Cybersecurity Services For Building Cyber Resilience and Reducing Risk

Sean McCloskey
Branch Chief
Cybersecurity Advisor Program
Cybersecurity and Infrastructure Security Agency

October 5, 2020

CISA
CYBER+INFRASTRUCTURE

WHO WE ARE

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Who We Are

CISA works with public sector, private sector, and government partners to share information, build greater trust, and lead the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

FEDERAL NETWORK PROTECTION

PROACTIVE CYBER PROTECTION

INFRASTRUCTURE RESILIENCE & FIELD OPERATIONS

EMERGENCY COMMUNICATIONS

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

A Nation with secure and resilient critical infrastructure that ensures our security, economic prosperity, and way of life.

MISSION

Strengthen the Nation's cyber and physical infrastructure by managing and reducing systemic and catastrophic risk in partnership with the private sector, collaboration with the public sector, and protection of federal government networks.

CYBERSECURITY ADVISOR PROGRAM

CISA
CYBER+INFRASTRUCTURE

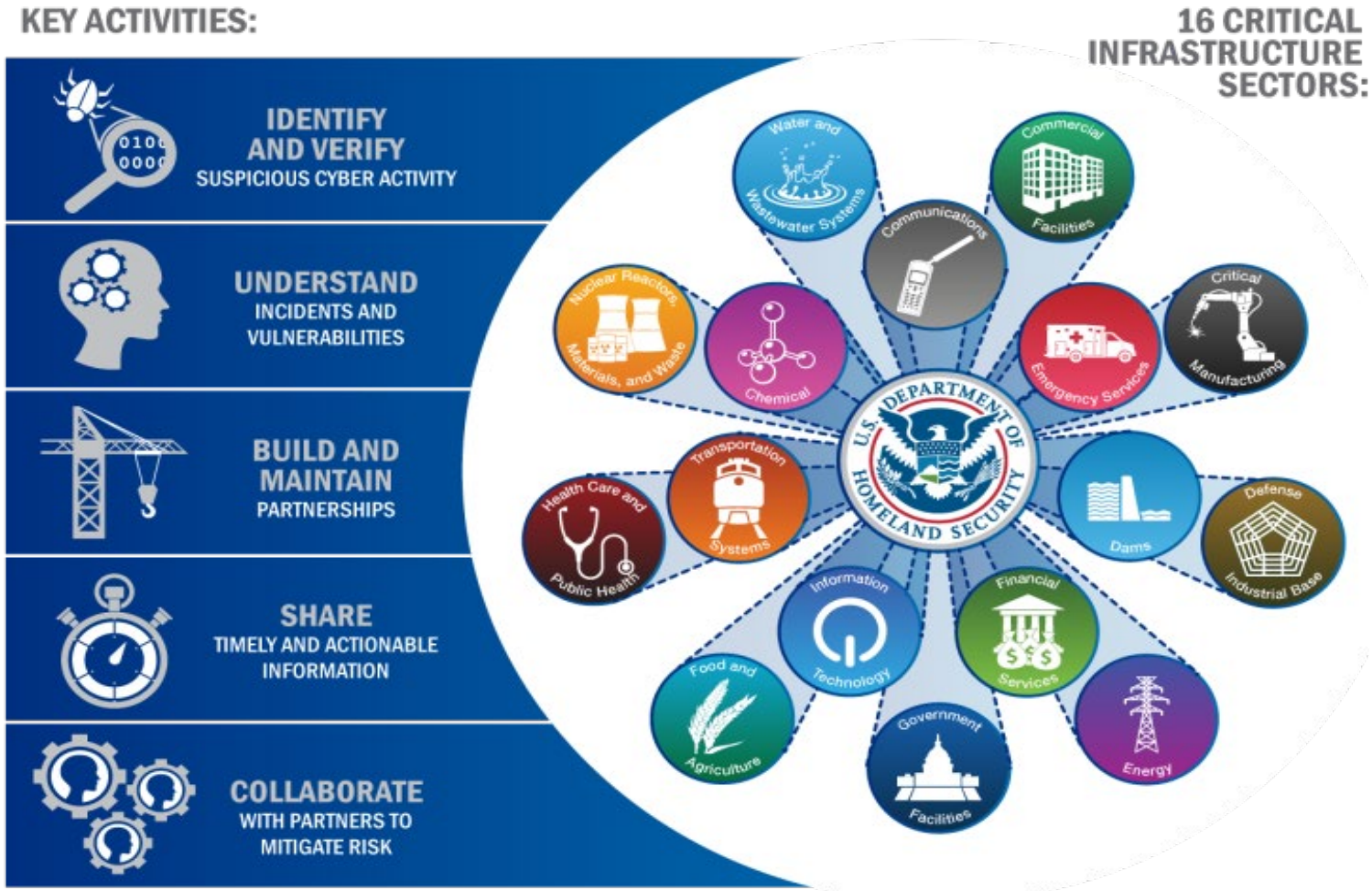
Cybersecurity Advisor Program

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):

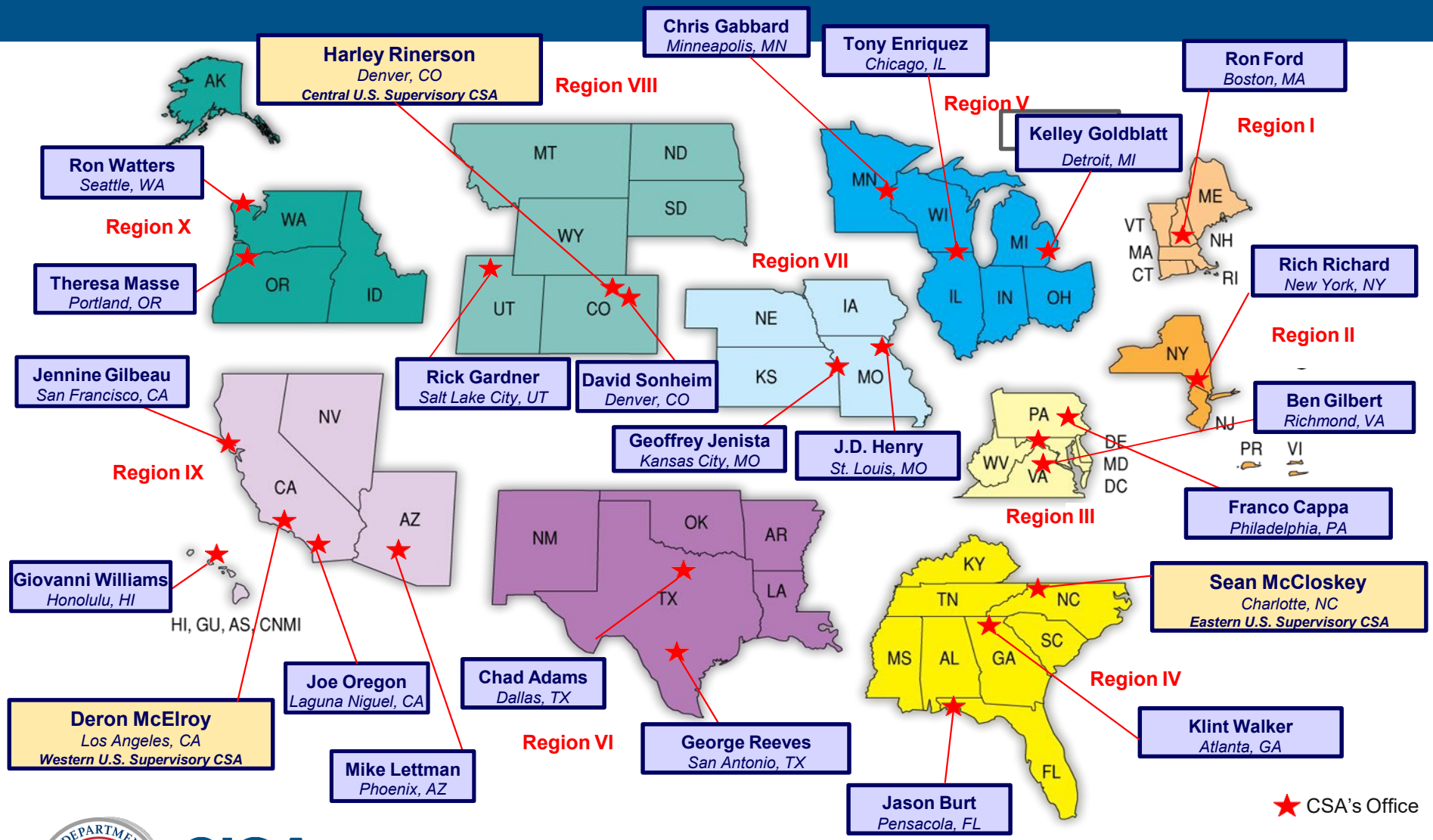
- **Assess**: Evaluate critical infrastructure cyber risk.
- **Promote**: Encourage best practices and risk mitigation strategies.
- **Build**: Initiate, develop capacity, and support cyber communities-of-interest and working groups.
- **Educate**: Inform and raise awareness.
- **Listen**: Collect stakeholder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

Serving Critical Infrastructure



CISA
CYBER+INFRASTRUCTURE

CSA Deployed Personnel



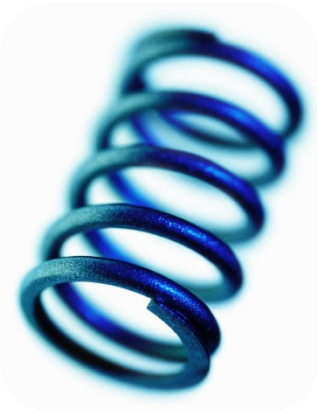
CISA
CYBER+INFRASTRUCTURE

CYBERSECURITY AND RESILIENCE

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

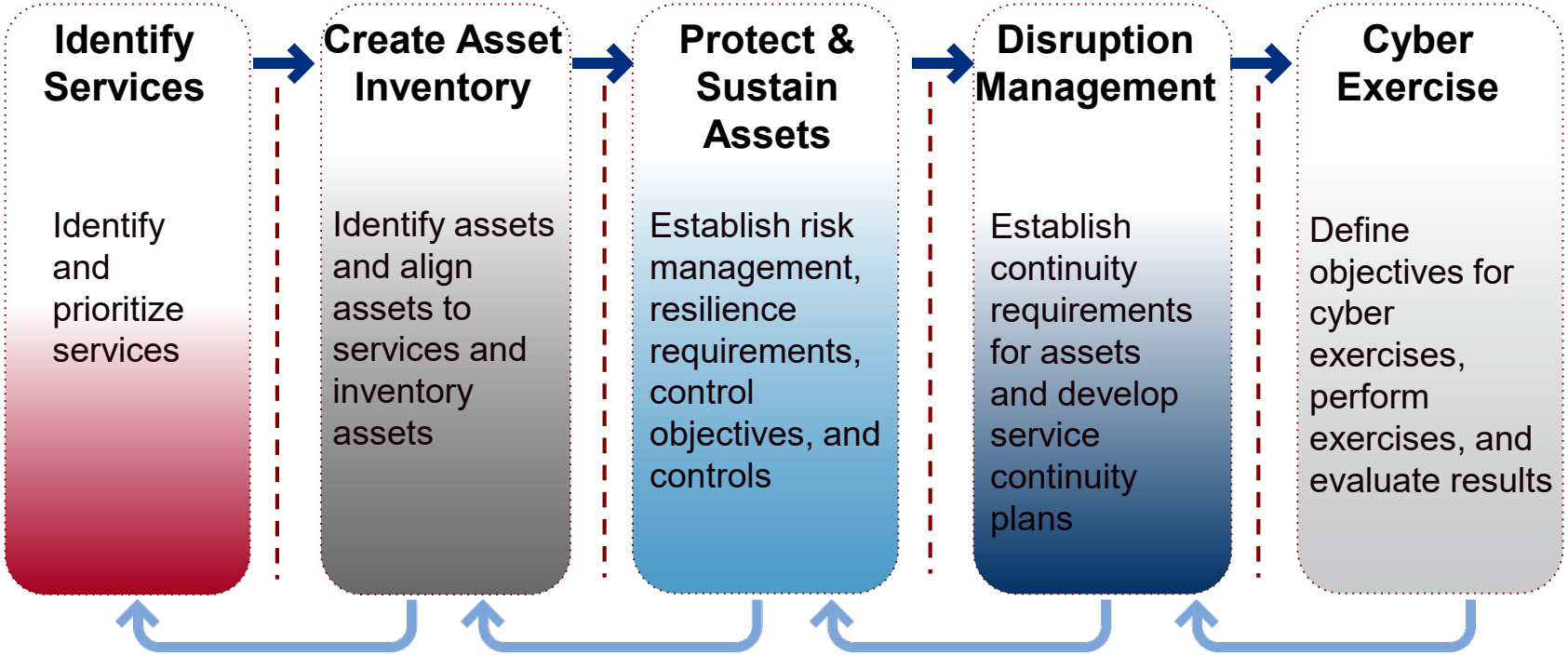
Operational resilience emerges from what we do, such as:

- 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

CISA
CYBERSECURITY SERVICES

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

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 (EVERYONE)----------
- Vulnerability Scanning / Hygiene (Technical)----------
- Validated Architecture Design Review (Technical)-------
- Risk and Vulnerability Assessment (Technical)----------

TECHNICAL
(Network-Administrator Level)

CISA
CYBER+INFRASTRUCTURE

Protected Critical Infrastructure Information Program

Protected Critical Infrastructure Information (PCII) Program Guards Your Information

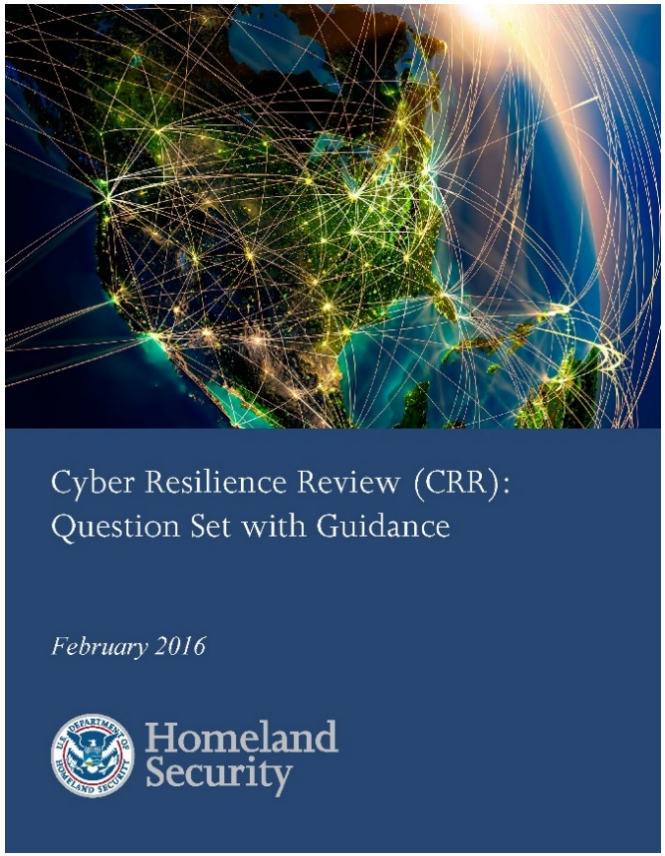
- Sensitive critical infrastructure information voluntarily given to CISA is protected by law from
  - Public release under Freedom of Information Act requests,
  - Public release under State, local, tribal, or territorial disclosure laws,
  - Use in civil litigation and
  - Use in regulatory purposes.

CISA CYBER+INFRASTRUCTURE

CYBER 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

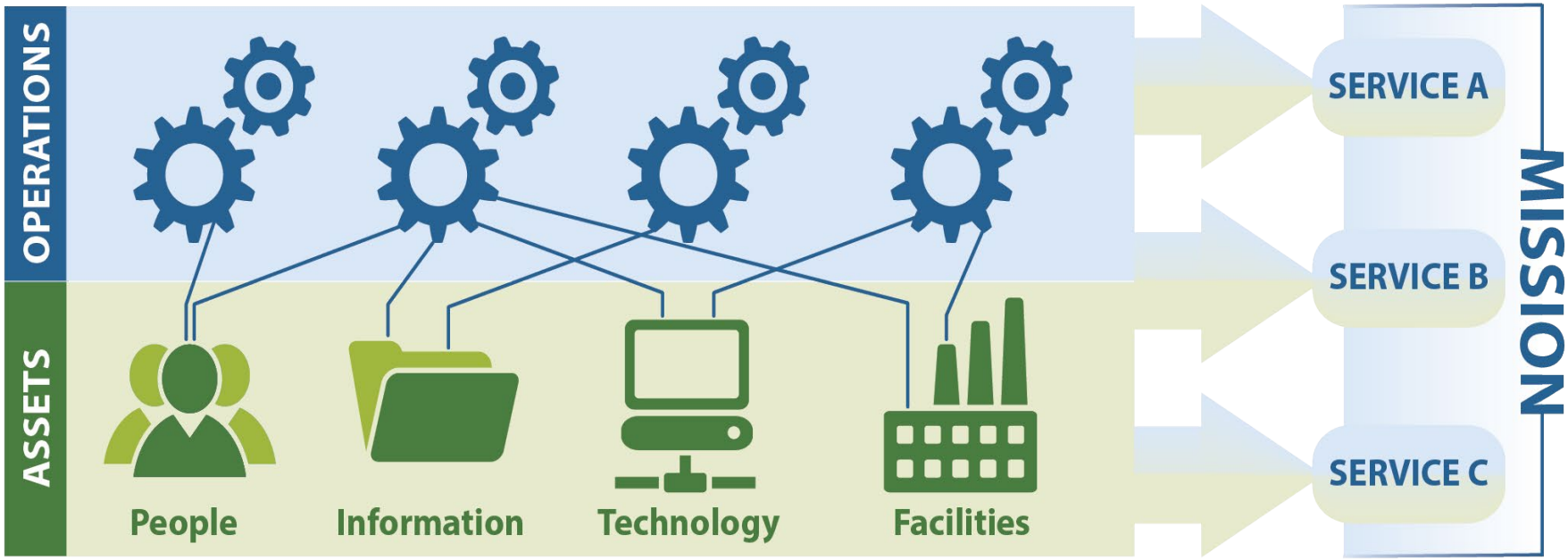


CRR Question Set & Guidance

CISA
CYBER+INFRASTRUCTURE

Critical Service Focus

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



CISA
CYBER+INFRASTRUCTURE

Cyber Resilience Review Domains

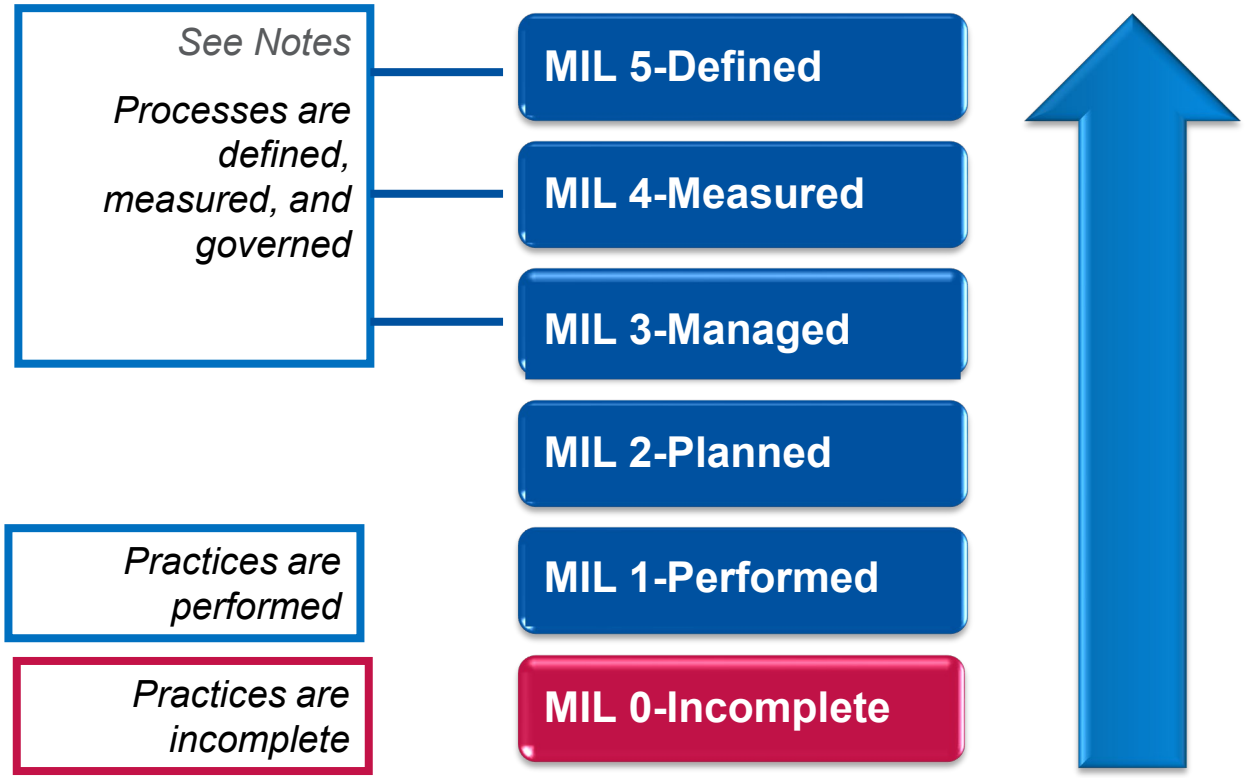
Asset Management Know your assets being protected & their requirements, e.g., CIA	**Risk Management** Know and address your biggest risks that considers cost and your risk tolerances
Configuration and Change Management Manage asset configurations and changes	**Service Continuity Management** Ensure workable plans are in place to manage disruptions
Controls Management Manage and monitor controls to ensure they are meeting your objectives	**Situational Awareness** Discover and analyze information related to immediate operational stability and security
External Dependencies Management Know your most important external entities and manage the risks posed to essential services	**Training and Awareness** Ensure your people are trained on and aware of cybersecurity risks and practices
Incident Management Be able to detect and respond to incidents	**Vulnerability Management** Know your vulnerabilities and manage those that pose the most risk

For more information: http://www.us-cert.gov/ccubedvp

CISA
CYBER+INFRASTRUCTURE

Process Institutionalization

CRR maturity indicator levels (MILs) are to measure process institutionalization:



Higher MIL degrees translate to more stable processes that:

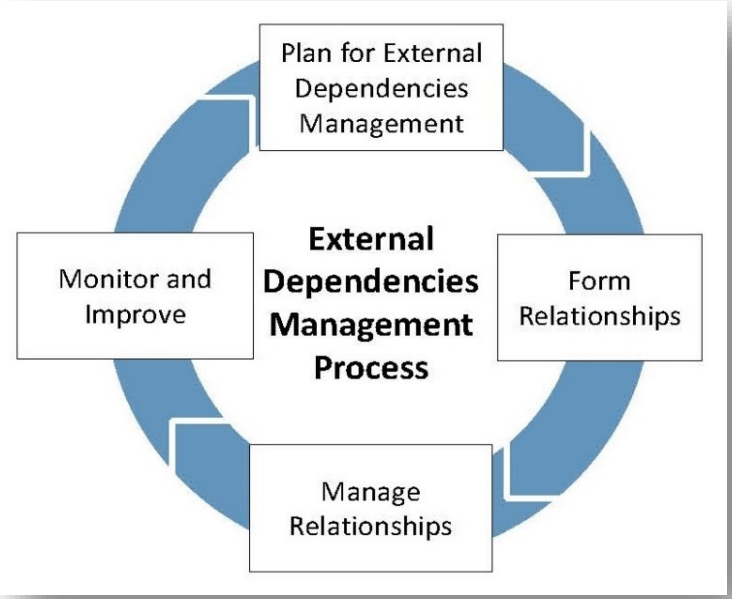
- Produce consistent results over time
- Are retained during times of stress

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

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.*

CYBER INFRASTRUCTURE SURVEY

CISA
CYBER+INFRASTRUCTURE

Cyber Infrastructure Survey Highlights

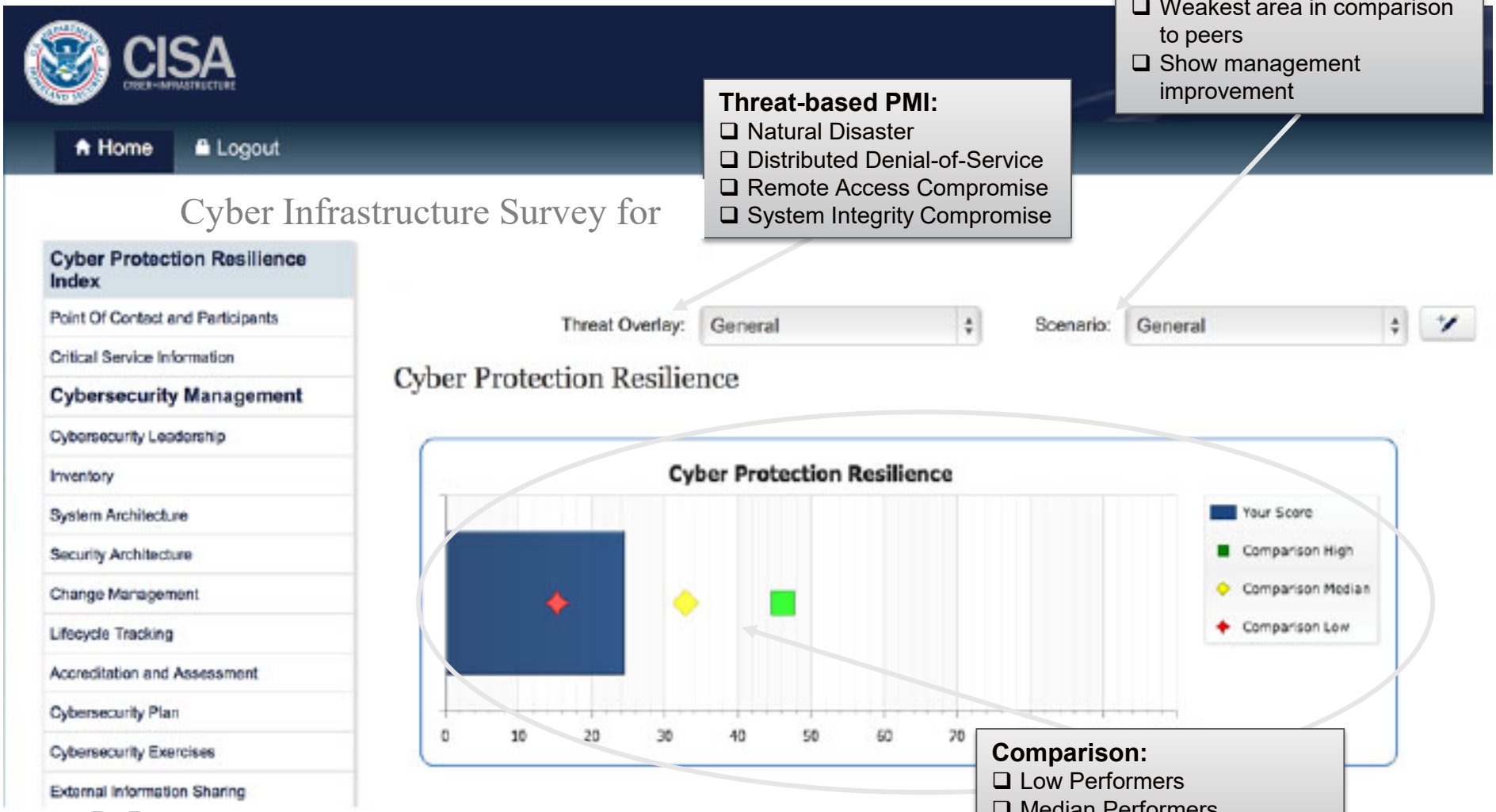
- Purpose: Evaluate security controls, cyber preparedness, overall resilience.
- Delivery: CSA-facilitated
- Benefits:
  - Effective assessment of cybersecurity controls in place for a critical service,
  - Easy-to-use interactive dashboard to support cybersecurity planning and resource allocation),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

CISA
CYBER+INFRASTRUCTURE

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

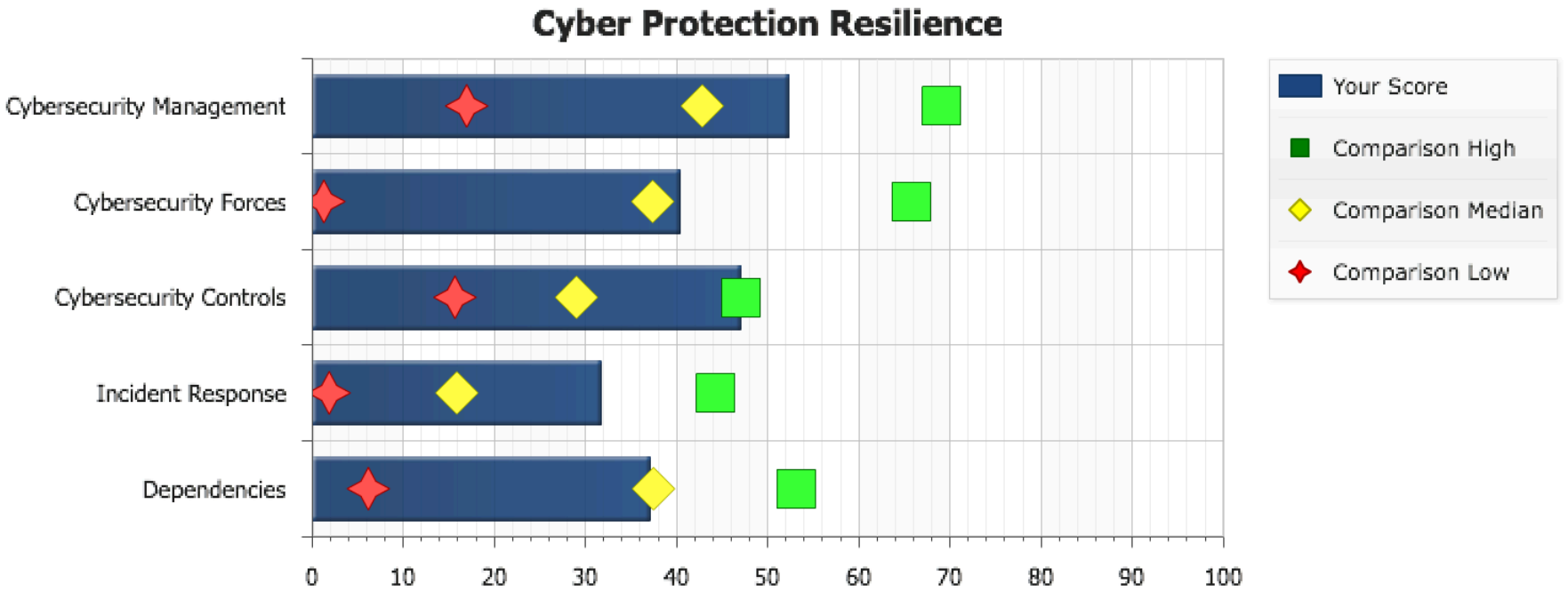


Comparison:
- ❑ Low Performers
- ❑ Median Performers
- ❑ High Performers

CISA
CYBER+INFRASTRUCTURE

CIS Dashboard - Comparison

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



CISA
CYBER+INFRASTRUCTURE

CISA Cyber Assessments in Brief, 1 of 2

Name	Cyber Resilience Review	Cyber Infrastructure Survey	External Dependency Management Review	Cybersecurity Evaluation Tool Assessment
Purpose	Identify cybersecurity management capabilities and maturity	Calculate a comparative analysis and valuation of protective measures in-place	Assess the activities and practices utilized by an organization to manage risks arising from external dependencies	Provide detailed, effective, and repeatable methodology for assessing control systems security encompassing the organization's infrastructure, policies, and procedures
Scope	Critical service view	Critical service view	Critical service view	Information Technology and Operational Technology systems
Time to Execute	8 Hours (1 business day)	2 ½ to 4 Hours	2 ½ to 4 Hours	Varies greatly (min 2 Hours), unknown for self-assessment
Information Sought	Capabilities and maturity indicators in 10 security domains	Protective measures in-place	Capabilities and maturity indicators across third-party relationship management lifecycle domains	Architecture diagrams, infrastructure, policies, and procedures documents
Preparation	1-hour questionnaire and planning call(s)	Planning call to scope evaluation	Planning call to scope evaluation	Self-assessment available from web site and used locally
Participants	IT / Security Manager, Continuity Planner, and Incident Responders	IT / Security Manager	IT / Security Manager with Continuity Planner and Contract Management	Operators, engineers, IT staff, policy / management personnel, and subject matter experts
Delivered By	CSAs cyberadvisor@hq.dhs.gov	CSAs cyberadvisor@hq.dhs.gov	CSAs cyberadvisor@hq.dhs.gov	Self-administered / CSAs https://ics-cert.us-cert.gov/

CISA CYBER+INFRASTRUCTURE

CISA Cyber Assessments in Brief, 2 of 2

Name	Validated Architecture Design Review	Phishing Campaign Assessment	Risk and Vulnerability Assessment	Vulnerability Scanning
Purpose	Provide analysis and representation of asset owner's network traffic, data flows, and relationships between devices and identifies anomalous communications flows.	Measure the susceptibility of an organization's personnel to social engineering attacks, specifically email phishing attacks.	Perform penetration and deep technical analysis of enterprise IT systems and an organization's external resistance to specific IT risks	Identify public-facing Internet security risks, at a high-level, through service enumeration and vulnerability scanning
Scope	Industrial Control Systems / Network Architecture, Traffic	Organization / Business Unit / Email Exchange Service	Organization / Business Unit / Network-Based IT Service	Public-Facing, Network-Based IT Service
Time to Execute	Variable (Hours to Days)	Approximately 6 Weeks	Variable (Days to Weeks)	Variable (Hours to Continuous)
Information Sought	Network design, configurations, log files, interdependencies, data flows and its applications	Click rate metrics gathered during phishing assessment	Low-level options and recommendations for improving IT network and system security	High-level network service and vulnerability information
Preparation	Coordinated via Email. Planning call(s).	Formal rules of engagement and pre-planning	Formal rules of engagement and extensive pre-planning	Formal rules of engagement and extensive pre-planning
Participants	Control system operators/ engineers, IT personnel, and ICS network, architecture, and topologies SMEs	IT/Security Manager and Network Administrators, end users	IT/Security Manager and Network Administrators	IT/Security Manager and Network Administrators
Delivered By	NCATS NCATS_INFO@hq.dhs.gov	NCATS NCATS_INFO@hq.dhs.gov	NCATs NCATS_INFO@hq.dhs.gov	NCATS NCATS_INFO@hq.dhs.gov

CISA CYBER+INFRASTRUCTURE

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

Free Federal Cyber Training

FedVTE enables cyber professionals to continue growing skills.

FedVTE is an online, on-demand training center that provides **free** cybersecurity training for U.S. veterans and federal, state, local, tribal, and territorial government employees. There are:

- Over 140,000 registered users, including employees at all levels of government
- Over 18,000 veteran users (through non-profit partner, Hire Our Heroes™)
- Over 5,000 SLTT registered users

FedVTE FEDERAL VIRTUAL TRAINING ENVIRONMENT

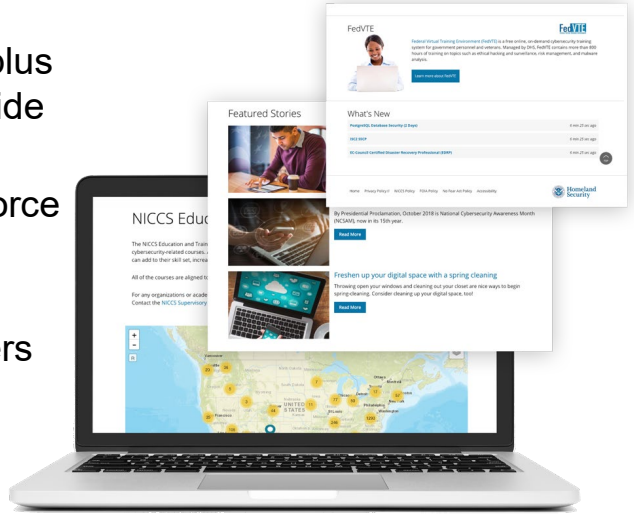
CISA CYBER+INFRASTRUCTURE

Cybersecurity Training Resources

CISA offers easily accessible education and awareness resources through the National Initiative for Cybersecurity Careers and Studies (NICCS) website.

The NICCS website includes:

- Searchable Training Catalog with 4,400 plus cyber-related courses offered by nationwide cybersecurity educators
- Interactive National Cybersecurity Workforce Framework
- Cybersecurity Program information: FedVTE, Scholarships for Service, Centers for Academic Excellence, and Cyber Competitions
- Tools and resources for cyber managers
- Upcoming cybersecurity events list



For more information, visit https://niccs.us-cert.gov/training/search

CISA CYBER+INFRASTRUCTURE

Our Nation's Cyber Workforce Foundation

The **National Cybersecurity Workforce Framework** is a collection of definitions that describe types of cybersecurity work and skills requires to perform it.

- ✓ When used nationally, the definitions help establish universally applicable cybersecurity skills, training/development, and curricula
- ✓ 7 Categories, 30+ Specialty Areas
- ✓ Baselines knowledge, skills, and abilities & tasks

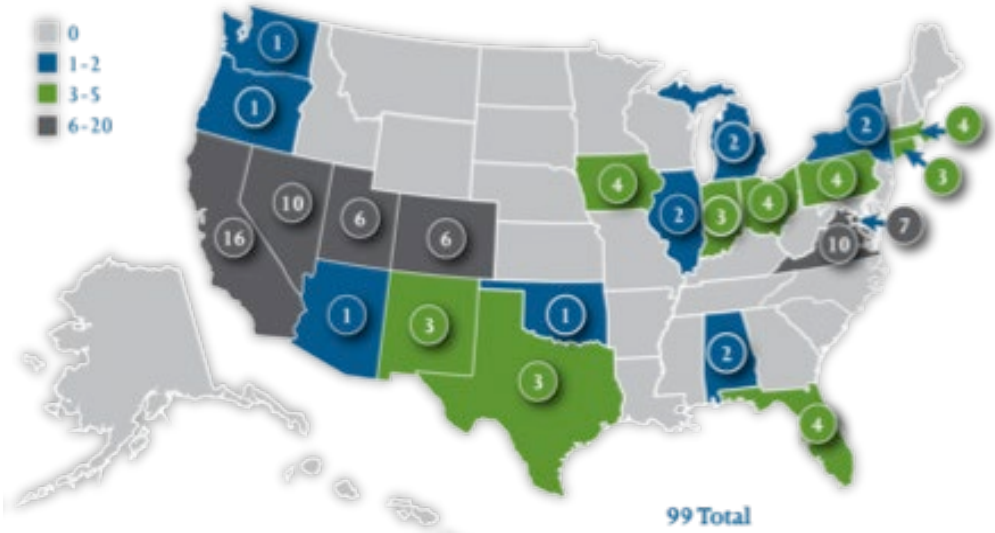
Operate & Maintain | **Securely Provision** | **Analyze** | **Collect & Operate** | **Oversight & Development** | **Protect & Defend** | **Investigate**

CISA CYBER+INFRASTRUCTURE

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 Resources

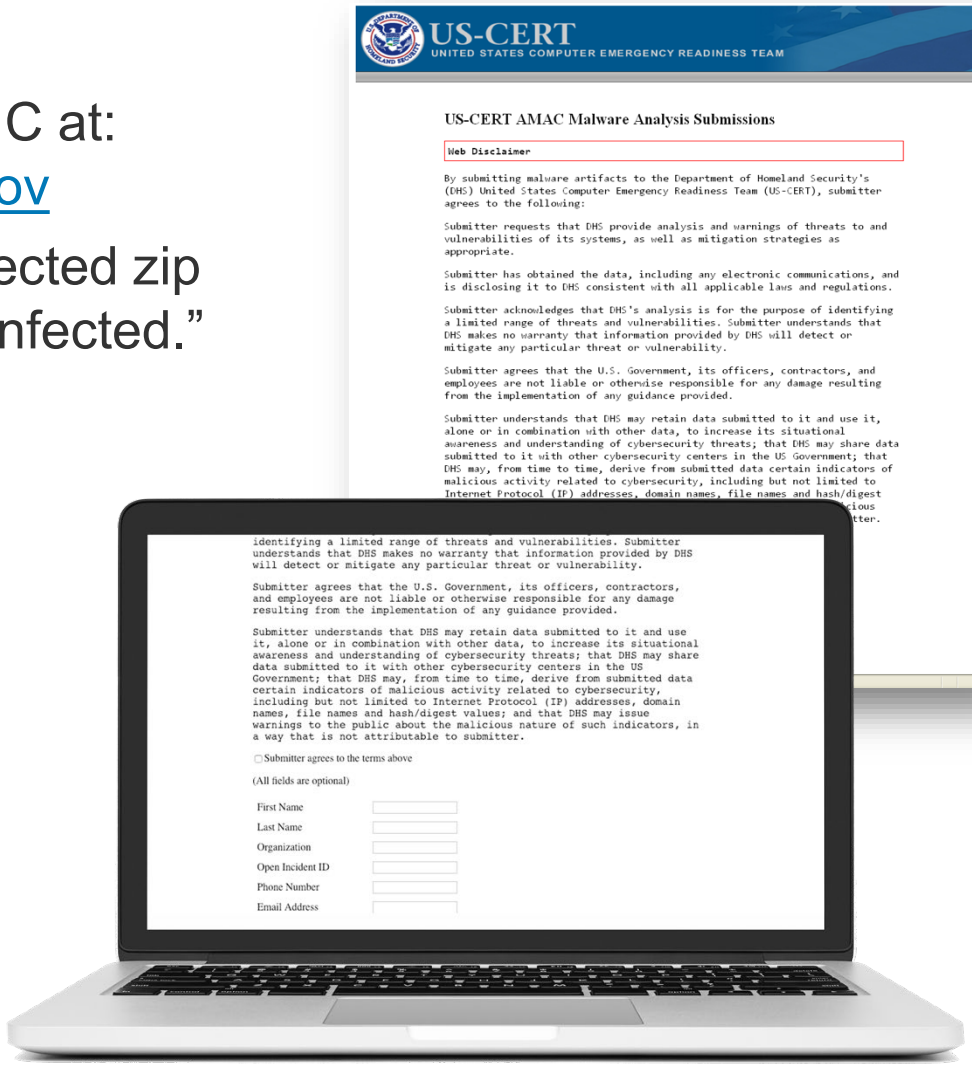


CISA
CYBER+INFRASTRUCTURE

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 Incident Response

Threat Response	Asset Response
Federal Bureau of Investigation 855-292-3937 or cywatch@ic.fbi.gov	**CISA Central** 888-282-0870 or Report incidents: https://www.us-cert.gov/report
U.S. Secret Service secretservice.gov/contact/field-offices	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.
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

Contact

General Inquiries

cyberadvisor@hq.dhs.gov

CISA Contact Information

Sean McCloskey **Branch Chief** **Cybersecurity Advisor Program**	**Sean.McCloskey@hq.dhs.gov**

Incident Reporting

https://www.us-cert.gov/report	ciocc.cyber@cisa.gov

Cybersecurity and Infrastructure Security Agency

CISA
CYBER+INFRASTRUCTURE

CISA

CYBER+INFRASTRUCTURE