U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

"DEFEND TODAY,
SECURE TOMORROW."

Ashley Jones
Cybersecurity State Advisor for the National Capital Region
Region III (MD, PA, DE, DC, VA, WV)
Cybersecurity Advisor Program
Cybersecurity and Infrastructure Security Agency

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient infrastructure for the American people.

MISSION

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

OVERALL GOALS

GOAL 1

DEFEND TODAY

Defend against urgent threats and hazards

seconds | days | weeks

GOAL 2

SECURE TOMORROW

Strengthen critical infrastructure and address long-term risks

months | years | decades

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Our Work

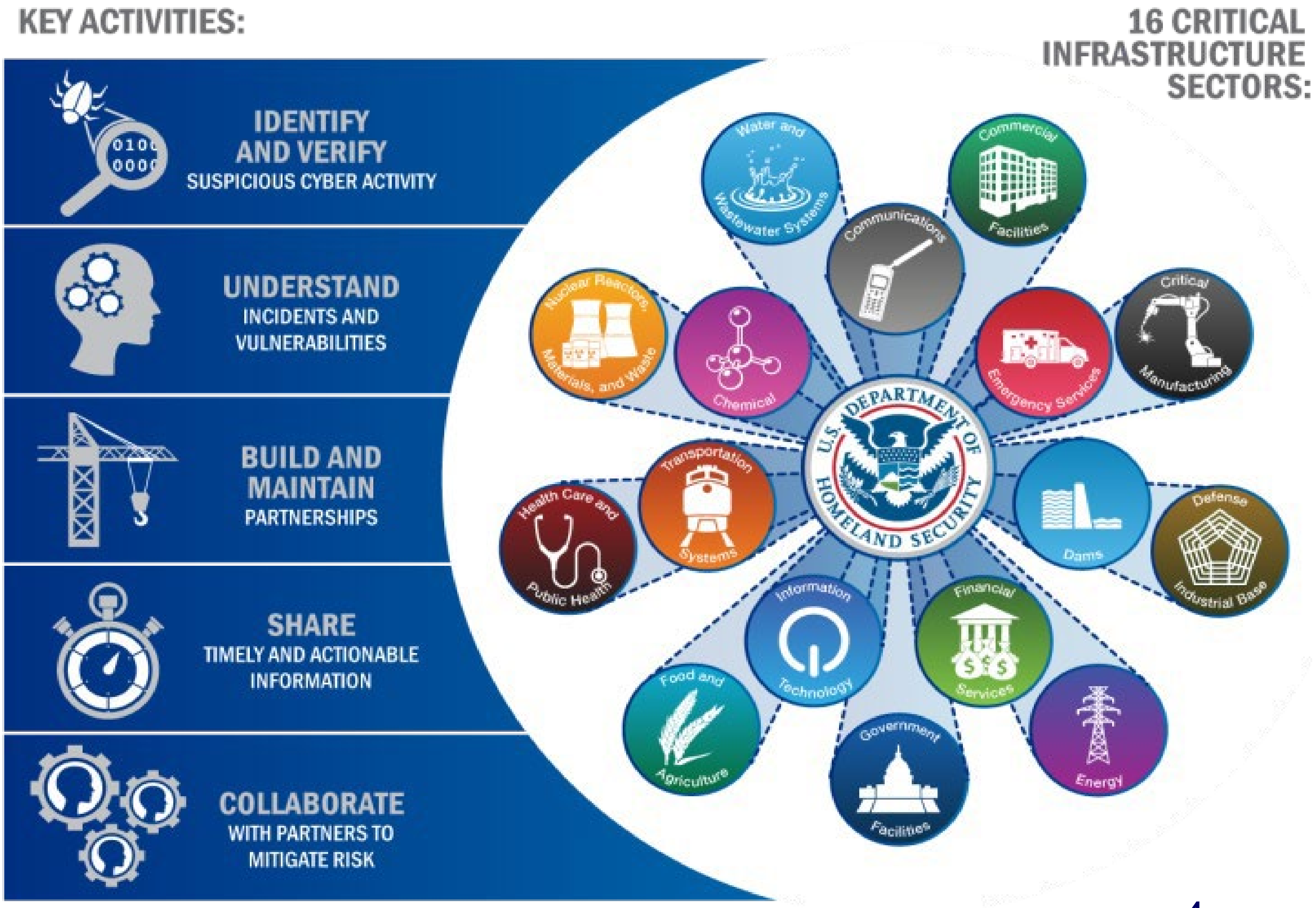
The Cybersecurity and Infrastructure Security Agency (CISA) works with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future

- PARTNERSHIP DEVELOPMENT
- INFORMATION AND DATA SHARING
- CAPACITY BUILDING
- INCIDENT MANAGEMENT & RESPONSE
- RISK ASSESSMENT AND ANALYSIS
- NETWORK DEFENSE
- EMERGENCY COMMUNICATIONS

Critical Infrastructure Significance

- ✓ Critical Infrastructure refers to the assets, systems, and networks, whether physical or cyber

- ✓ So vital to the Nation, that their incapacitation or destruction would have a debilitating effect on:
  - National Security
  - The Economy
  - Public Health or Safety
  - Our Way of Life



KEY ACTIVITIES:

IDENTIFY AND VERIFY SUSPICIOUS CYBER ACTIVITY

UNDERSTAND INCIDENTS AND VULNERABILITIES

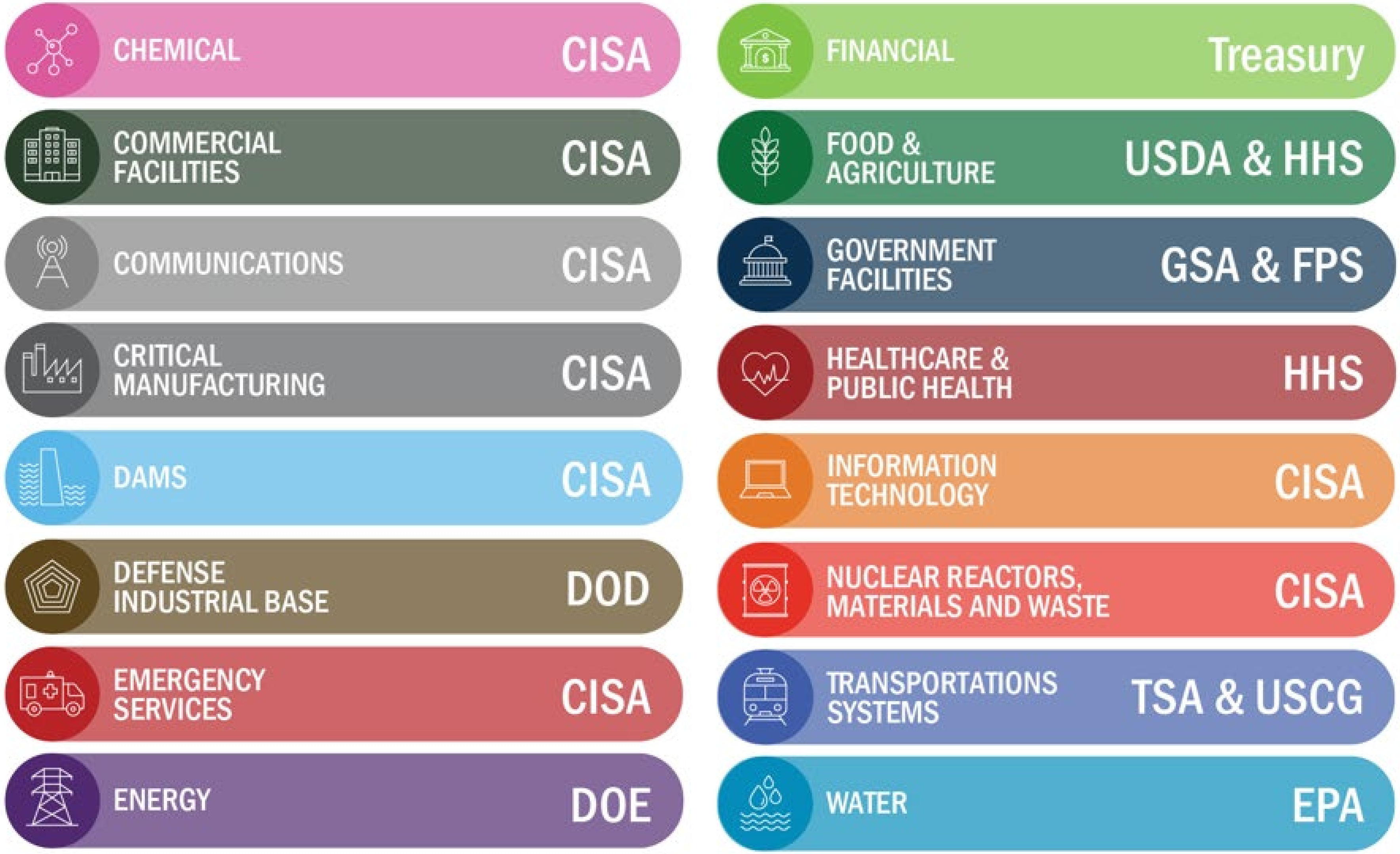
BUILD AND MAINTAIN PARTNERSHIPS

SHARE TIMELY AND ACTIONABLE INFORMATION

COLLABORATE WITH PARTNERS TO MITIGATE RISK

16 CRITICAL INFRASTRUCTURE SECTORS:

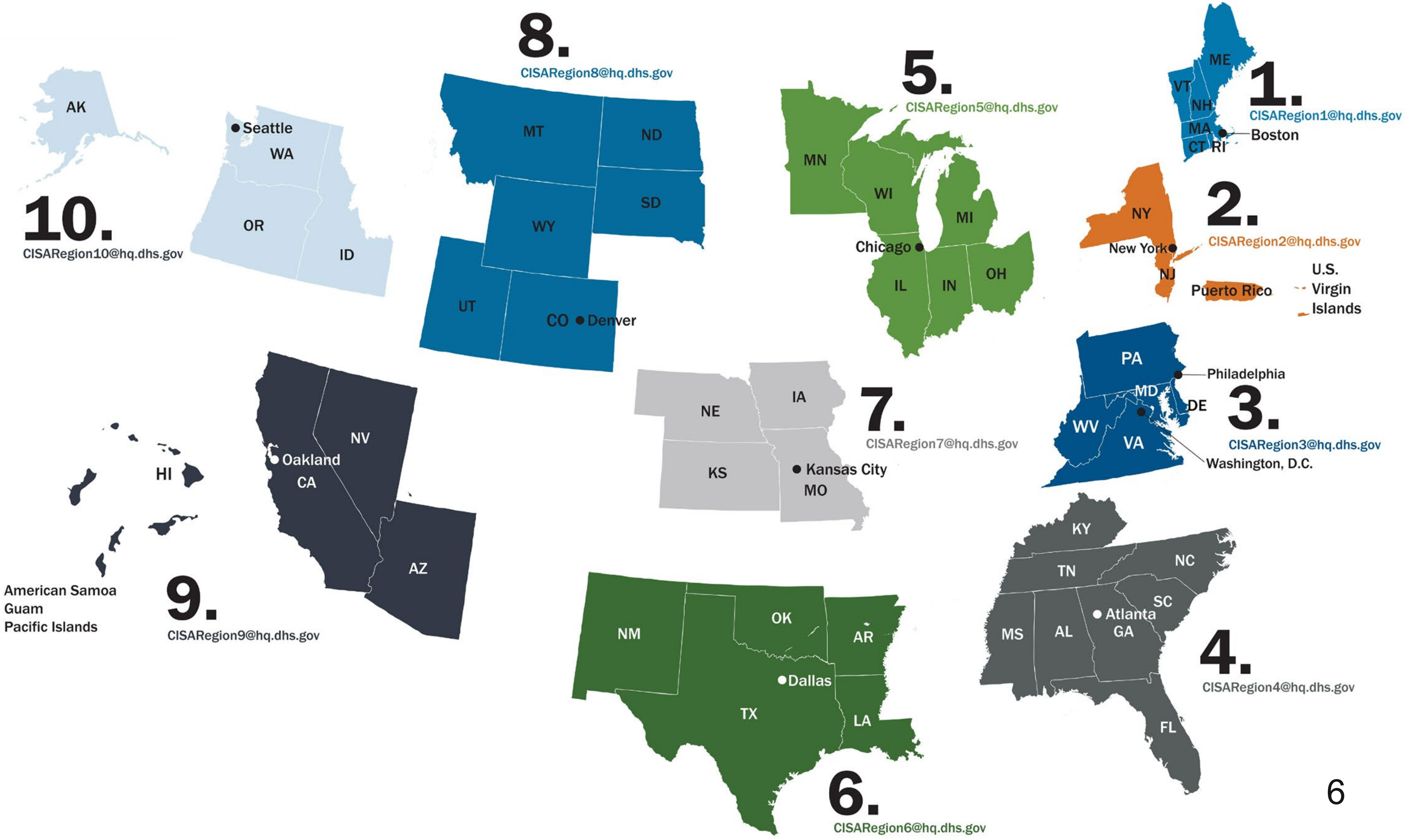
16 Critical Infrastructure Sectors & SRMAs



CHEMICAL	CISA
COMMERCIAL FACILITIES	CISA
COMMUNICATIONS	CISA
CRITICAL MANUFACTURING	CISA
DAMS	CISA
DEFENSE INDUSTRIAL BASE	DOD
EMERGENCY SERVICES	CISA
ENERGY	DOE
FINANCIAL	Treasury
FOOD & AGRICULTURE	USDA & HHS
GOVERNMENT FACILITIES	GSA & FPS
HEALTHCARE & PUBLIC HEALTH	HHS
INFORMATION TECHNOLOGY	CISA
NUCLEAR REACTORS, MATERIALS AND WASTE	CISA
TRANSPORTATIONS SYSTEMS	TSA & USCG
WATER	EPA

CISA Regions

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



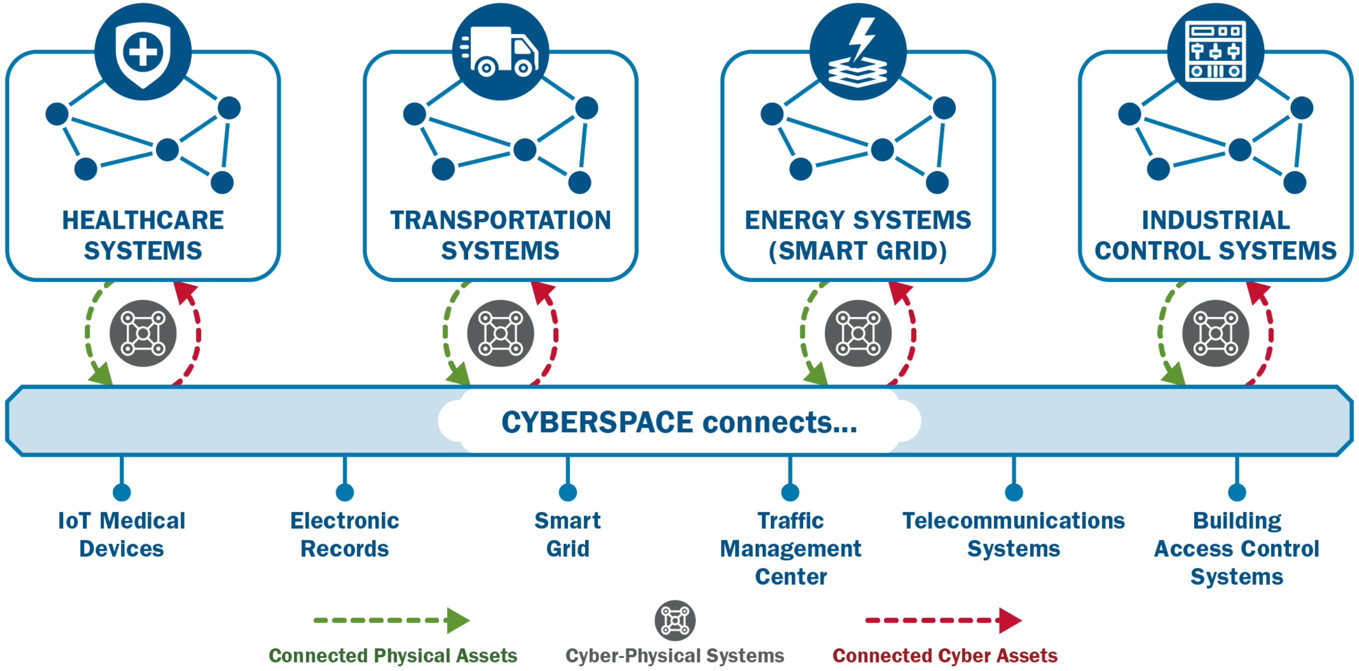
CISA Regional Teams

- Regional Director
- Deputy, Regional Director
- Chief, Protective Security Advisor
- **Protective Security Advisor (PSA)**
- Chief, Chemical Security Inspector
- **Chemical Security Inspector (CSI)**
- Senior Chemical Security Inspector
- Regional Operations Manager
- Critical Infrastructure Specialist
- Operations Analyst
- National Risk Management Center Regional Analyst
- Regional Regulatory Analyst (TBA)
- Administrative Officer
- Program Analyst for Business Support (TBA)
- Outreach Coordinator
- Interagency Security Committee (ISC) Regional Advisor
- Regional Training & Exercise Coordinator
- Regional Planner (TBA)
- External Affairs Officer
- Chief, Cybersecurity Advisor
- **Cybersecurity Advisor (CSA)**
- **Emergency Communications Coordinator (ECC)**
- **Bombing Prevention Coordinator (BPC)**

Gray: Regional Office
Blue: Field Personnel

Cyber-Physical Convergence

Today's threats are targeting physical and cyber assets through sophisticated hybrid attacks with potentially devastating impacts to data, property and physical safety. CISA defines convergence as formal collaboration between previously disjoined security functions.



HEALTHCARE SYSTEMS
TRANSPORTATION SYSTEMS
ENERGY SYSTEMS (SMART GRID)
INDUSTRIAL CONTROL SYSTEMS
CYBERSPACE connects...
IoT Medical Devices
Electronic Records
Smart Grid
Traffic Management Center
Telecommunications Systems
Building Access Control Systems
Connected Physical Assets
Cyber-Physical Systems
Connected Cyber Assets

Protective Security Advisors

Five mission areas that directly support the protection of critical infrastructure

1. Plan, coordinate, and conduct security surveys and assessments (i.e., IST, SAFE)
2. Plan and conduct outreach activities
3. Support National Special Security Events (NSSEs) & Special Event Activity Rating (SEAR) events
4. Respond to incidents
5. Coordinate and support improvised explosive device awareness and risk mitigation training

Sampling of Voluntary & No-Cost Cybersecurity Offerings

- **Assessments & Evaluations**
  - Cross-Sector Cybersecurity Performance Goals (CPG)
  - Cyber Resilience Reviews (CRR™)
  - Cyber Infrastructure Surveys
  - Phishing Campaign Assessment
  - Vulnerability Scanning & Web Application Scanning
  - Risk and Vulnerability Assessments (aka "Pen" Tests)
  - External Dependencies Management Reviews
  - Cyber Security Evaluation Tool (CSET™)
  - Validated Architecture Design Review (VADR)

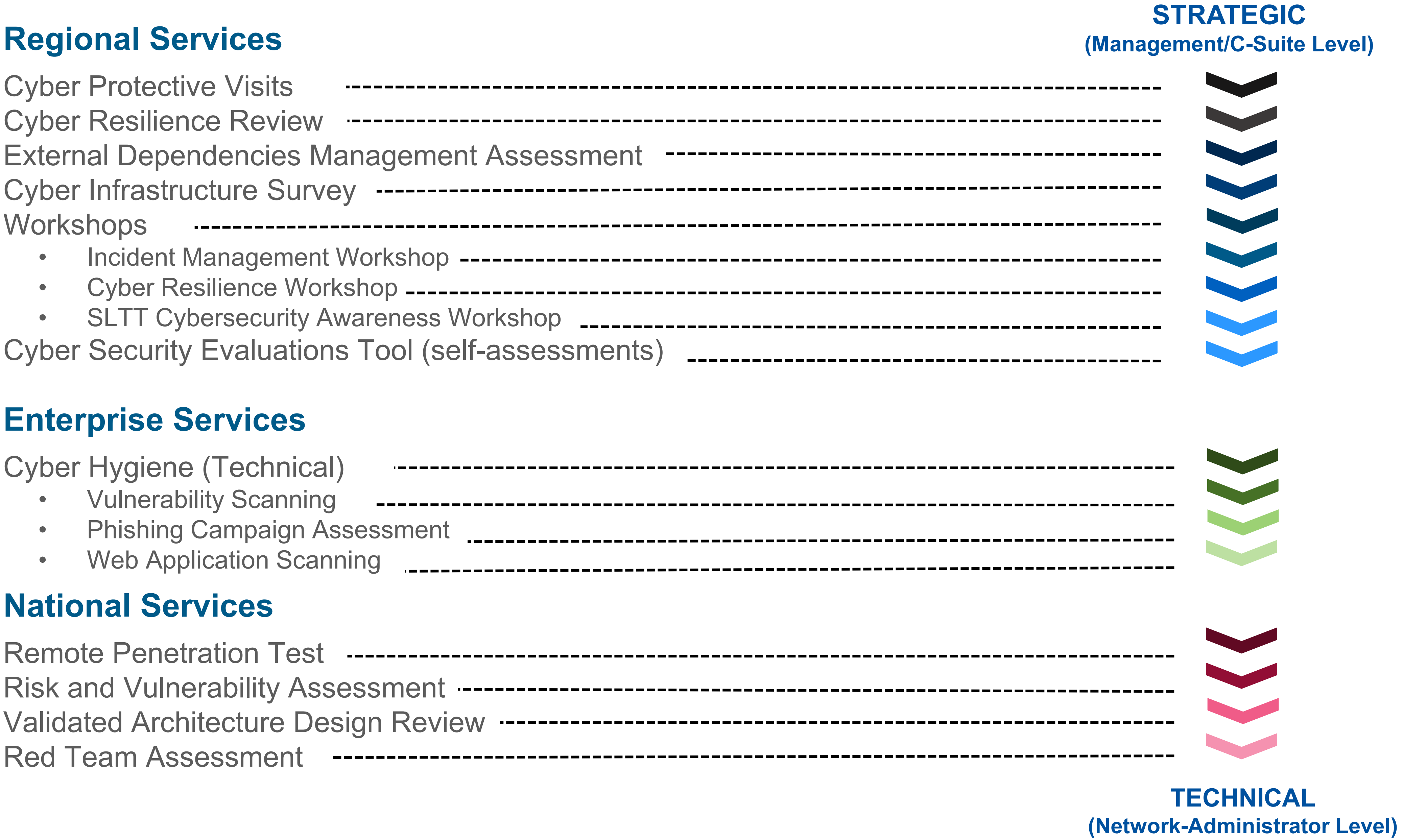
- **Preparedness Activities**
  - Alert and notifications on threats, vulnerabilities, and mitigations
  - Information / Threat Indicator Sharing
  - Cybersecurity Training and Awareness
  - Cyber Exercises and "Playbooks"
  - National Cyber Awareness System
  - Vulnerability Notes Database
  - Information Products and Recommended Practices
  - Workshops (Cyber Resilience, Cyber Incident Management, Election Security, etc.)

- **Partnership Development**
  - Informational Exchanges
  - Working Group Support
  - Cyber Information Sharing and Collaboration Program (CISCP)

- **Strategic Messaging & Advisement**
  - Resource Briefings
  - Keynotes and Panels
  - Threat Briefings
  - Topic Specifics (e.g., NCSAM, SCRM, ICS, etc.)

- **Incident Response Assistance**
  - Remote / On-Site Assistance
  - Malware Analysis
  - Hunt and Incident Response Teams
  - Incident Coordination
  - Targeted (Victim) Notifications

CISA Service Delivery Model



STRATEGIC
(Management/C-Suite Level)

Regional Services

Cyber Protective Visits
Cyber Resilience Review
External Dependencies Management Assessment
Cyber Infrastructure Survey
Workshops

- Incident Management Workshop
- Cyber Resilience Workshop
- SLTT Cybersecurity Awareness Workshop

Cyber Security Evaluations Tool (self-assessments)

Enterprise Services

Cyber Hygiene (Technical)

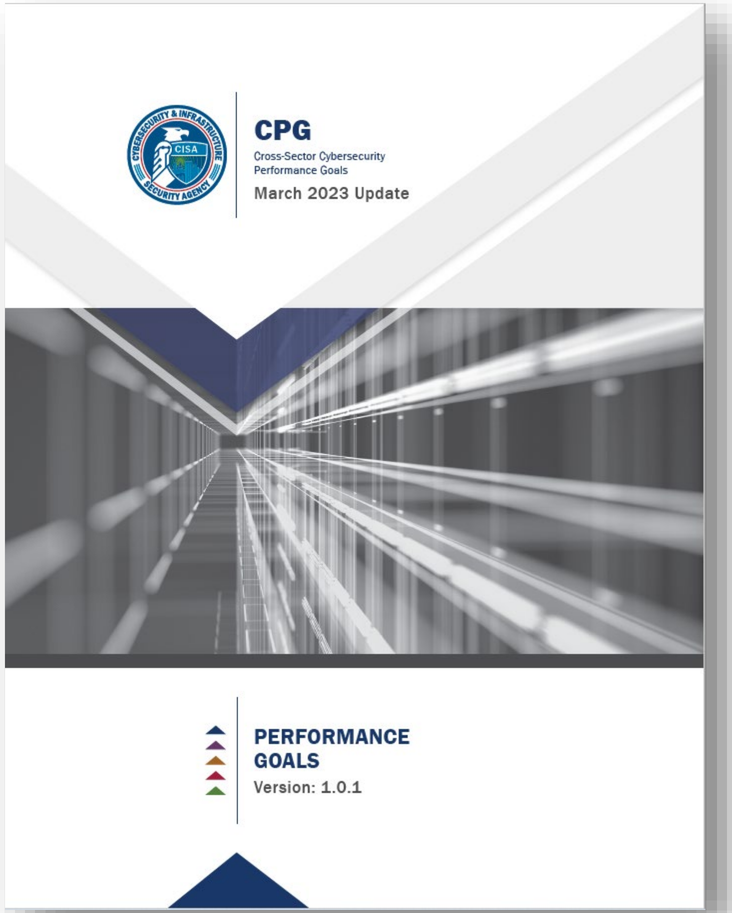
- Vulnerability Scanning
- Phishing Campaign Assessment
- Web Application Scanning

National Services

Remote Penetration Test
Risk and Vulnerability Assessment
Validated Architecture Design Review
Red Team Assessment

TECHNICAL
(Network-Administrator Level)

Cross-Sector Cybersecurity Performance Goals (CPG)



CPG

Cross-Sector Cybersecurity Performance Goals

March 2023 Update

PERFORMANCE GOALS

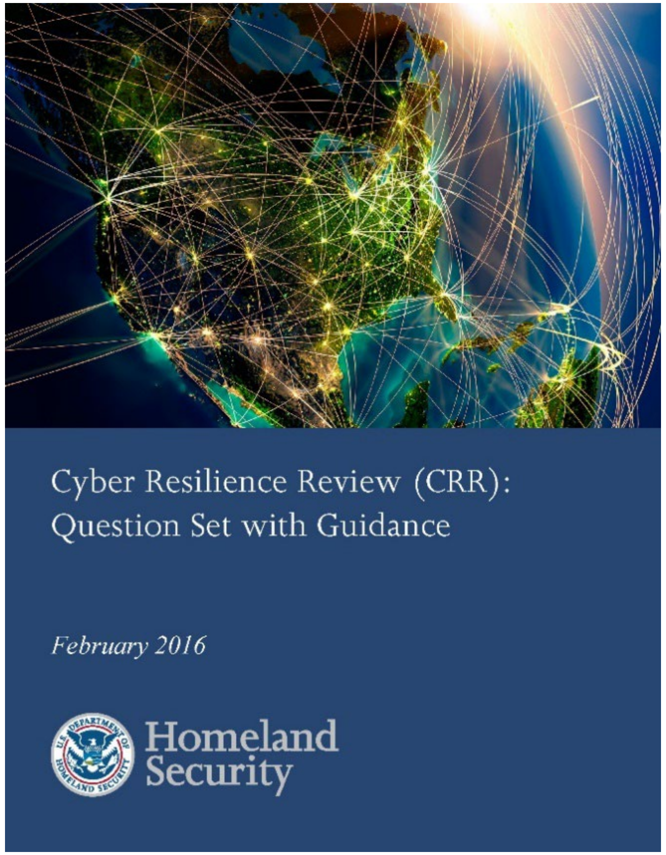
Version: 1.0.1

- Interview-based assessment of baseline set of cybersecurity practices broadly applicable across critical infrastructure with known risk-reduction value:
  - Align to the NIST CSF functions of Identify, Protect, Detect, Respond, Recover (38 Questions)
  - A benchmark for critical infrastructure operators to measure and improve their cybersecurity maturity.
  - A combination of recommended practices for IT and OT owners, including a prioritized set of security practices.
    - Available as: **CSA-facilitated**, or **self-assessment**
    - When facilitated, 2-person teams *(mastery level can conduct solo)*
  - **1-2** hours to complete and can be combined with a SAFE Assessment
  - CRR report

Cyber Resilience Review

- **Purpose:** Evaluate operational resilience and cybersecurity practices of **critical services.**
- **Delivery:** Either CSA-facilitated, or self-administered
- **Benefits:** Report detailing an organizations capability and maturity in security management, and gaps against NIST CSF

***Voluntary assessment** that is available at **no-cost** to requesting organizations*



Cyber Resilience Review (CRR):
Question Set with Guidance

February 2016

Homeland Security

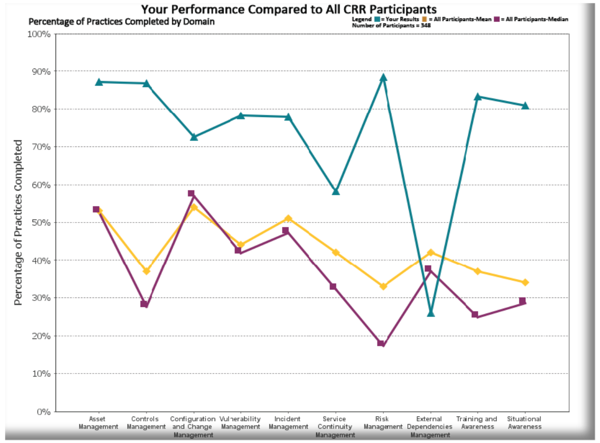
CRR Question Set & Guidance

Cyber Resilience Review Domains

Asset Management Know your assets being protected & their requirements, e.g., Confidentiality, Integrity, and Availability	**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: https://www.cisa.gov/cyber-resource-hub

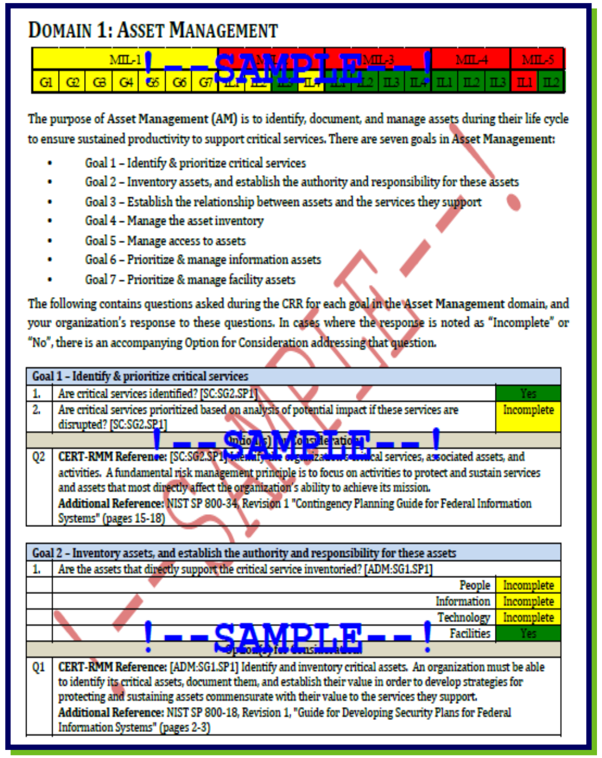
CRR Sample Report includes:



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	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.

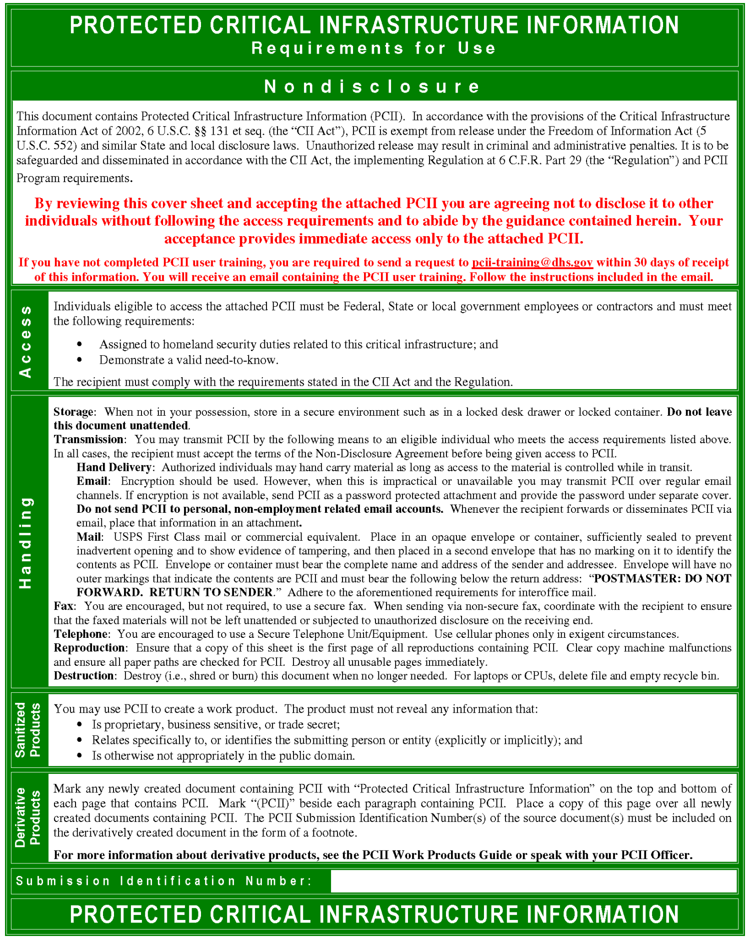
Goal 1 - Identify & prioritize critical services		
1.	Are critical services identified? [SC:SG2.SP1]	Yes
2.	Are critical services prioritized based on analysis of potential impact if these services are disrupted? [SC:SG2.SP1]	Incomplete
Option(s) for Consideration		
Q2	**CERT-RMM Reference:** [SC:SG2.SP1] 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)	

Protected Critical Infrastructure Information

- The Protected Critical Infrastructure Information (PCII) Program protects critical infrastructure information voluntarily shared with the federal government for homeland security purposes.

- PCII protects from release through:
  - ✓ Freedom of Information Act disclosure requests
  - ✓ State, local, tribal, territorial disclosure laws
  - ✓ Use in civil litigation
  - ✓ Use for regulatory purposes



PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

Requirements for Use

Nondisclosure

This document contains Protected Critical Infrastructure Information (PCII). In accordance with the provisions of the Critical Infrastructure Information Act of 2002, 6 U.S.C. §§ 131 et seq. (the "CII Act"), PCII is exempt from release under the Freedom of Information Act (5 U.S.C. 552) and similar State and local disclosure laws. Unauthorized release may result in criminal and administrative penalties. It is to be safeguarded and disseminated in accordance with the CII Act, the implementing Regulation at 6 C.F.R. Part 29 (the "Regulation") and PCII Program requirements.

By reviewing this cover sheet and accepting the attached PCII you are agreeing not to disclose it to other individuals without following the access requirements and to abide by the guidance contained herein. Your acceptance provides immediate access only to the attached PCII.

If you have not completed PCII user training, you are required to send a request to pcii-training@dhs.gov within 30 days of receipt of this information. You will receive an email containing the PCII user training. Follow the instructions included in the email.

Access

Individuals eligible to access the attached PCII must be Federal, State or local government employees or contractors and must meet the following requirements:

- Assigned to homeland security duties related to this critical infrastructure; and
- Demonstrate a valid need-to-know.

The recipient must comply with the requirements stated in the CII Act and the Regulation.

Handling

Storage: When not in your possession, store in a secure environment such as in a locked desk drawer or locked container. **Do not leave this document unattended**.

Transmission: You may transmit PCII by the following means to an eligible individual who meets the access requirements listed above. In all cases, the recipient must accept the terms of the Non-Disclosure Agreement before being given access to PCII.

Hand Delivery: Authorized individuals may hand carry material as long as access to the material is controlled while in transit.

Email: Encryption should be used. However, when this is impractical or unavailable you may transmit PCII over regular email channels. If encryption is not available, send PCII as a password protected attachment and provide the password under separate cover. **Do not send PCII to personal, non-employment related email accounts.** Whenever the recipient forwards or disseminates PCII via email, place that information in an attachment.

Mail: USPS First Class mail or commercial equivalent. Place in an opaque envelope or container, sufficiently sealed to prevent inadvertent opening and to show evidence of tampering, and then placed in a second envelope that has no marking on it to identify the contents as PCII. Envelope or container must bear the complete name and address of the sender and addressee. Envelope will have no outer markings that indicate the contents are PCII and must bear the following below the return address: "**POSTMASTER: DO NOT FORWARD. RETURN TO SENDER**." Adhere to the aforementioned requirements for interoffice mail.

Fax: You are encouraged, but not required, to use a secure fax. When sending via non-secure fax, coordinate with the recipient to ensure that the faxed materials will not be left unattended or subjected to unauthorized disclosure on the receiving end.

Telephone: You are encouraged to use a Secure Telephone Unit/Equipment. Use cellular phones only in exigent circumstances.

Reproduction: Ensure that a copy of this sheet is the first page of all reproductions containing PCII. Clear copy machine malfunctions and ensure all paper paths are checked for PCII. Destroy all unusable pages immediately.

Destruction: Destroy (i.e., shred or burn) this document when no longer needed. For laptops or CPUs, delete file and empty recycle bin.

Sanitized Products

You may use PCII to create a work product. The product must not reveal any information that:

- Is proprietary, business sensitive, or trade secret;
- Relates specifically to, or identifies the submitting person or entity (explicitly or implicitly); and
- Is otherwise not appropriately in the public domain.

Derivative Products

Mark any newly created document containing PCII with "Protected Critical Infrastructure Information" on the top and bottom of each page that contains PCII. Mark "(PCII)" beside each paragraph containing PCII. Place a copy of this page over all newly created documents containing PCII. The PCII Submission Identification Number(s) of the source document(s) must be included on the derivatively created document in the form of a footnote.

For more information about derivative products, see the PCII Work Products Guide or speak with your PCII Officer.

Submission Identification Number:

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

CyHy - Vulnerability Scanning

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

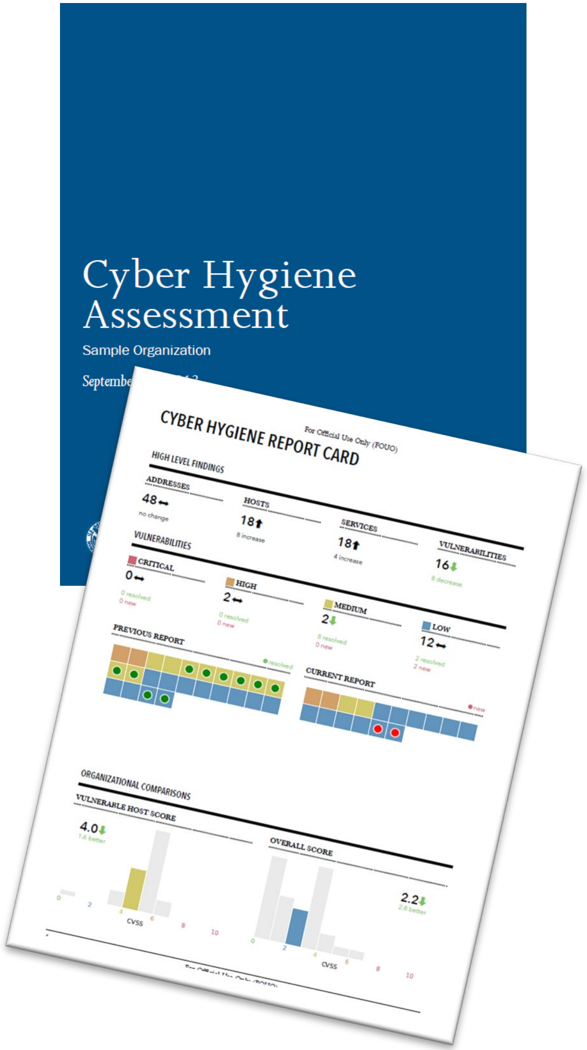
Delivery: Online by CISA

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

- Email us at vulnerability@cisa.dhs.gov with the subject line “Requesting Cyber Hygiene Services” to get started.



Cyber Hygiene Assessment

Sample Organization

Septembe

CYBER HYGIENE REPORT CARD

For Official Use Only (FOUO)

HIGH LEVEL FINDINGS

ADDRESSES 48 ↔ no change

HOSTS 18 ↑ 8 increase

SERVICES 18 ↑ 4 increase

VULNERABILITIES 16 ↓ 8 decrease

VULNERABILITIES

CRITICAL 0 ↔ 0 resolved 0 new

HIGH 2 ↔ 0 resolved 0 new

MEDIUM 2 ↓ 8 resolved 0 new

LOW 12 ↔ 2 resolved 2 new

PREVIOUS REPORT

CURRENT REPORT

ORGANIZATIONAL COMPARISONS

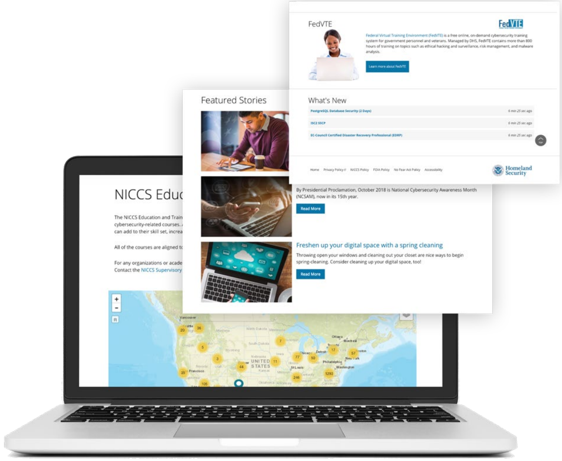
VULNERABLE HOST SCORE 4.0 ↓ 1.6 better

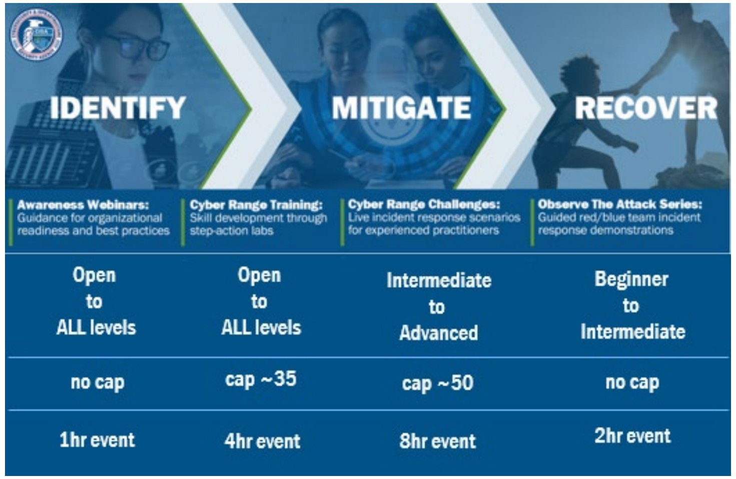
OVERALL SCORE 2.2 ↓ 2.8 better

Cybersecurity Training Resources

CISA is committed to providing the nation with access to cybersecurity training and workforce development efforts to develop a more resilient and capable cyber nation.

- **The NICCS website:** Searchable Training Catalog with over 6,000 cyber-related courses offered by nationwide cybersecurity educators
    - Interactive National Cybersecurity Workforce Framework
    - **FedVTE**
    - Scholarships for Service, Centers for Academic Excellence, and Cyber Competitions
    - Tools and resources for cyber managers
- Incident Response Training though IMR Series
- Industrial Control Systems (ICS) Training



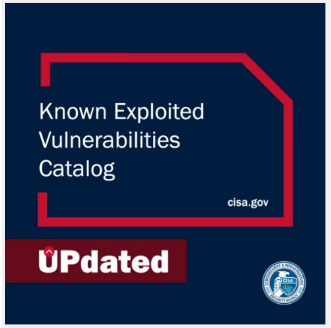

IDENTIFY
MITIGATE
RECOVER

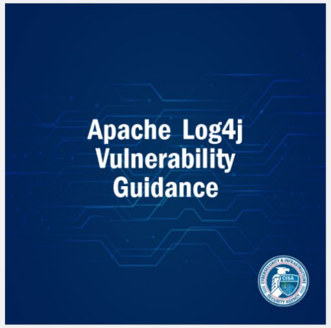
Awareness Webinars: Guidance for organizational readiness and best practices	**Cyber Range Training:** Skill development through step-action labs	**Cyber Range Challenges:** Live incident response scenarios for experienced practitioners	**Observe The Attack Series:** Guided red/blue team incident response 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

For more information, visit https://www.cisa.gov/cybersecurity-training-exercises

Recent CISA Resources:

- Incident and Vulnerability Response Playbooks: https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf
- Known Exploited Vulnerabilities Catalog: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Cyber Incident Resource Guide for Governors: https://www.cisa.gov/gov_cyberguide
- Stop Ransomware: https://www.cisa.gov/stopransomware
- Cyber Training, Exercises, Tabletops: https://www.cisa.gov/cybersecurity-training-exercises
- Free Cyber Tools and Services: https://www.cisa.gov/free-cybersecurity-services-and-tools





CISA Insights
Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats

Additional CISA Resources:

- **CSET Tool Download:** https://www.cisa.gov/stopransomware/cyber-security-evaluation-tool-csetr

- **Cyber Hygiene Services:** email us at vulnerability@cisa.dhs.gov with the subject line “Requesting Cyber Hygiene Services” to get started.

- **Cyber Resource Hub:** https://www.cisa.gov/cyber-resource-hub

- **Cyber Essentials:** https://www.cisa.gov/cyber-essentials

- **Vulnerability Disclosure Policy Template:** https://www.cisa.gov/vulnerability-disclosure-policy-template

- **CISA Incident Reporting Form:** https://us-cert.cisa.gov/forms/report

- **Cybersecurity Training and Exercises:** https://www.cisa.gov/cybersecurity-training-exercises

- **CISA Tabletop Exercise Packages:** https://www.cisa.gov/cisa-tabletop-exercises-packagesCISA

- **Know Exploited Vulnérabilités (KEV) Catalog:** https://www.cisa.gov/known-exploited-vulnerabilities-catalog

- **Cyber Incident Response : https://us-cert.cisa.gov/forms/report and/or Filing a Complaint with IC3:** https://www.ic3.gov/

Additional Information Sharing Opportunities

- **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.

Elections Infrastructure ISAC™

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

ONG-ISAC

National Defense ISAC

RETAIL & HOSPITALITY ISAC

Real Estate ISAC Information Sharing and Analysis Center
Serving the Commercial Facilities Sector

WATER ISAC

SPACE ISAC

REN-ISAC

DNG-ISAC

H-ISAC HEALTH - ISAC

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA

Maritime Transportation System Information Sharing and Analysis Center

M+E ISAC MEDIA + ENTERTAINMENT INFORMATION SHARING ANALYSIS CENTER

FS-ISAC

IT ISAC

E-ISAC ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

AUTO-ISAC Automotive Information Sharing and Analysis Center

AVIATION ISAC

Ashley Jones
Cybersecurity Advisor, Region 3
National Capitol Region
Ashley.Jones@cisa.dhs.gov

Regional Support:
CISARegion3@hq.dhs.gov

To Report an Incident:
https://us-cert.cisa.gov/report

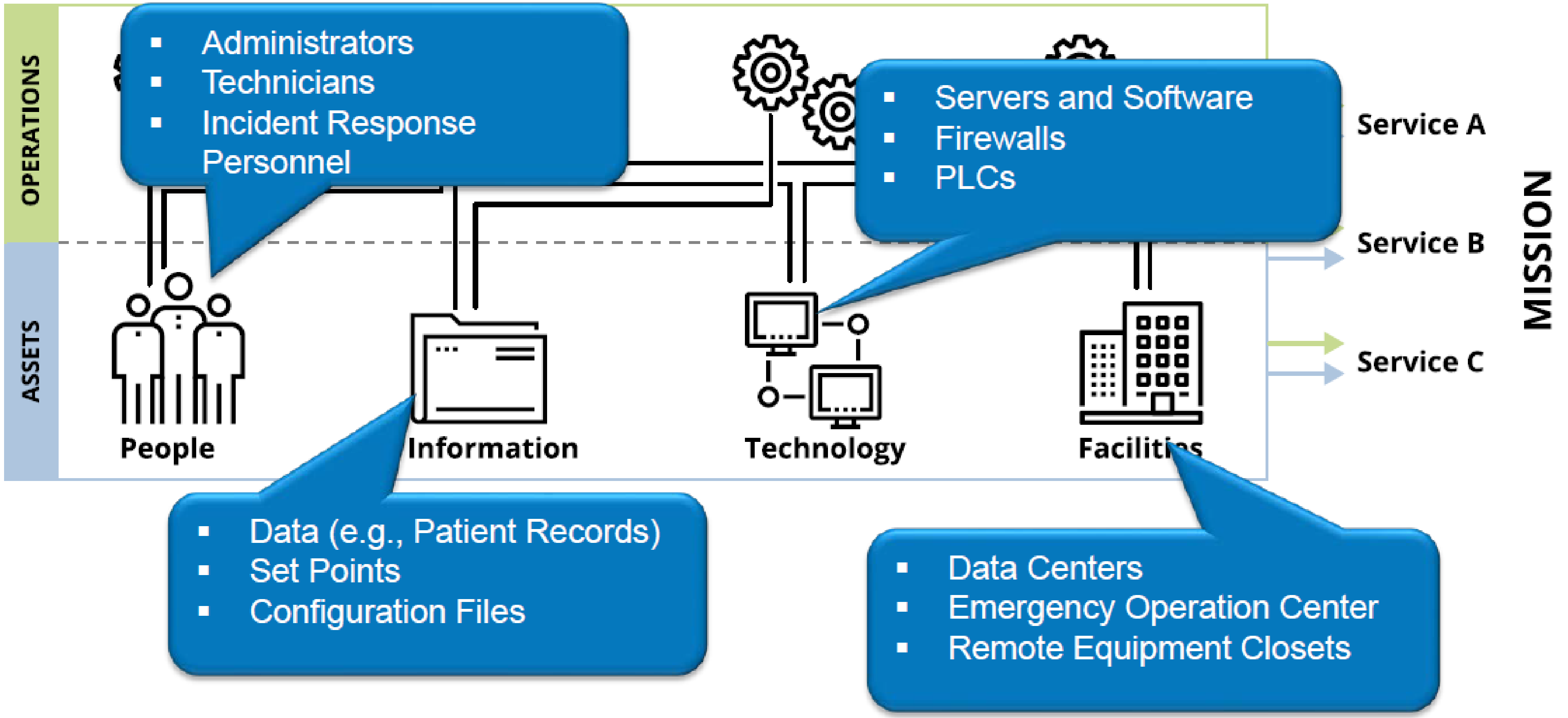
Media Inquiries:
CISAMedia@cisa.dhs.gov

CYBERSECURITY & INFRASTRUCTURE

CISA

SECURITY AGENCY

Critical Service Assets and Examples



- Administrators
- Technicians
- Incident Response Personnel

- Servers and Software
- Firewalls
- PLCs

- Data (e.g., Patient Records)
- Set Points
- Configuration Files

- Data Centers
- Emergency Operation Center
- Remote Equipment Closets