CISA CYBERSECURITY SERVICES

Kenneth Stacy
Supervisory Cybersecurity Advisor (CSA)
CISA Region 4 – Tampa, FL
Cybersecurity and Infrastructure Security Agency

CISA
CYBER+INFRASTRUCTURE

Kenneth D. Stacy, CISSP, ISSEP, CGRC

Ken is a SCSA for the Cybersecurity and Infrastructure Security Agency (CISA). In this role directs and provides cybersecurity engagements with stakeholders to help secure businesses, organizations, and information across 16 critical infrastructure sectors. Prior to joining CISA, Ken served 23 years in the United States Air Force (USAF) in the Metrology and Communications career fields. Upon retirement from the USAF, he worked in private industry providing defensive cybersecurity engineering services to 12 main European operating bases for the United States Air Forces in Europe. Since 2004, Ken has served as a government civilian employee in a variety of cybersecurity roles within the Department of Defense, the Department of the Interior, and the United States Postal Service. Ken has 20 years of experience in the domains of cybersecurity risk management, system & enterprise security management, defensive cyber operations, incident response, and cybersecurity program implementation and management. In 2023 Ken was awarded the Joint Meritorious Civilian Service Award for outstanding service as the Chief Information Security Officer (CISO) for the United States Africa Command.

Cybersecurity and Infrastructure Security Agency (CISA)

As America's Cyber Defense Agency and the National Coordinator for Critical Infrastructure Security and Resilience, CISA leads the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure that Americans rely on every hour of every day.

CISA

STRATEGIC PLAN

2023–2025

GOAL 1

CYBER DEFENSE:
Spearhead the National Effort to Ensure Defense and Resilience of Cyberspace

GOAL 2

RISK REDUCTION & RESILIENCE:
Reduce Risks to, and Strengthen Resilience of, America's Critical Infrastructure

GOAL 3

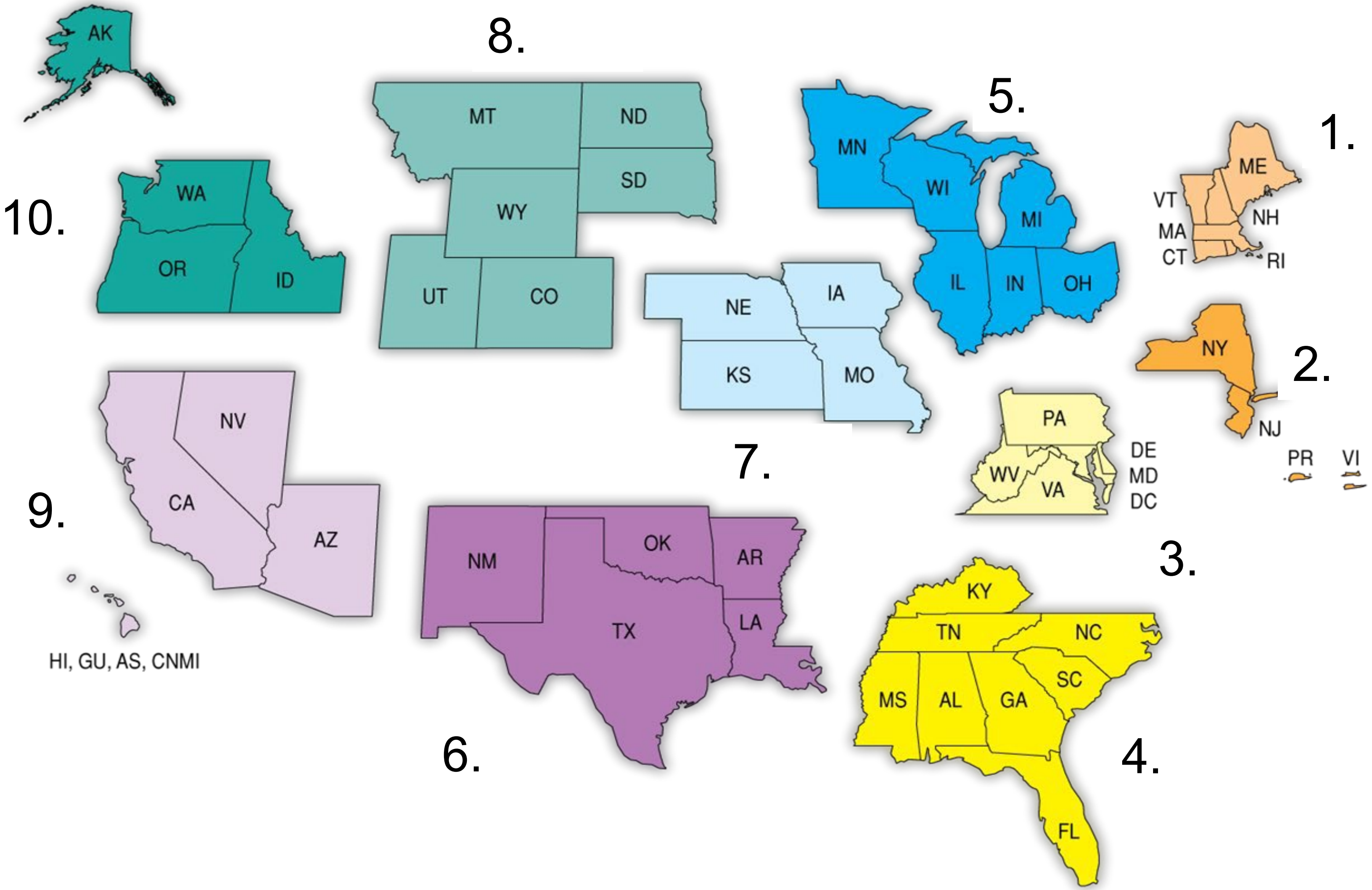
OPERATIONAL COLLABORATION:
Strengthen Whole-of-Nation Operational Collaboration and Information Sharing

GOAL 4

AGENCY UNIFICATION:
Unify as One CISA Through Integrated Functions, Capabilities, and Workforce

CSA Regions

1	Boston, MA
2	New York, NY
3	Philadelphia, PA
4	Atlanta, GA
5	Chicago, IL
6	Dallas, TX
7	Kansas City, MO
8	Denver, CO
9	Oakland, CA
10	Seattle, WA



Serving Critical Infrastructure

KEY ACTIVITIES

IDENTIFY AND VERIFY
SUSPICIOUS CYBER ACTIVITY

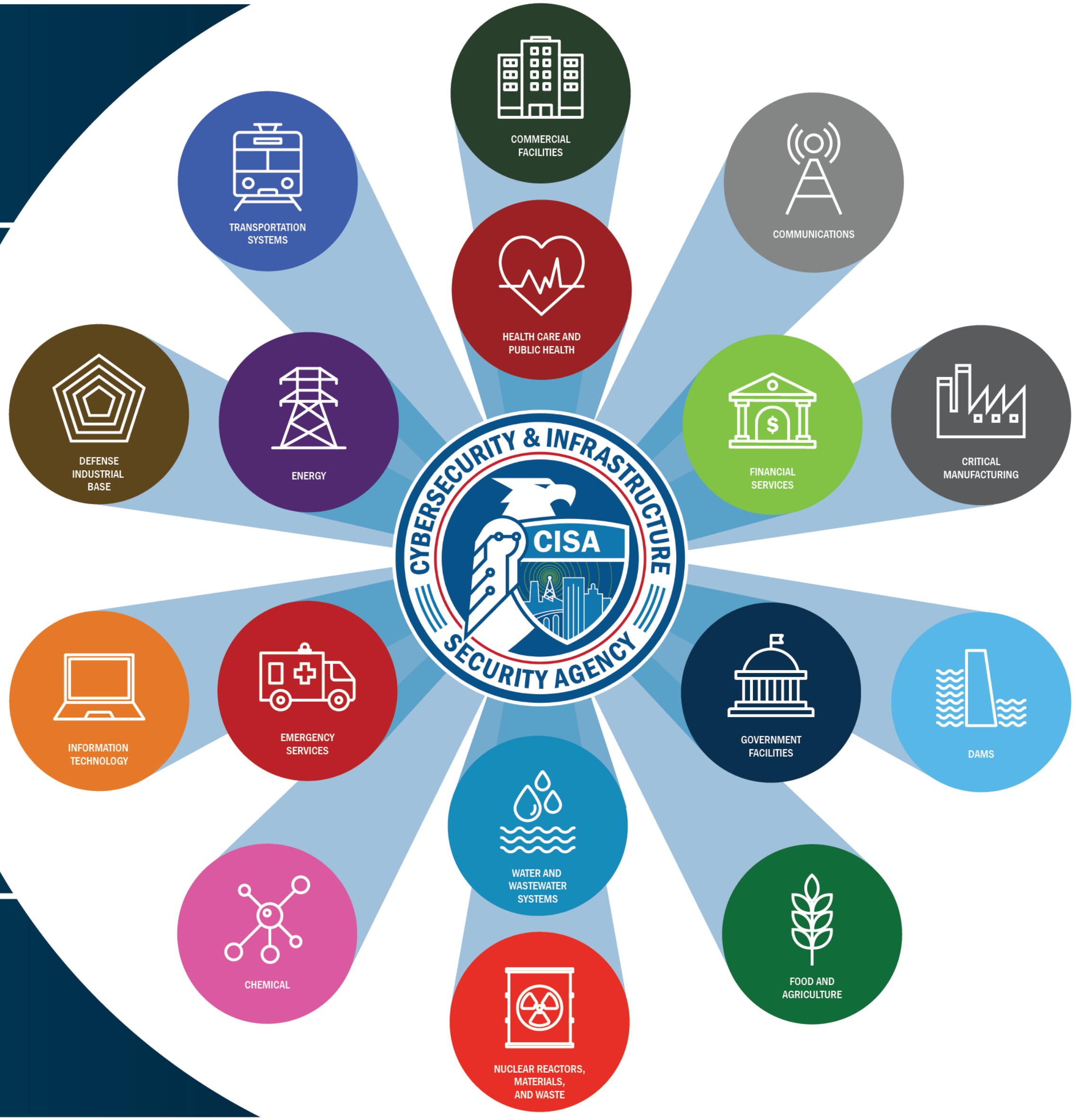
UNDERSTAND
INCIDENTS AND VULNERABILITIES

BUILD AND MAINTAIN
PARTNERSHIPS

SHARE
TIMELY AND ACTIONABLE INFORMATION

COLLABORATE
WITH PARTNERS TO MITIGATE RISK

16 CRITICAL INFRASTRUCTURE SECTORS



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

- COMMERCIAL FACILITIES
- TRANSPORTATION SYSTEMS
- COMMUNICATIONS
- HEALTH CARE AND PUBLIC HEALTH
- DEFENSE INDUSTRIAL BASE
- ENERGY
- FINANCIAL SERVICES
- CRITICAL MANUFACTURING
- INFORMATION TECHNOLOGY
- EMERGENCY SERVICES
- GOVERNMENT FACILITIES
- DAMS
- WATER AND WASTEWATER SYSTEMS
- CHEMICAL
- FOOD AND AGRICULTURE
- NUCLEAR REACTORS, MATERIALS, AND WASTE

Cybersecurity Advisor Program

To provide direct coordination, outreach, and regional support and assistance in the protection of cyber components essential to the Nation's Critical Infrastructure.

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

Cyber Preparedness
Strategic Messaging
Working Groups
Partnership
Assessments
Incident Coordination

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

CYBERSECURITY SERVICES AND ASSESSMENTS

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 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

[Protected Critical Infrastructure Information (PCII) Program | CISA]

Cybersecurity Services (Voluntary & No Cost)

Regional Resources:

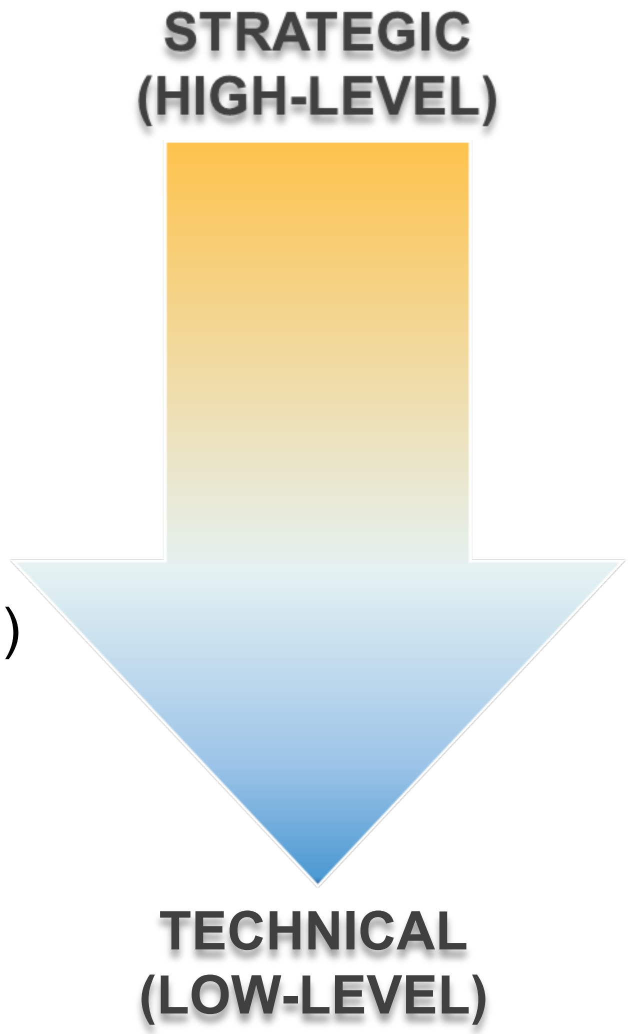
- Cyber Resilience Review (CRR)
- External Dependencies Management (EDM)
- Cyber Infrastructure Survey (CIS)
- Cybersecurity Performance Goals (CPG)
- Ransomware Readiness Assessment (RRA)

National Resources:

- Cyber Tabletop Exercises (CTTX)
- Vulnerability Scanning Service (Cyber Hygiene)
- Remote Pen Test and OT Design Reviews

Tools:

- Known Exploited Vulnerabilities (KEV)
- Cyber Security Evaluation Tool (CSET)
- Decider (MITRE ATT&CK)
- Untitled Goose (Azure)



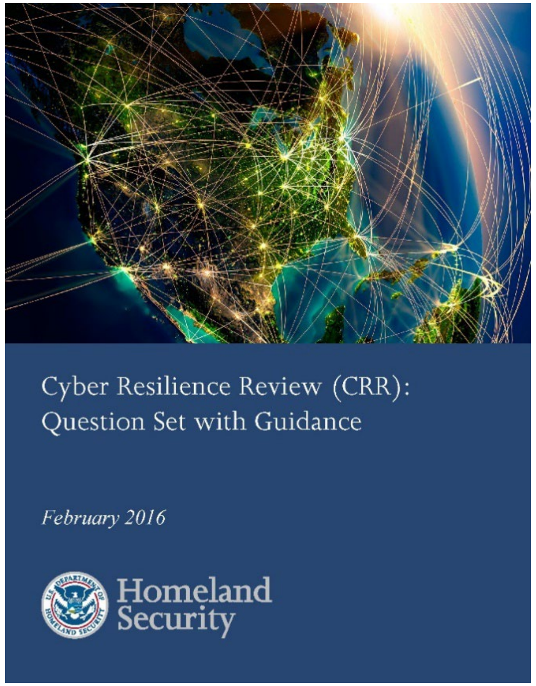
The Cyber Security Evaluation Tool (CSET®)

- Department of Homeland Security desktop software tool that assists organizations in protecting their key national cyber assets.
- Provides a systematic approach for assessing the security posture of their cyber systems and networks
- High-level and detailed questions related to all industrial control and IT systems
- Provides a plain-language explanation, references, and professionally designed reports to address issues identified in the assessment
- Ability to compare to baseline, or two separate assessments

https://www.cisa.gov/downloading-and-installing-cset

Cyber Resilience Review

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



Cyber Resilience Review (CRR):
Question Set with Guidance

February 2016

Homeland Security

https://www.cisa.gov/resources-tools/services/cyber-resilience-review-crr

Cyber Resilience Review Domains

Asset Management
Know your assets being protected & their requirements, e.g., CIA

Configuration and Change Management
Manage asset configurations and changes

Controls Management
Manage and monitor controls to ensure they are meeting your objectives

External Dependencies Management
Know your most important external entities and manage the risks posed to essential services

Incident Management
Be able to detect and respond to incidents

Risk Management
Know and address your biggest risks that considers cost and your risk tolerances

Service Continuity Management
Ensure workable plans are in place to manage disruptions

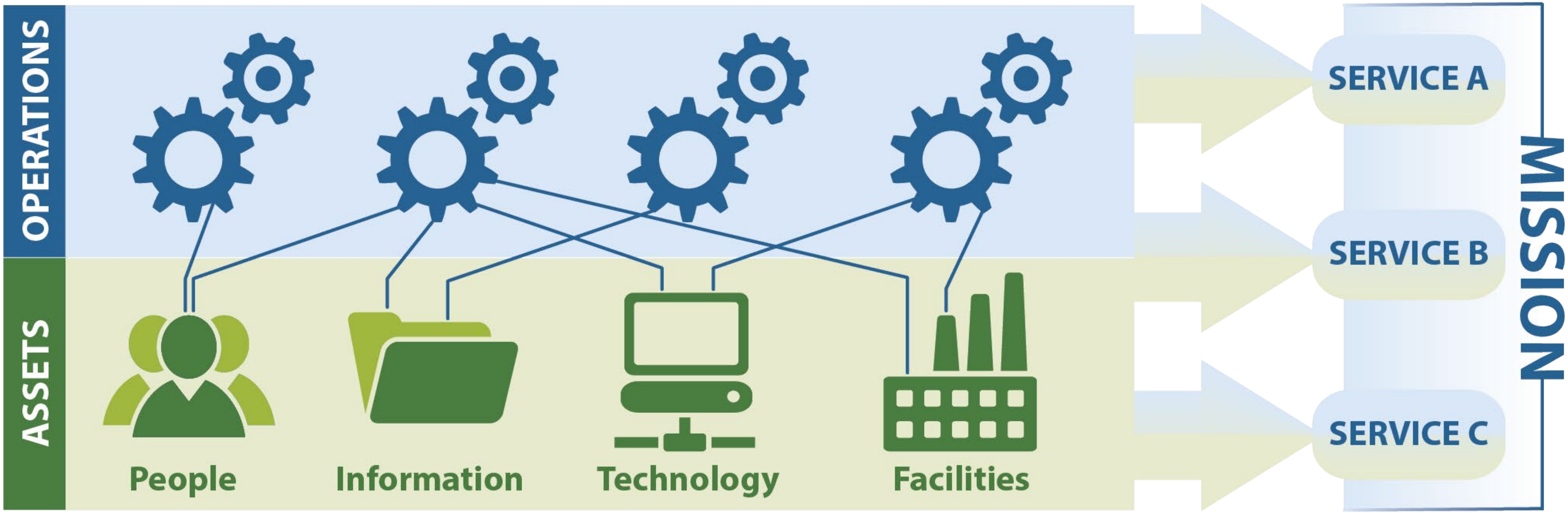
Situational Awareness
Discover and analyze information related to immediate operational stability and security

Training and Awareness
Ensure your people are trained on and aware of cybersecurity risks and practices

Vulnerability Management
Know your vulnerabilities and manage those that pose the most risk

http://www.us-cert.gov/ccubedvp

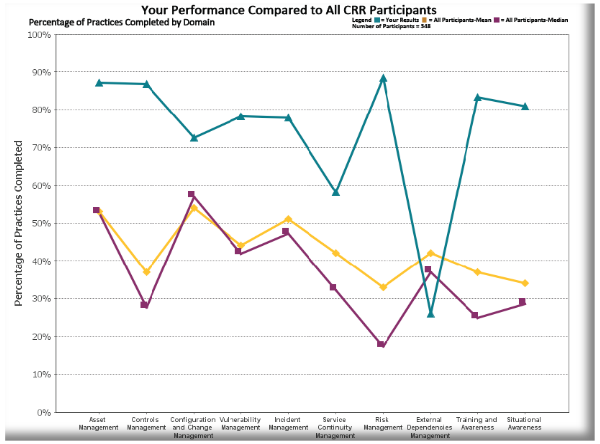
Critical Service Focus



Organizations use assets (people, information, technology, and facilities) to provide operational services and accomplish missions.

CRR Sample Report

Each CRR report includes:



Comparison data with other CRR participants

**facilitated only*

NIST Cybersecurity Framework Summary

NIST CSF Summary

Legend

Identify (ID)

Protect (PR)

Detect (DE)

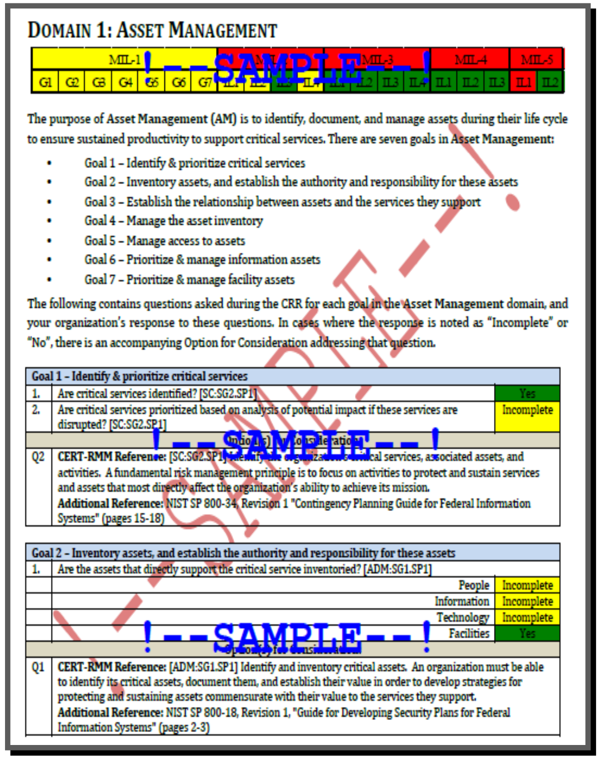
Respond (RS)

Recover (RC)

BUSINESS CONFIDENTIAL

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	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

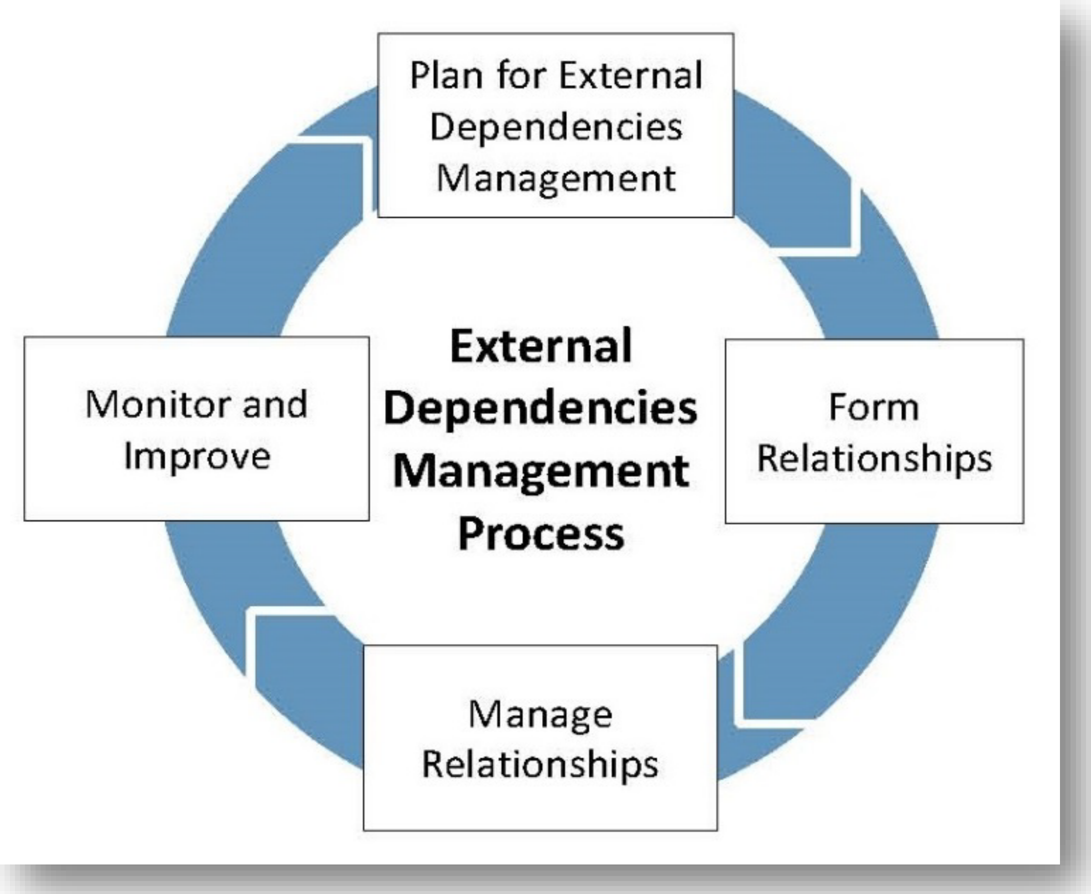
The following contains questions asked during the CRR for each goal in the Asset Management domain, and your organization's response to these questions. In cases where the response is noted as “Incomplete” or “No”, there is an accompanying Option for Consideration addressing that question.

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(s) for Consideration		
Q2	**CERT-RMM Reference:** [SC:SG2.SP1] Identify the organization's 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(s) 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)	

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 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.

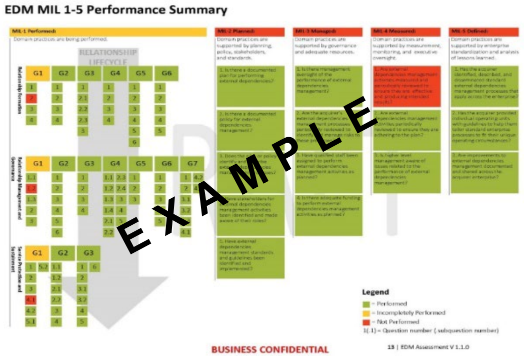
Service Protection and Sustainment

Assesses whether the acquirer accounts for its dependence on external entities as part of its operational activities around managing incidents, disruptions, and threats.

EDM Assessment Report

Each EDM report includes:

- Performance summary of existing capability managing external dependencies



EDM MIL 1-5 Performance Summary

MIL-1 Performed:	MIL-2 Planned:	MIL-3 Managed:	MIL-4 Measured:	MIL-5 Defined:
Domain practices are being performed.	Domain practices are supported by planning, policy, stakeholders, and standards.	Domain practices are supported by governance and adequate resources.	Domain practices are supported by measurement, monitoring, and executive oversight.	Domain practices are supported by enterprise standardization and analysis of lessons learned.

RELATIONSHIP LIFECYCLE
Relationship Formation
Relationship Management and Governance
Service Protection and Sustainment
G1
G2
G3
G4
G5
G6
G7

Legend
- 🟩 = Performed
- 🟨 = Incompletely Performed
- 🟥 = Not Performed
- 1(.1) = Question number (.subquestion number)

BUSINESS CONFIDENTIAL

13 | EDM Assessment V 1.1.0

EXAMPLE

- Comparison data with other EDM participants

EDM MIL-1 Performance Summary

EDM MIL-1 Summary

Total number of practices performed
Total number of practices incompletely performed
Total number of practices not performed
87
0
3
97%
Percentage of practices fully performed
practices performed
number practice questions
practices not performed
9
5
5
(example responses)
practices incompletely performed

PRACTICE LEVEL PERFORMANCE SUMMARY

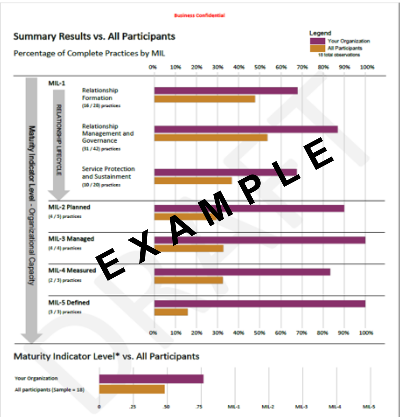
	Goal		
Relationship Formation 27 0 1 96%	**Goal 1** – Acquirer service and asset priorities are established.	4	3 / 1
	Goal 2 – Forming relationships with external entities is planned.	4	4
	Goal 3 – Risk management includes external dependencies.	5	5
	Goal 4 – External entities are evaluated.	4	4
	Goal 5 – Formal agreements include resilience requirements.	6	6
	Goal 6 – Technology asset supply chain risks are managed.	5	
Relationship Management and Governance 41 0 1 98%	**Goal 1** – External dependencies are identified and prioritized.	5	4 / 1
	Goal 2 – Supplier risk management is cont[illegible]	6	6
	Goal 3 – Supplier performance [illegible] governed and managed.	4	4
	Goal 4 – Change and capacity [illegible] are applied to external dependencies.	11	11
	[illegible] Supplier [illegible] are managed.	3	3
	[illegible] Infrastructure and governmental dependencies are managed.	5	5
	Goal 7 – External entity access to acquirer assets is managed.	8	8
Service Protection and Sustainment 19 0 1 95%	**Goal 1** – Disruption planning includes external dependencies.	7	6 / 1
	Goal 2 – Planning and controls are maintained and updated.	6	6
	Goal 3 – Situational awareness extends to external dependencies.	7	7

DRAFT

EXAMPLE

BUSINESS CONFIDENTIAL

11 | EDM Assessment V 1.1.0



Business Confidential

Summary Results vs. All Participants

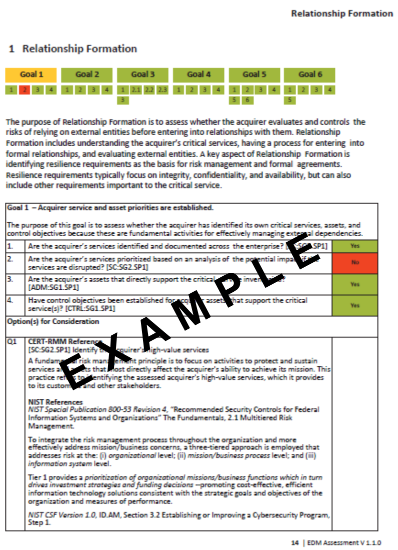
Percentage of Complete Practices by MIL

Maturity Indicator Level* vs. All Participants

DRAFT

EXAMPLE

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



Relationship Formation

1 Relationship Formation

The purpose of Relationship Formation is to assess whether the acquirer evaluates and controls the risks of relying on external entities before entering into relationships with them. Relationship Formation includes understanding the acquirer's critical services, having a process for entering into formal relationships, and evaluating external entities. A key aspect of Relationship Formation is identifying resilience requirements as the basis for risk management and formal agreements. Resilience requirements typically focus on integrity, confidentiality, and availability, but can also include other requirements important to the critical service.

Goal 1 – Acquirer service and asset priorities are established. The purpose of this goal is to assess whether the acquirer has identified its own critical services, assets, and control objectives because these are fundamental activities for effectively managing external dependencies.		
1.	Are the acquirer's services identified and documented across the enterprise? [SC:SG1.SP1]	Yes
2.	Are the acquirer's services prioritized based on an analysis of the potential impact if the services are disrupted? [SC:SG2.SP1]	No
3.	Are the acquirer's assets that directly support the critical service inventoried? [ADM:SG1.SP1]	Yes
4.	Have control objectives been established for acquirer assets that support the critical service(s)? [CTRL:SG1.SP1]	Yes
Option(s) for Consideration		
Q1	**CERT-RMM Reference** [SC:SG2.SP1] Identify the acquirer's high-value services A fundamental risk management principle is to focus on activities to protect and sustain services and assets that most directly affect the acquirer's ability to achieve its mission. This practice refers to identifying the assessed acquirer's high-value services, which it provides to its customers and other stakeholders. **NIST References** *NIST Special Publication 800-53 Revision 4*, "Recommended Security Controls for Federal Information Systems and Organizations" The Fundamentals, 2.1 Multitiered Risk Management. To integrate the risk management process throughout the organization and more effectively address mission/business concerns, a three-tiered approach is employed that addresses risk at the: (i) *organizational* level; (ii) *mission/business process* level; and (iii) *information system* level. Tier 1 provides a *prioritization of organizational missions/business functions which in turn drives investment strategies and funding decisions* --promoting cost-effective, efficient information technology solutions consistent with the strategic goals and objectives of the organization and measures of performance. *NIST CSF Version 1.0*, ID.AM, Section 3.2 Establishing or Improving a Cybersecurity Program, Step 1.	

EXAMPLE

14 | EDM Assessment V 1.1.0

Cybersecurity Performance Goals (CPG)

- A baseline set of cybersecurity practices applicable across critical infrastructure with known risk-reduction value
- A combination of recommended practices for IT/OT/ICS owners, including a prioritized set of security practices.
- Mapped to the relevant NIST Cybersecurity Framework subcategories
- CISA is working to generate sector specific goals for 16 critical infrastructure
  - The first four are Energy, Financial Services, IT, and Chemical Sectors.

https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

Ransomware Readiness Assessment

- No Cost Voluntary Self Assessment Module of the Cybersecurity Evaluation tool (CSET)

- Systematic process to evaluate operational and information technology network security against a ransomware threat.

- Provides a dashboard to present the assessment results in both summary and detailed form.

https://www.cisa.gov/news-events/alerts/2021/06/30/cisas-cset-tool-sets-sights-ransomware-threat

Vulnerability Scanning / Hygiene

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

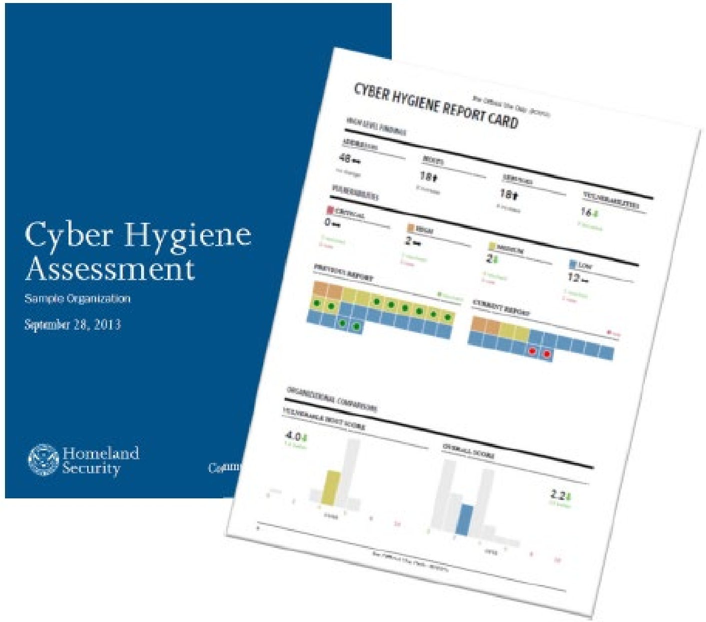
Delivery: Identify public-facing Internet security risks, through service enumeration and vulnerability scanning online by CISA.

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



Cyber Hygiene Assessment

Sample Organization

September 28, 2013

Homeland Security

CYBER HYGIENE REPORT CARD

https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services

Pre-Ransomware Notification Program

- Ransomware actors often take time before encrypting or stealing information, a window of time that often lasts from hours to days (dwell time).

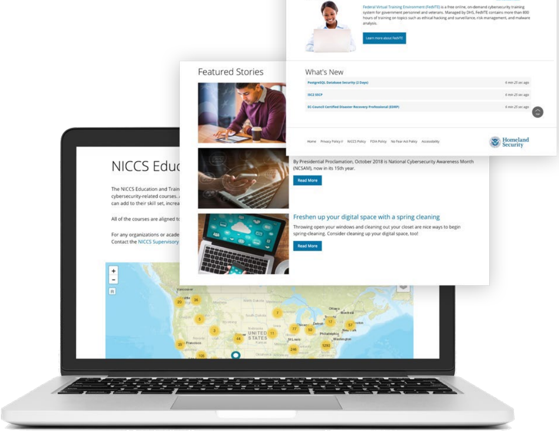
- CISA receives tips from the cybersecurity research community, infrastructure providers, and threat intelligence companies about potential early-stage ransomware activity.

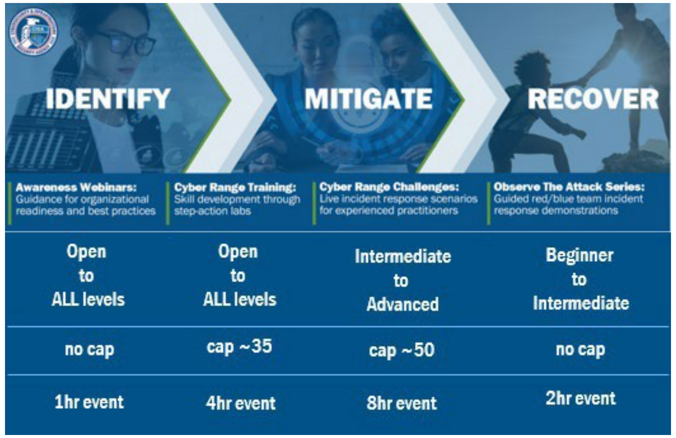
- Local CISA field forces receive notification and contact the affected entity.

https://www.cisa.gov/stopransomware

Cybersecurity Training Resources

- **National Initiative for Cybersecurity Careers and Studies (NICCS) website:** Searchable Training Catalog with over 6,000 cyber- related courses offered by nationwide cybersecurity educators
    - Workforce Framework for Cybersecurity (NICE Framework)
    - Federal Virtual Training Environment (FedVTE)
    - Scholarships for Service, Centers for Academic Excellence, and Cyber Competitions
    - Tools and resources for cyber managers
- Incident Response Training
- Industrial Control Systems Training and Assessments





IDENTIFY	MITIGATE		RECOVER
Awareness Webinars: Guidance for organizational readiness and best practices	**Cyber Range Training:** Skill development through step-action labs	**Cyber Range Challenges:** Live incident response scenarios for experienced practitioners	**Observe The Attack Series:** Guided red/blue team incident response demonstrations
Open to ALL levels	Open to ALL levels	Intermediate to Advanced	Beginner to Intermediate
no cap	cap ~35	cap ~50	no cap
1hr event	4hr event	8hr event	2hr event

https://www.cisa.gov/cybersecurity-training-exercises

CISA Tabletop Exercise Packages

Tools to conduct planning exercises on a wide range of threat scenarios.

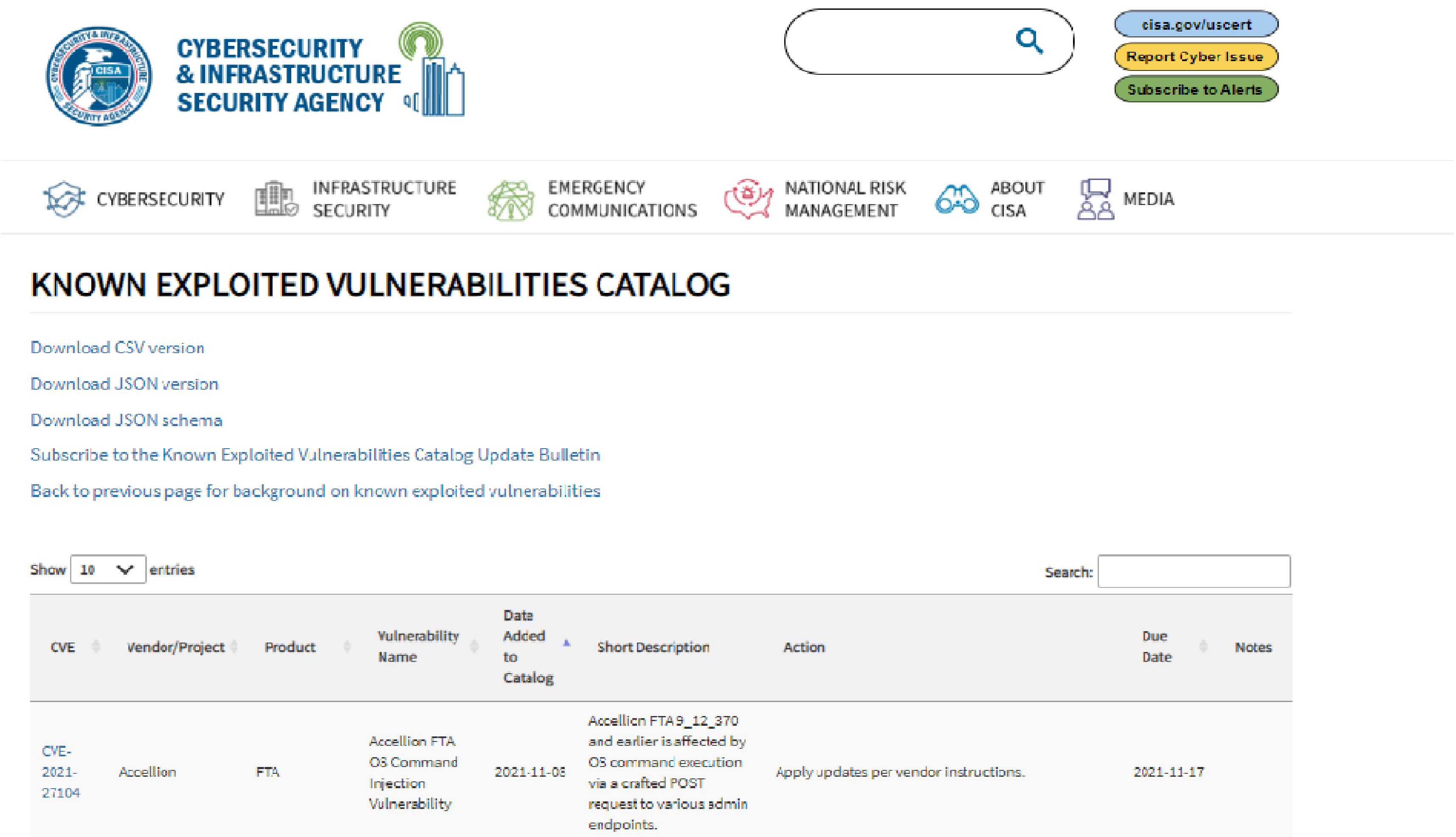
- Comprehensive set of resources designed to assist conducting your own exercises.

- Each package is customizable and includes template exercise objectives, scenarios, and discussion questions as well as a collection of references and resources.

- Scenarios cover a broad array of physical and cybersecurity topics, such as natural disasters, pandemics, civil disturbances, industrial control systems, ransomware, vehicle ramming, insider threats, and active assailants.

https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

CISA Known Exploited Vulnerabilities Catalog (KEV)



KNOWN EXPLOITED VULNERABILITIES CATALOG

Download CSV version

Download JSON version

Download JSON schema

Subscribe to the Known Exploited Vulnerabilities Catalog Update Bulletin

Back to previous page for background on known exploited vulnerabilities

CVE	Vendor/Project	Product	Vulnerability Name	Date Added to Catalog	Short Description	Action	Due Date	Notes
CVE-2021-27104	Accellion	FTA	Accellion FTA OS Command Injection Vulnerability	2021-11-03	Accellion FTA 9_12_370 and earlier is affected by OS command execution via a crafted POST request to various admin endpoints.	Apply updates per vendor instructions.	2021-11-17	

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Secure-by-Design / Secure-by-Default

- **Secure-by-Design**
  - Security of the customers is a core business requirement
  - Principles should be implemented during the design phase of a product's development lifecycle
  - Use memory safe programming languages such as C#, Rust, Ruby, Java, Go, and Swift
- **Secure-by-Default**
  - Products secure to use out of the box with little to no configuration
  - Encryption in transit and at rest, integrity checking, phishing-resistant MFA, zero-trust principles, and automatic and signed software updates

Together, these two principles move the burden of staying secure to the **manufacturers.**

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

https://www.cisa.gov/securebydesign

SHIELDS UP

To Wrap Up: Key Takeaways

1. Become familiar with CISA webpage and Subscribe to CISA Advisories
    - www.cisa.gov
2. Engage with your local CISA region and contact your CSA
    - http://www.cisa.gov/about/contact-us
3. Sign-up for CISA's cyber hygiene services and other resilience services
    - Engage your local CSA
4. Report suspected Cyber Incidents to CISA Central
    - Call 888-282-0870 or email central@cisa.gov (24/7)

Contact

CISA Contact Information

Ken Stacy SCSA (Tampa)	kenneth.stacy@cisa.dhs.gov (202) 765-4247
Neal Arnold CSA (Orlando)	neal.arnold@cisa.dhs.gov (202) 394-8316

General Inquiries

CISARegion4@hq.dhs.gov

CISA Central

central@cisa.gov

FBI Internet Crime Complaint Center

www.ic3.gov