyber Infrastructure Surveys
    - Phishing Campaign Assessment
    - Vulnerability Scanning
    - Risk and Vulnerability Assessments (aka “Pen” Tests)
    - External Dependency Management Reviews
    - Cyber Security Evaluation Tool (CSET™)
    - Validated Architecture Design Review (VADR)

- **Response Assistance**
  - Remote / On-Site Assistance
  - Malware Analysis
  - Hunt and Incident Response Teams
  - Incident Coordination

- **Cybersecurity Advisors**
  - Assessments
  - Working group collaboration
  - Best Practices private-public
  - Incident assistance coordination

- **Protective Security Advisors**
  - Assessments
  - Incident liaisons between government and private sector
  - Support for National Special Security Events

CISA
CYBER+INFRASTRUCTURE

EDM Assessment Organization and Structure

- Structure and scoring similar to Cyber Resilience Review
- Uses one Maturity Indicator Level (MIL) scale with three lifecycle domains.

Relationship Formation *Assesses whether the acquirer evaluates and controls the risks of relying on external entities before entering into relationships with them.*
Relationship Management and Governance *Assesses whether the acquirer manages ongoing relationships to maintain the resilience of the critical service, and mitigate dependency risk.*
Service Protection and Sustainment *Asseses whether the acquirer accounts for its dependence on external entities as part of its operational activities around managing incidents, disruptions, and threats.*

Example of CIS Dashboard

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

Threat-based PMI:
- ❑ Natural Disaster
- ❑ Distributed Denial-of-Service
- ❑ Remote Access Compromise
- ❑ System Integrity Compromise

CISA CYBER+INFRASTRUCTURE

Home | Logout

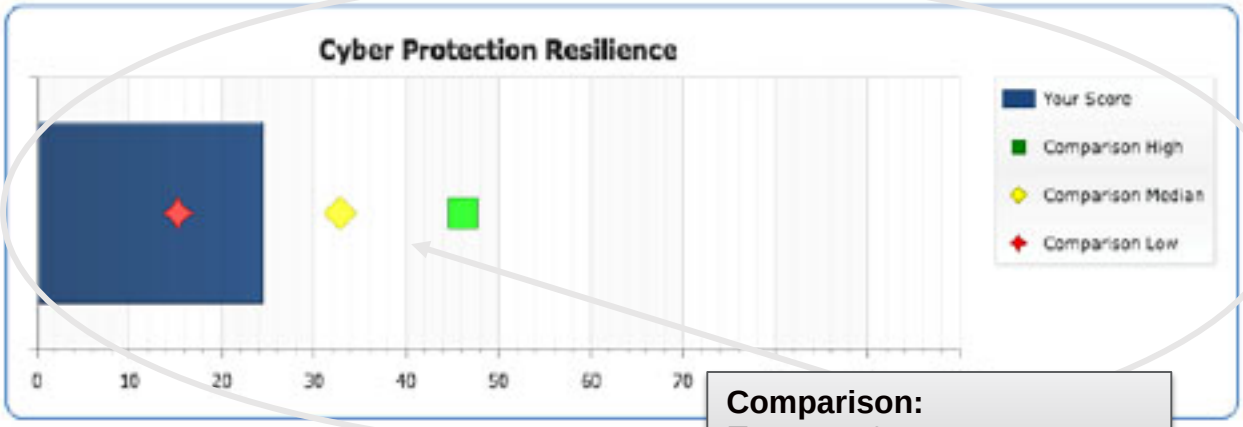
Cyber Infrastructure Survey for

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



Comparison:
- ❑ Low Performers
- ❑ Median Performers
- ❑ High Performers

VALIDATED ARCHITECTURE DESIGN REVIEW

CISA
CYBER+INFRASTRUCTURE

Validated Architecture Design Review

Purpose: Analyze network architecture, system configurations, log file review, network traffic and data flows to identify abnormalities in devices and communications traffic.

Delivery: CISA staff working with entity staff

Benefits:

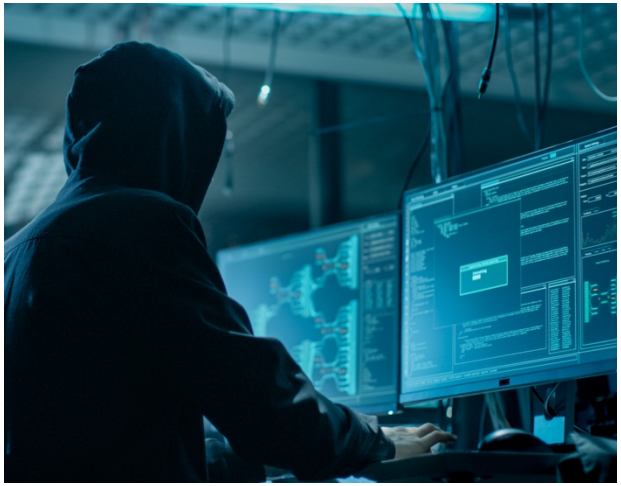
- In-depth review of network and operating system
- Recommendations to improve an organization's operational maturity and enhancing their cybersecurity posture
- Evaluation of network architecture

CISA
CYBER+INFRASTRUCTURE

RISK AND VULNERABILITY ASSESSMENT
[PENETRATION TEST]

Risk and Vulnerability Assessment

- **Purpose**: Perform network penetration and deep technical analysis of enterprise IT systems and an organization's external resistance to specific IT risks
- **Delivery**: Onsite by CISA
- **Benefits**:
  - Identification of vulnerabilities
  - Specific remediation recommendations
  - Improves an entity's cyber posture, limits exposure, reduces rates of exploitation
  - Increases speed and effectiveness of future cyber attack responses.



CISA CYBER+INFRASTRUCTURE

Risk and Vulnerability Assessment Specifics

Assessment Aspects

Service	Description
Vulnerability Scanning and Testing	Conduct Vulnerability Assessments
Penetration Testing	Exploit weakness, test responses in systems, applications, network, and security controls
Social Engineering	Craft e-mail at targeted audience to test security awareness, used as an attack sector to internal network
Wireless Discovery & Identification	Identify wireless signals and 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