CISA CYBERSECURITY SERVICES

Stephanie Watt
Alabama Cybersecurity State Coordinator/ Advisor, Region 4
Cybersecurity Advisor Program
Cybersecurity and Infrastructure Security Agency

CISA Mission and Vision

MISSION:

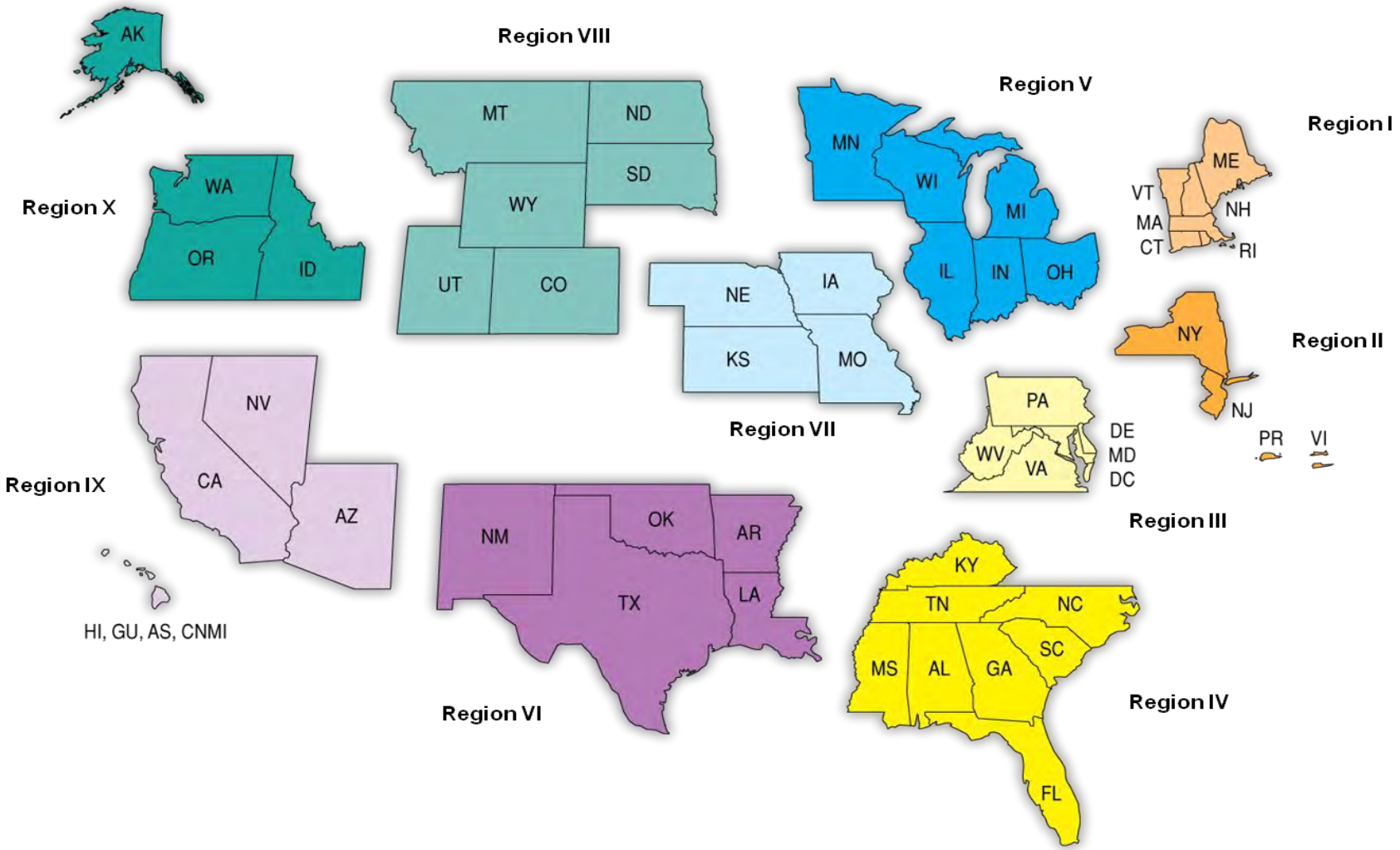
We lead the National effort to understand, manage, and reduce risk to our cyber and physical infrastructure.

VISION:

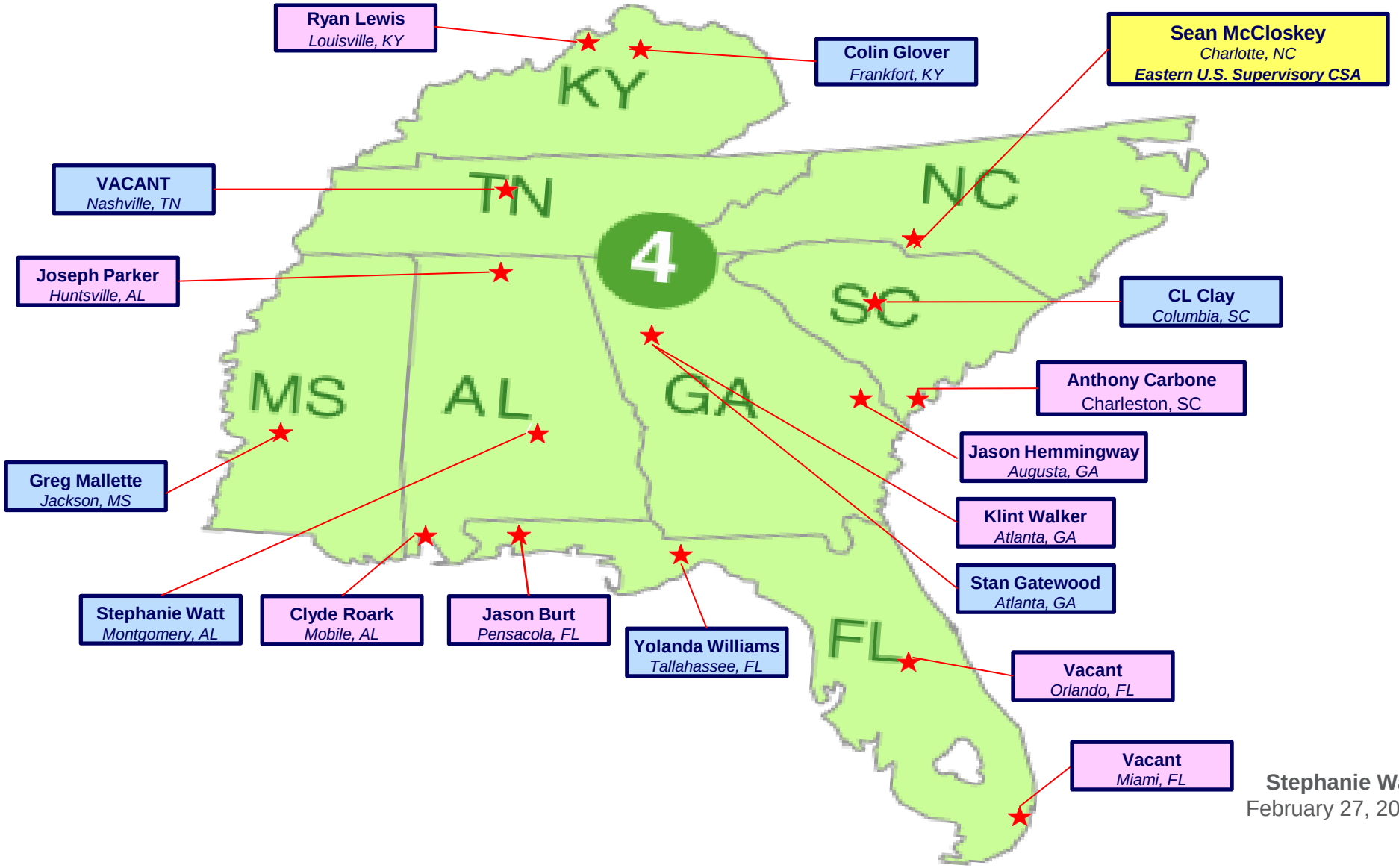
Secure and resilient infrastructure for the American people.

CYBERSECURITY ADVISOR PROGRAM

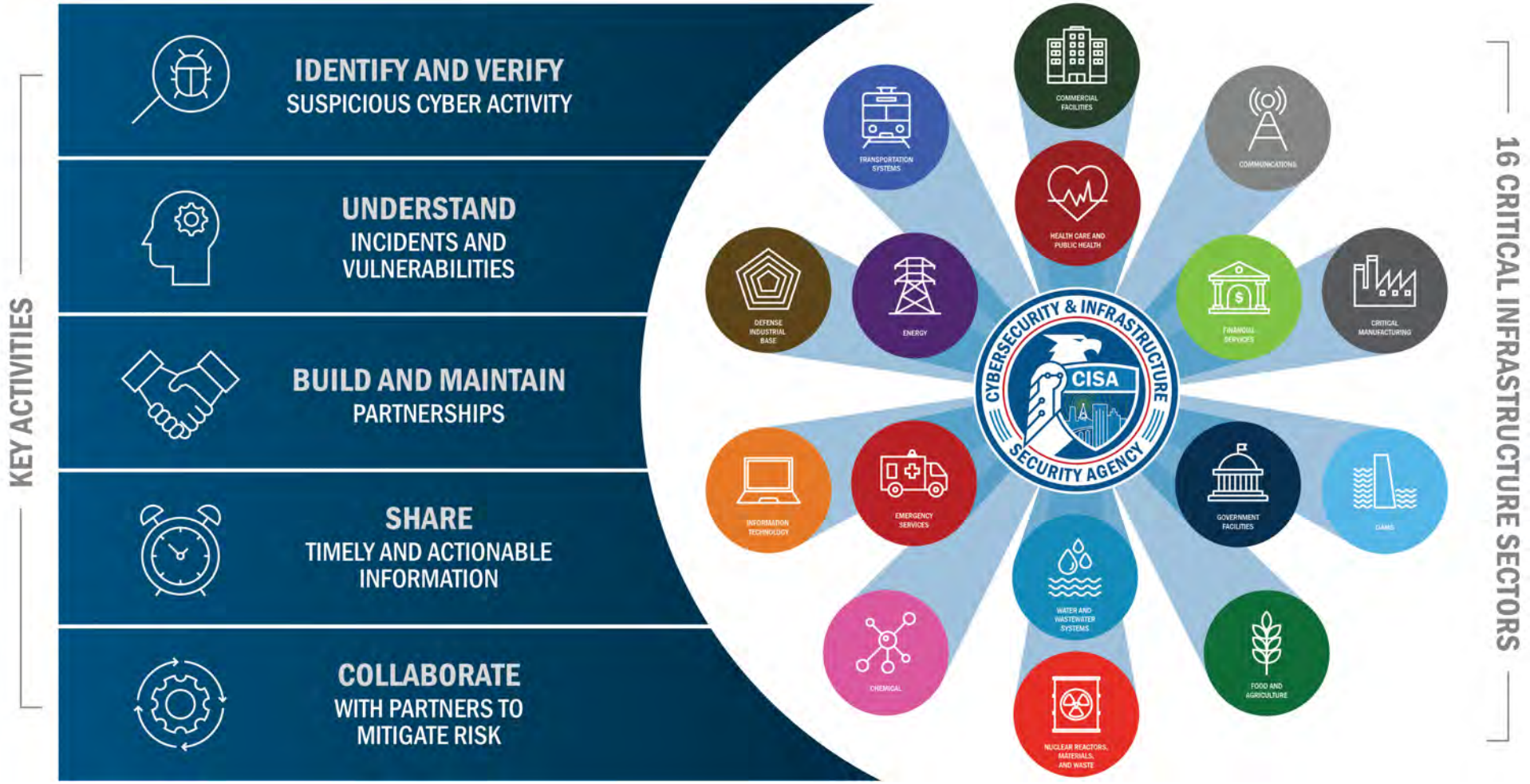
CSA Regionally Deployed Personnel



CISA Region 4 Cyber Support



Serving Critical Infrastructure



CISA CYBER SERVICES

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.

Range of Cybersecurity Services

STRATEGIC
(C-Suite Level)

- Cyber Resilience Review (Strategic)
- External Dependencies Management (Strategic)
- Cyber Infrastructure Survey (Strategic)
- Cybersecurity Evaluations Tool (Strategic/Technical)
- **Vulnerability Scanning / Hygiene (Technical)**

TECHNICAL
(Network-Administrator Level)

Stephanie Watt
February 27, 2023

VULNERABILITY SCANNING / HYGIENE

Vulnerability Scanning / Hygiene

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

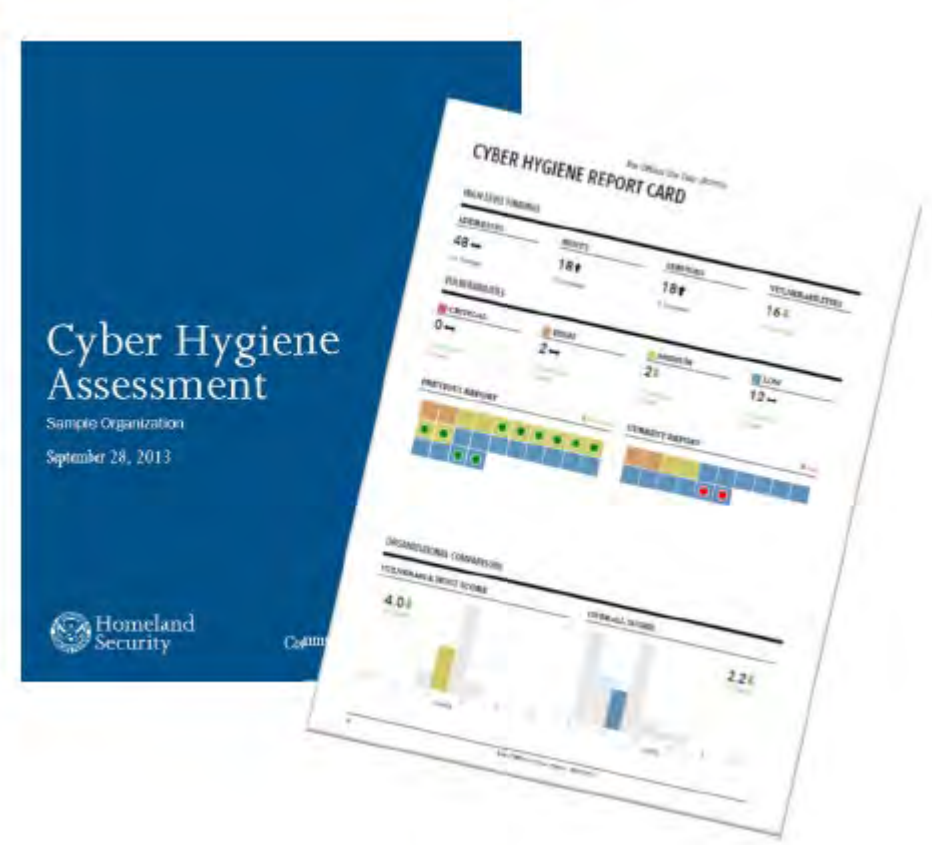
Delivery: Identify public-facing Internet security risks, through service enumeration and vulnerability scanning online by CISA.

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



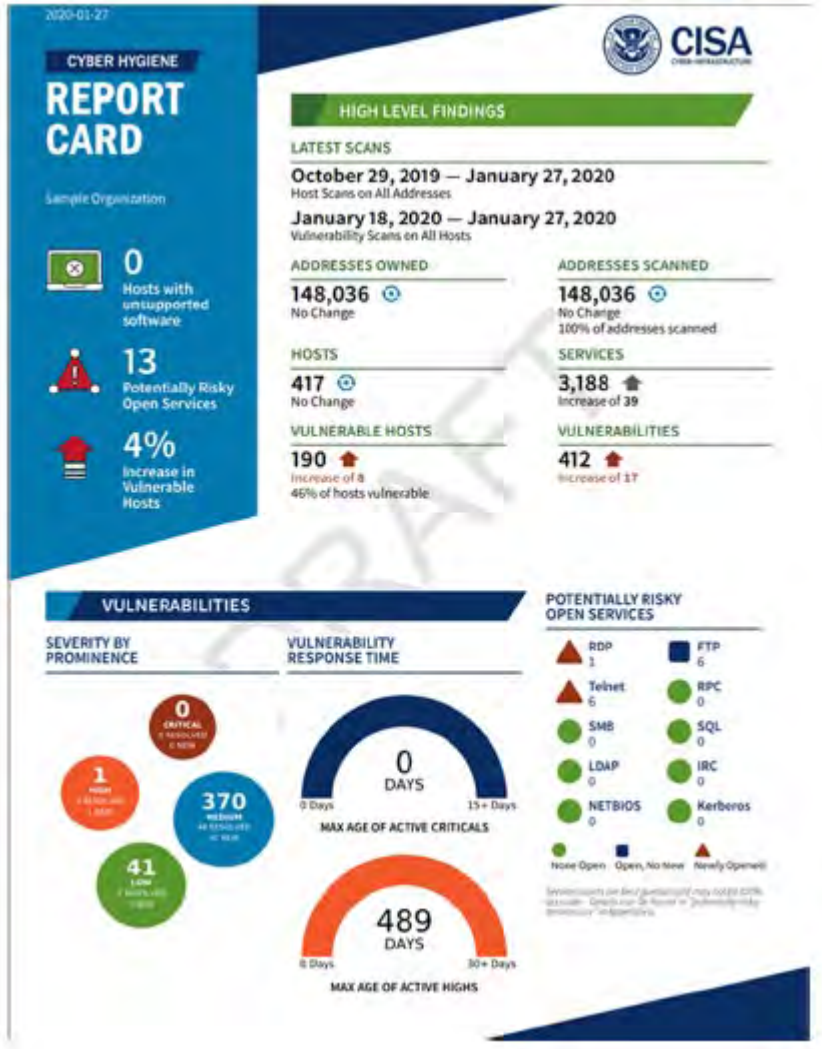
Cyber Hygiene Report Card

High Level Findings

- Latest Scans
- Addresses Owned
- Addresses Scanned
- Hosts
- Services
- Vulnerable Hosts
- Vulnerabilities

Vulnerabilities

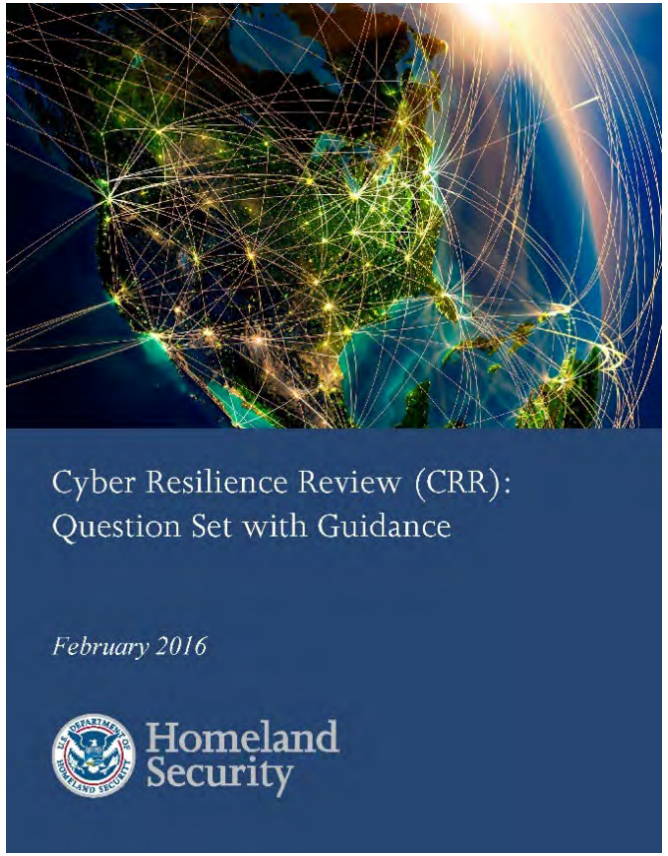
- Severity by Prominence
- Vulnerability Response Time
- Potentially Risky Open Services



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

Stephanie Watt
February 27, 2023

Cyber Resilience Review Domains

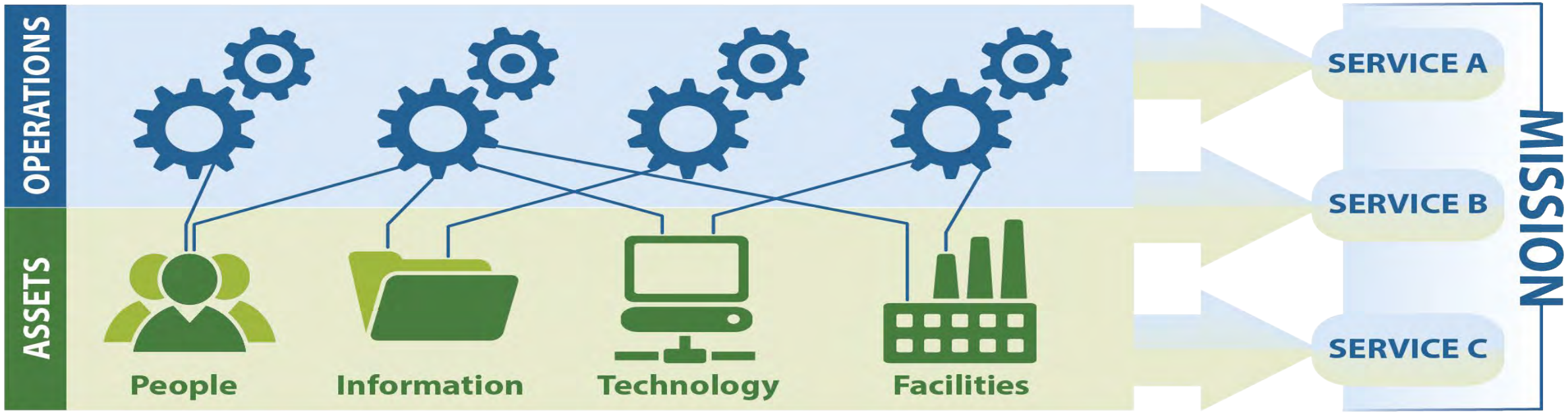
Asset Management Know your assets being protected & their requirements, e.g., CIA	**Risk Management** Know and address your biggest risks that considers cost and your risk tolerances
Configuration and Change Management Manage asset configurations and changes	**Service Continuity Management** Ensure workable 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

Stephanie Watt
February 27, 2023

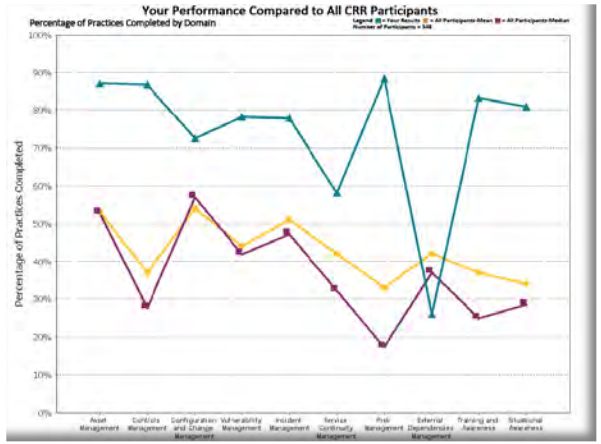
Critical Service Focus

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



CRR Sample Report

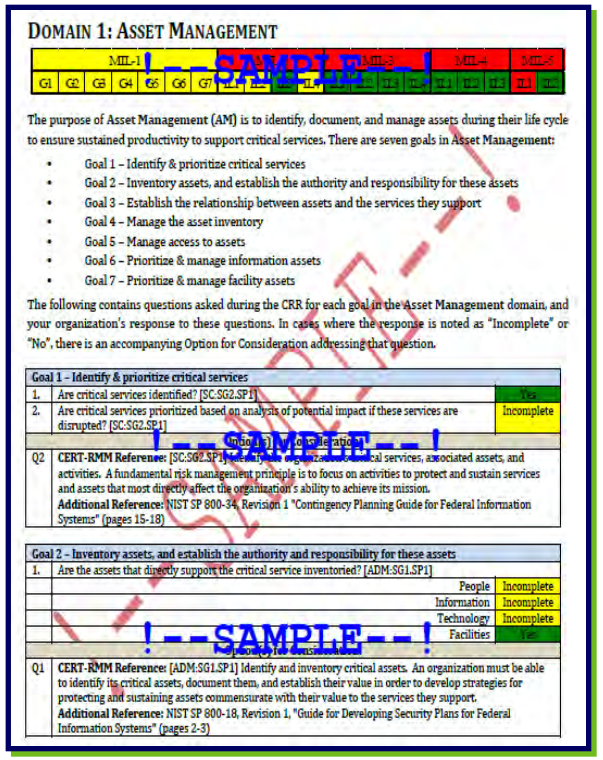
Each CRR report includes:



Comparison data with other CRR participants
**facilitated only*

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

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



EXTERNAL DEPENDENCIES MANAGEMENT ASSESSMENT

Stephanie Watt
February 27, 2023

EDM Assessment Organization and Structure

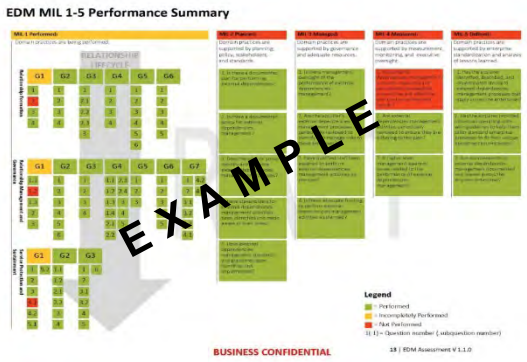
- Structure and scoring similar to Cyber Resilience Review
- Uses one Maturity Indicator Level (MIL) scale with three lifecycle domains.

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.*

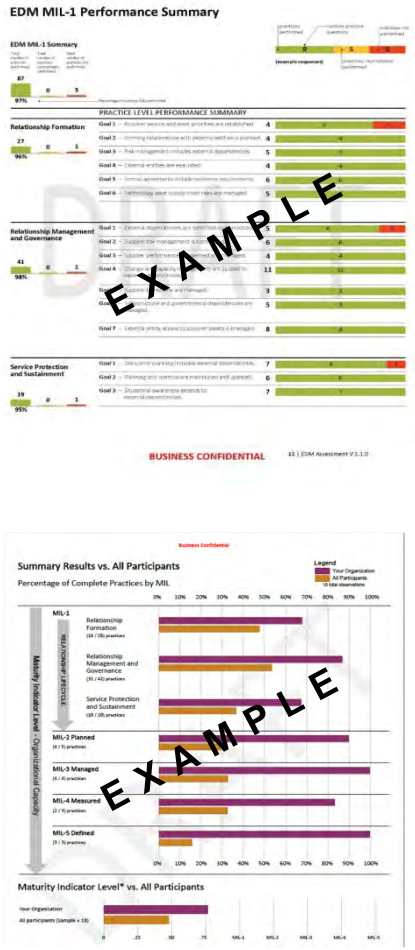
EDM Assessment Report

Each EDM report includes:

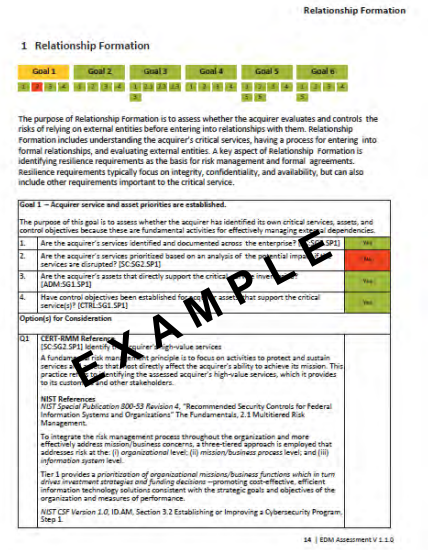
- Performance summary of existing capability managing external dependencies



- Comparison data with other EDM participants



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



Stephanie Watt
February 27, 2023

CYBER INFRASTRUCTURE SURVEY

Stephanie Watt
February 27, 2023

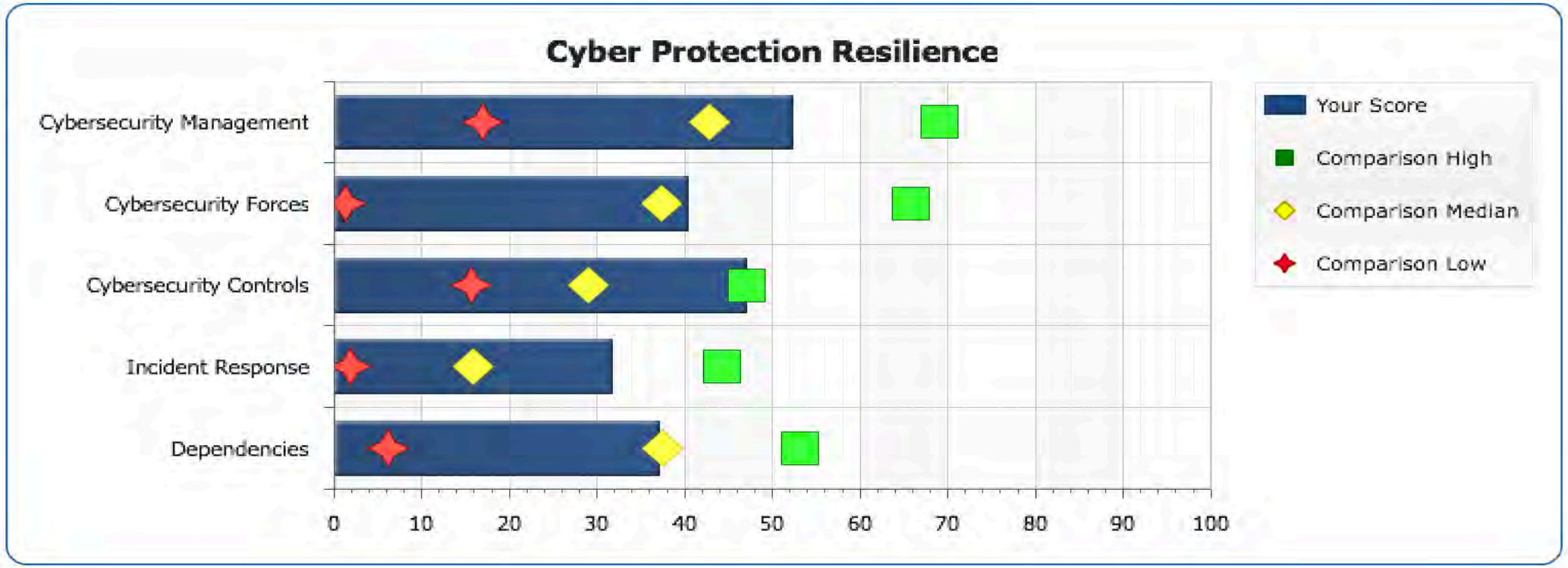
Cyber Infrastructure Survey (CIS)

- 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.

Stephanie Watt
February 27, 2023

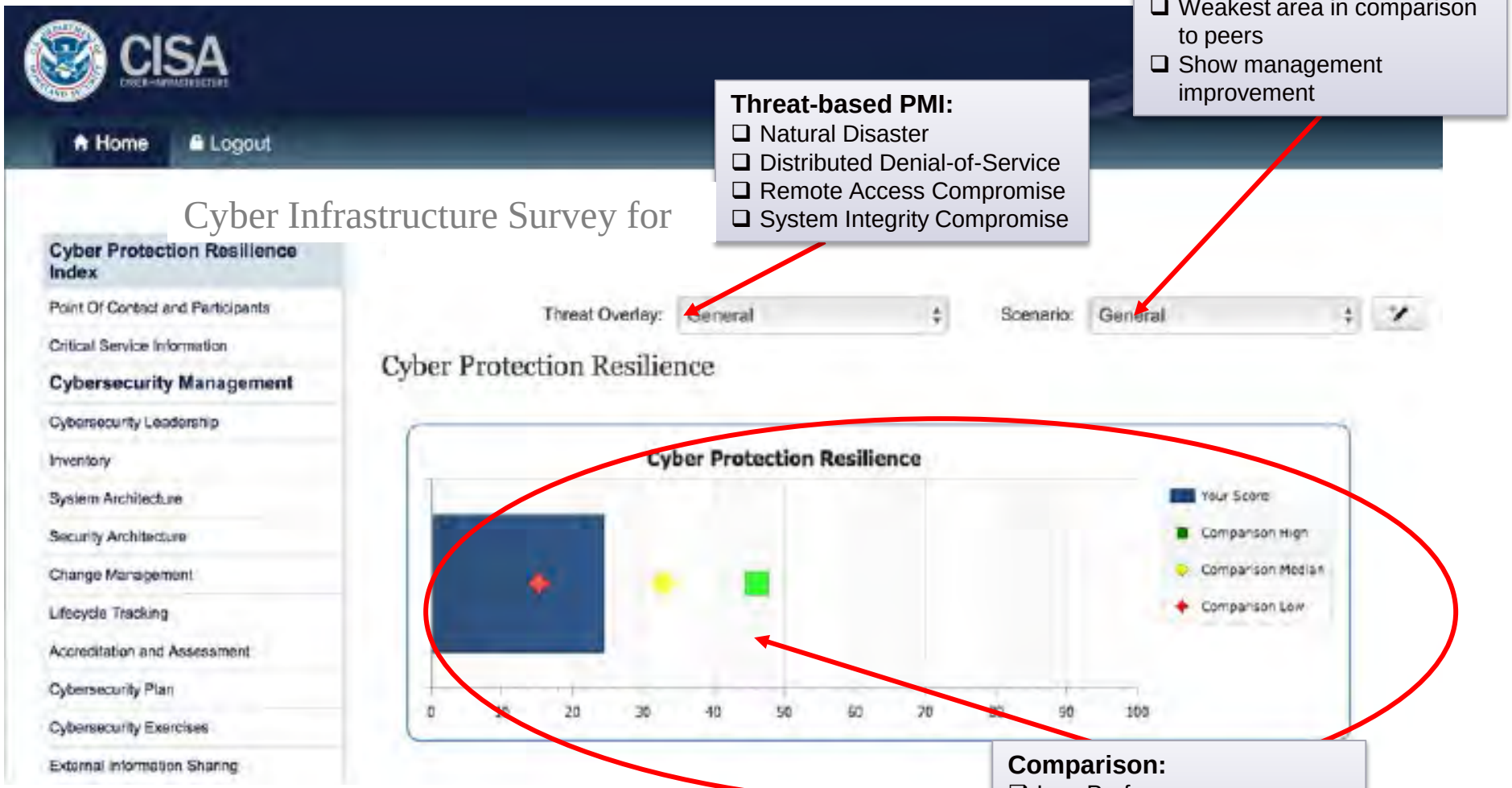
CIS Dashboard - Comparison

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



Stephanie Watt
February 27, 2023

Example of CIS Dashboard



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

CISA Resources

- Known Exploited Vulnerabilities Catalog | CISA
- Free Cybersecurity Services and Tools | CISA
- Downloading and Installing CSET | CISA
- Release Ransomware Readiness Assessment CSET v10.3 · cisagov/cset · GitHub

PISCES

- No-Cost cybersecurity monitoring effort for small public organizations
- Benefits:
  - Provides small communities with professional cybersecurity analysts
  - Prepares students to succeed in the cybersecurity workforce
  - Provides Universities structured curriculum and hands-on learning experiences
  - Information sharing between communities and state fusion center

How to Reach Us

Contact Information

Stephanie Watt
Alabama Cybersecurity State Coordinator/ Advisor - Alabama
Stephanie.Watt@cisa.dhs.gov
(202) 615-4615 (Cell)

Joe Parker
Region 4 Cybersecurity Advisor - Alabama
Joseph.Parker@cisa.dhs.gov
(202) 894-4869 (Cell)

Clyde Roark
Region 4 Cybersecurity Advisor - Alabama
Clyde.Roark@cisa.dhs.gov
(850) 776-2894 (Cell)