CISA CYBER MISSION AND RESOURCE BRIEF

Ernesto Ballesteros, JD, MS, CISSP, CISA, Security+
Cybersecurity State Coordinator of Texas
Region 6 | Texas

AGENDA:

- About CISA
- Cybersecurity Resources & Services
- Information Sharing & Situational Awareness Resources
- Training & Education Resources
- Incident Reporting
- Next Steps for Partnering

About CISA

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient infrastructure for the American people.

MISSION

CISA partners with industry and government to understand and manage risk to our Nation's critical infrastructure.

OVERALL GOALS

GOAL 1

DEFEND TODAY

Defend against urgent threats and hazards

seconds | days | weeks

GOAL 2

SECURE TOMORROW

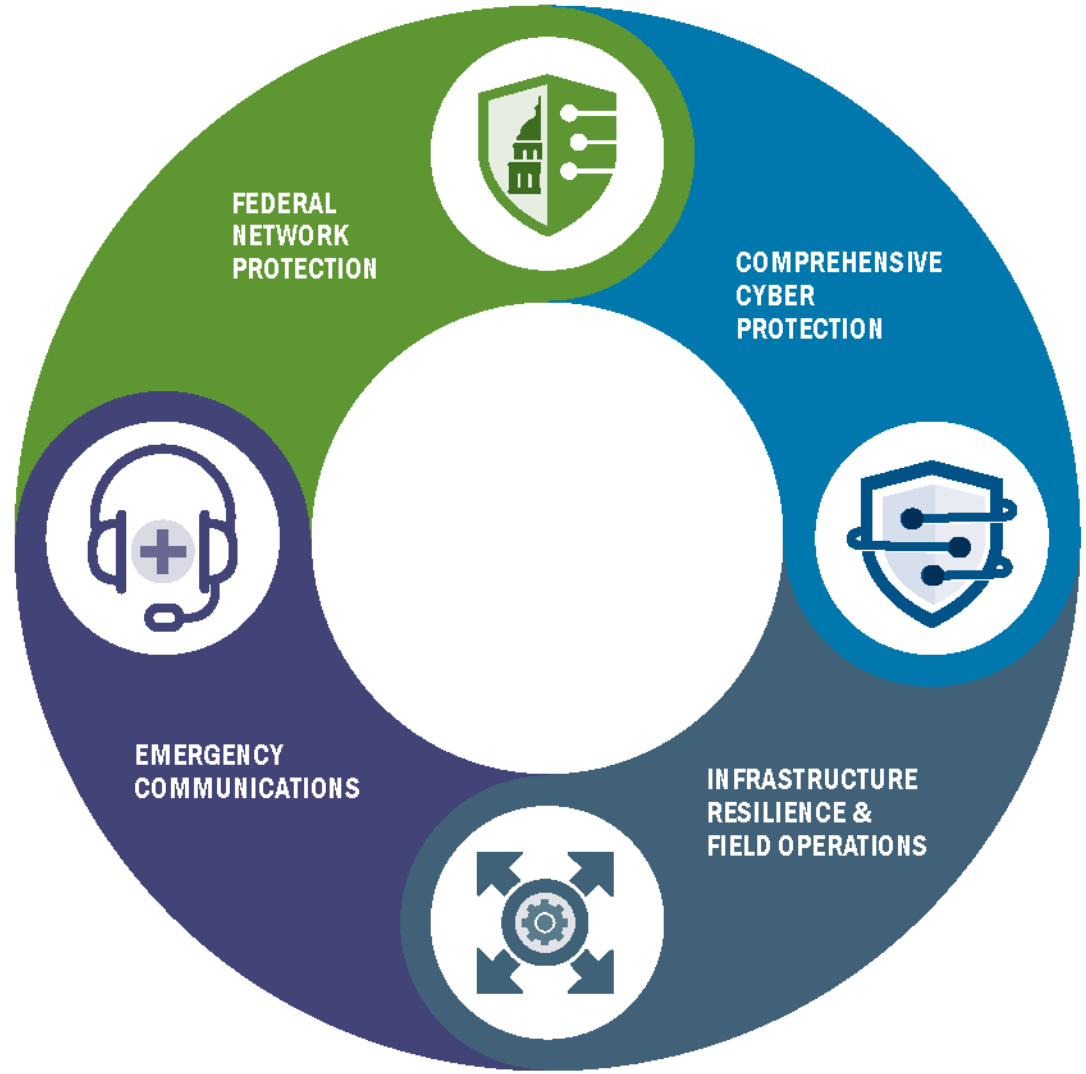
Strengthen critical infrastructure and address long-term risks

months | years | decades

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

We are the Nation's Risk Advisor

The Cybersecurity and Infrastructure Security Agency (CISA) is the pinnacle of national risk management for cyber and physical infrastructure

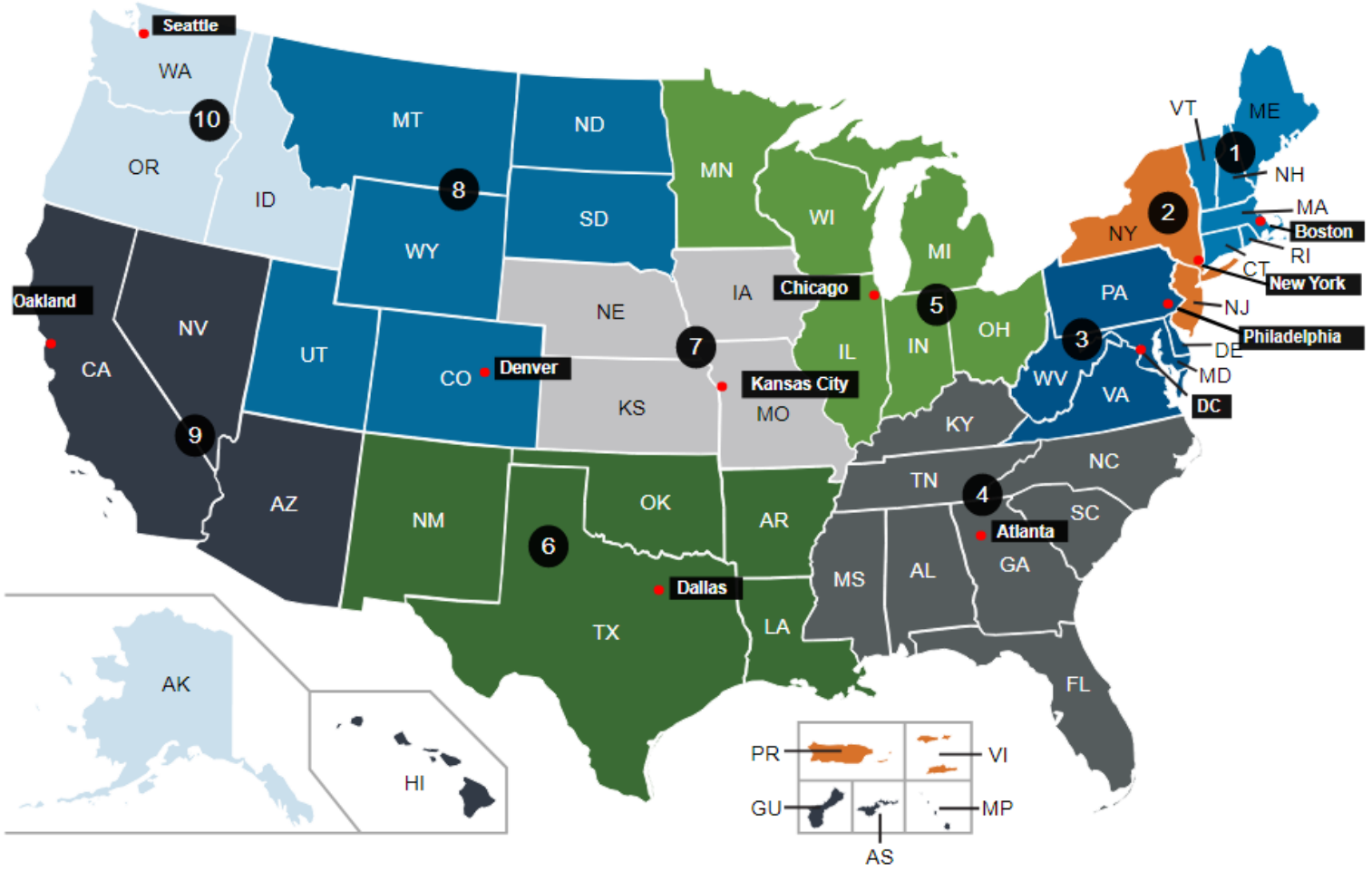


Critical Infrastructure Sectors

CISA assists the public and private sectors to secure their networks and focuses on organizations in the following 16 critical infrastructure sectors, per Presidential Policy Directive 21.

CISA Regions

Region	Location
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



[CISA Region 6: CISARegion6@hq.dhs.gov](mailto:CISARegion6@hq.dhs.gov)

Cybersecurity State Coordinator (Texas)

§665c. Cybersecurity State Coordinator

[6 United States Code, Section 665(c) (2021)]

(a) Appointment

The Director shall appoint an employee of the Agency in each State, with the appropriate cybersecurity qualifications and expertise, who shall serve as the Cybersecurity State Coordinator.

(b) Duties

The duties of a Cybersecurity State Coordinator appointed under subsection (a) shall include-

(1) building strategic public and, on a voluntary basis, private sector relationships, including by advising on establishing governance structures to facilitate the development and maintenance of secure and resilient infrastructure;

(2) serving as the Federal cybersecurity risk advisor and supporting preparation, response, and remediation efforts relating to cybersecurity risks and incidents;

(3) facilitating the sharing of cyber threat information to improve understanding of cybersecurity risks and situational awareness of cybersecurity incidents;

(4) raising awareness of the financial, technical, and operational resources available from the Federal Government to non-Federal entities to increase resilience against cyber threats;

(5) supporting training, exercises, and planning for continuity of operations to expedite recovery from cybersecurity incidents, including ransomware;

(6) serving as a principal point of contact for non-Federal entities to engage, on a voluntary basis, with the Federal Government on preparing, managing, and responding to cybersecurity incidents;

(7) assisting non-Federal entities in developing and coordinating vulnerability disclosure programs consistent with Federal and information security industry standards;

(8) assisting State, local, Tribal, and territorial governments, on a voluntary basis, in the development of State cybersecurity plans;

(9) coordinating with appropriate officials within the Agency; and

(10) performing such other duties as determined necessary by the Director to achieve the goal of managing cybersecurity risks in the United States and reducing the impact of cyber threats to non-Federal entities.

(c) Feedback

The Director shall consult with relevant State, local, Tribal, and territorial officials regarding the appointment, and State, local, Tribal, and territorial officials and other non-Federal entities regarding the performance, of the Cybersecurity State Coordinator of a State.

(Pub. L. 107–296, title XXII, §2217, formerly §2215, as added Pub. L. 116–283, div. A, title XVII, §1717(a)(1)(B), Jan. 1, 2021, 134 Stat. 4099 ; renumbered §2217 and amended Pub. L. 117–81, div. A, title XV, §1547(b)(1)(A)(iv), Dec. 27, 2021, 135 Stat. 2061 .)

Ernesto Ballesteros, JD, MS, CISSP, CISA
Cybersecurity State Coordinator of Texas
Email: ernesto.ballesteros@cisa.dhs.gov

Cybersecurity State Coordinator of Texas

PROFESSIONAL EXPERIENCE

- Cybersecurity State Coordinator of Texas, Cybersecurity & Infrastructure Security Agency, (Washington D.C.; Texas/Region 6)
- Adjunct Law Professor, St. Mary's University School of Law *NSA/DHS CAE-CDE (San Antonio, Texas)
- Information Security Officer, The Alamo Colleges District (San Antonio, Texas)
- State Cybersecurity Coordinator, Texas Department of Information Resources (Austin, Texas)
- Chairman, Texas Cybersecurity Council, Texas Department of Information Resources (Austin, Texas)
- Information Systems Auditor, CPS Energy (San Antonio, Texas)
- Director, The Center for Information Assurance Management and Leadership (a nationally recognized NSA/DHS Center for Academic Excellence in Cyber Defense Education)
- Assistant Professor of Computer Information Systems and Security, Our Lady of the Lake University *NSA/DHS CAE-CDE (San Antonio, Texas)
- Information Security Officer, Jefferson Bank (San Antonio, Texas)
- Information Security Consultant, Omnikron Systems, Inc. (Los Angeles, California)

FORMAL EDUCATION

- Law School: Doctor of Jurisprudence (IT, Intellectual Property, and Privacy Law)
- Graduate School: Master of Science, Computer Information Systems and Security
- Undergraduate: Bachelor of Science, Computer Information Systems and Security

PROFESSIONAL CREDENTIALS

- (ISC)2 Computer Information Systems Security Professional (CISSP)
- ISACA Certified Information Systems Auditor (CISA)
- CompTIA Security+

Ernesto Ballesteros, JD, MS, CISSP, CISA
Cybersecurity State Coordinator of Texas
Email: ernesto.ballesteros@cisa.dhs.gov

Cybersecurity Advisors (CSAs)

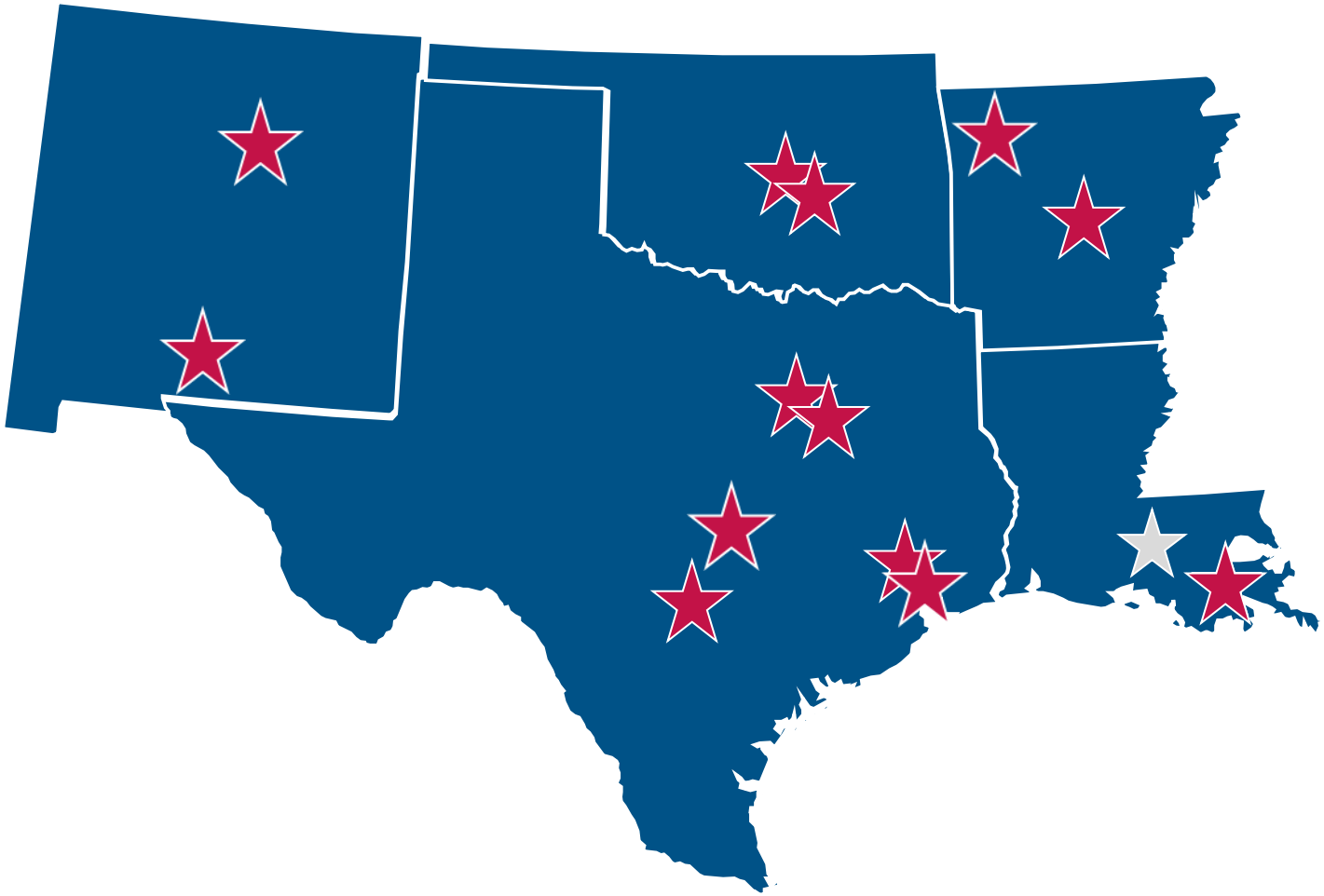
To provide direct coordination, outreach, and regional support in order to protect cyber components essential to the sustainability, preparedness, and protection of the Nation's Critical Infrastructure and Key Resources (CIKR) and State, Local, Tribal, and Territorial (SLTT) governments.

- **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.

Reg 6 | On-Hand / Projected Cyber Personnel

On-Hand

Projected



Cybersecurity and Election Security Resources and Services

CISA's No-Cost Cybersecurity Resources

CISA's Cybersecurity State Coordinators & Cybersecurity Advisors (CSAs)

- **Cybersecurity Assessments**
  - **Baseline Assessments**
    - Ransomware Readiness Assessment (RRA)
    - Cybersecurity Performance Goals (CPG)
  - **Intermediate Assessments**
    - Cyber Infrastructure Survey (CIS)
    - Cyber Resilience Essentials (CRE)
  - **Advanced Assessments**
    - External Dependencies Management (EDM)
    - Incident Management Review (IMR)
    - Cyber Resilience Review (CRR)
- **Cyber Hygiene Services**
  - External Vulnerability Scanning Service
  - Web Application Scanning Service
- **Workshops & Exercises**
  - Asset Management Workshop (AMW)
  - Cyber Resilience Workshop (CRW)
  - Incident Management Workshop (IMW)
  - Vulnerability Management Workshop (VMW)
  - Digital Forensics Workshop I (DFW I)
  - Digital Forensics Workshop II (DFW II)
  - Cyber Tabletop Exercise (CTTX)
- **Technical Assessments***
  - Remote Penetration Test (RPT)
  - Risk and Vulnerability Assessment (RVA)
  - Validated Architecture Design Review (VADR)

***Note:** Eligibility for technical assessments is contingent upon assessment of the stakeholder's capabilities by their Cybersecurity Advisor (CSA).

Cybersecurity State Coordinator (TX): ernesto.ballesteros@cisa.dhs.gov

Cybersecurity Assessments

Cybersecurity Performance Goals (CPGs)

The CPGs are a prioritized subset of IT and operational technology (OT) cybersecurity practices that critical infrastructure owners and operators can implement to meaningfully reduce the likelihood and impact of known risks and adversary techniques.

The goals were informed by existing cybersecurity frameworks and guidance, as well as the real-world threats and adversary tactics, techniques, and procedures (TTPs) observed by CISA and its government and industry partners.

By implementing these goals, owners and operators will not only reduce risks to critical infrastructure operations, but the also the American people.

CPG Checklist

This document is to be used in tandem with the CPGs to help prioritize and track your organization's implementation.

ACCOUNT SECURITY (1.0)

1.1 Detection of Unsuccessful (Automated) Login Attempts — PR.AC-7	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT
COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** LOW **TTP OR RISK ADDRESSED:** Brute Force - Password Guessing (T1110.001) Brute Force - Password Cracking (T1110.002) Brute Force - Password Spraying (T1110.003) Brute Force - Credential Stuffing (T1110.004) **RECOMMENDED ACTION:** All unsuccessful logins are logged and sent to an organization's security team or relevant logging system. Security teams are notified (e.g., by an alert) after a specific number of consecutive, unsuccessful login attempts in a short period (e.g., 5 failed attempts over 2 minutes). This alert is logged and stored in the relevant security or ticketing system for retroactive analysis. For IT assets, there is a system-enforced policy that prevents future logins for the suspicious account. For example, this could be for some minimum time, or until the account is re-enabled by a privileged user. This configuration is enabled when available on an asset. For example, Windows 11 can automatically lock out accounts for 10 minutes after 10 incorrect logins over a 10 minute period.	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED

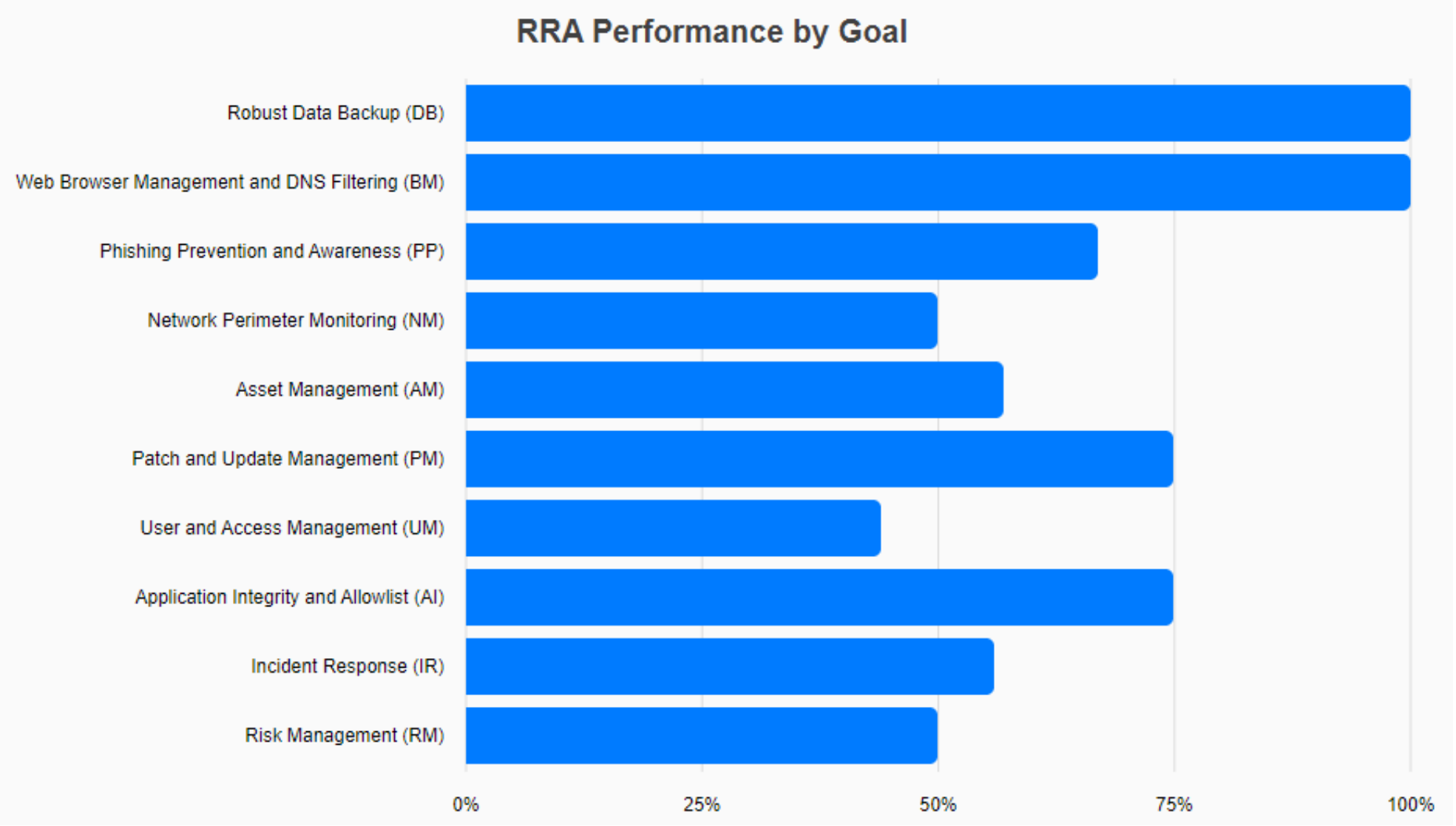
Ransomware Readiness Assessment (RRA)

To understand your cybersecurity posture and assess how well your organization is equipped to defend and recover from a ransomware incident, take the Ransomware Readiness Assessment (RRA). The RRA is a self-assessment based on a tiered set of practices to help organizations better assess how well they are equipped to defend and recover from a ransomware incident.

The RRA:

- Helps organizations evaluate their cybersecurity posture, with respect to ransomware, against recognized standards and best practice recommendations in a systematic, disciplined, and repeatable manner.
- Guides asset owners and operators through a systematic process to evaluate their operational technology (OT) and information technology (IT) network security practices against the ransomware threat.
- Provides an analysis dashboard with graphs and tables that present the assessment results in both summary and detailed form.

Goal Completion Summary Example



Cybersecurity Infrastructure Survey (CIS)

Structured, interview-based assessment (3 hours) of essential cybersecurity practices in-place for critical services within your organization.

Identifies interdependencies, capabilities, and the emerging effects related to current cybersecurity posture.

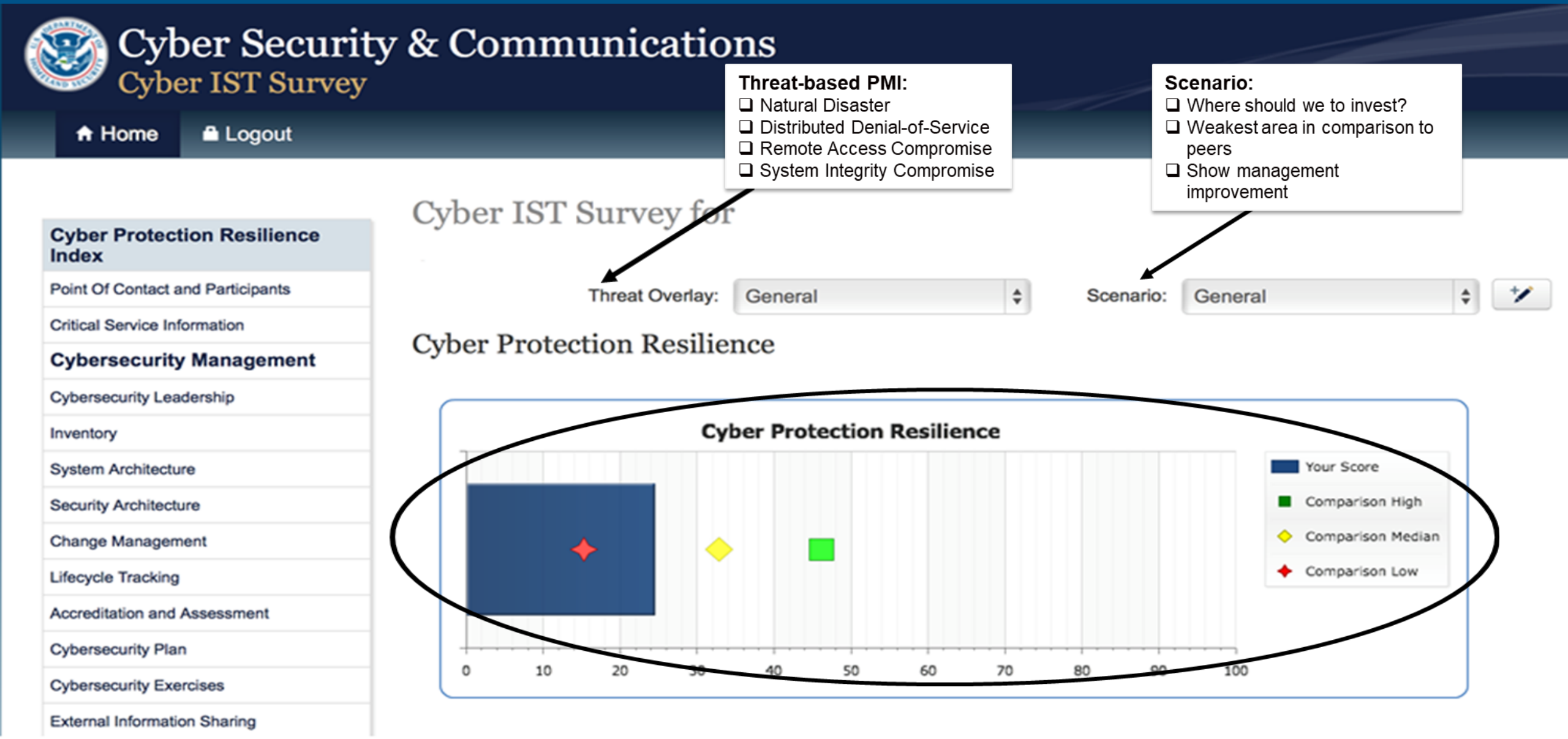
Focuses on protective measures, threat scenarios, and a service-based view of cybersecurity in context of the surveyed topics.

Broadly aligns to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).

CIS Survey Question Domains

CIS Domains	
Cybersecurity Forces	**Cybersecurity Management**
* Personnel	* Cybersecurity Leadership
* Cybersecurity Training	* Cyber Service Architecture
Cybersecurity Controls	* Change Management
* Authentication and Authorization Controls	* Lifecycle Tracking
* Access Controls	* Assessment and Evaluation
* Cybersecurity Measures	* Cybersecurity Plan
* Information Protection	* Cybersecurity Exercises
* User Training	* Information Sharing
* Defense Sophistication and Compensating Controls	**Dependencies**
Incident Response	* Data at Rest
* Incident Response Measures	* Data in Motion
* Alternate Site and Disaster Recovery	* Data in Process
	* End Point Systems

Example CIS Dashboard



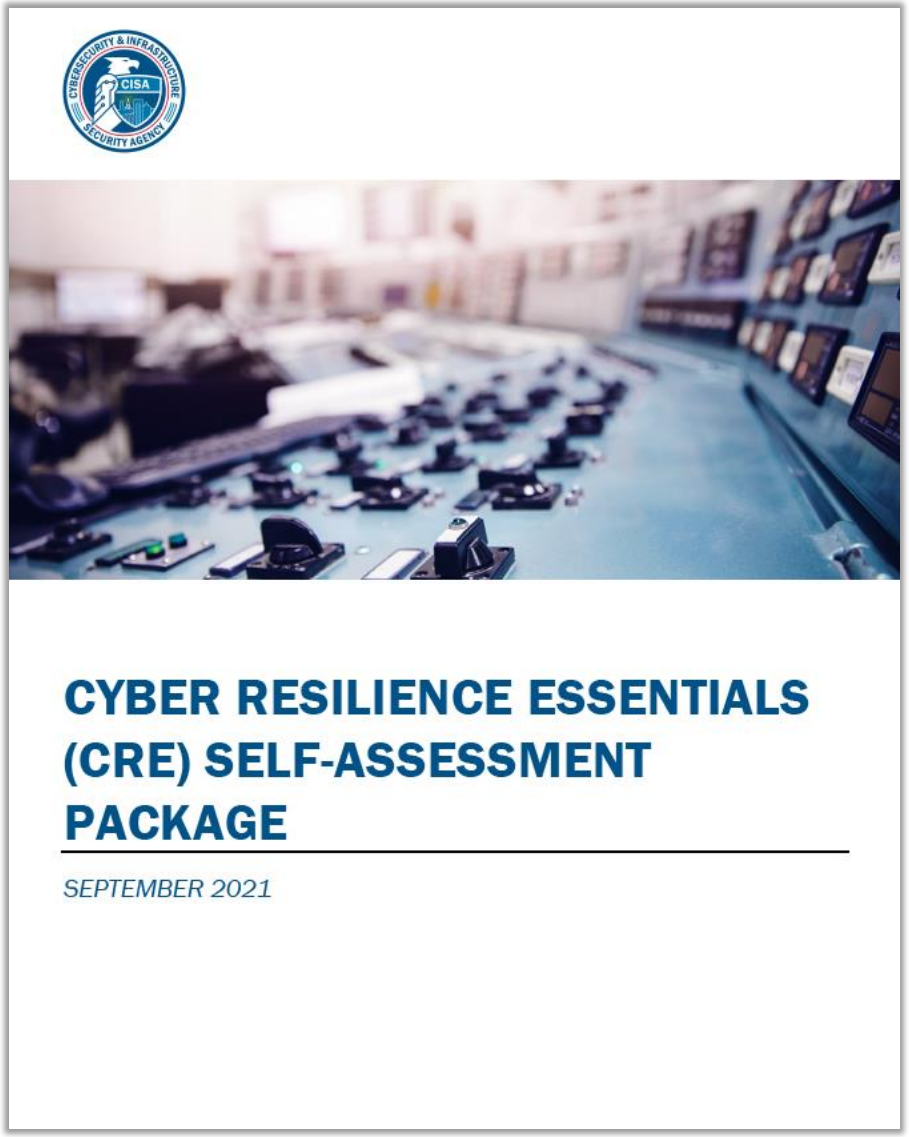
Cyber Resilience Essentials (CRE)

Purpose: An interview-based assessment that evaluates an organization's operational resilience and cybersecurity practices.

Evaluates that maturity of an organization's capacities and capabilities in performing, planning, managing, measuring, and defining cybersecurity capabilities.

Goal: Identify Cybersecurity Strengths & Weaknesses

- 11 Domains
- 103 Practices

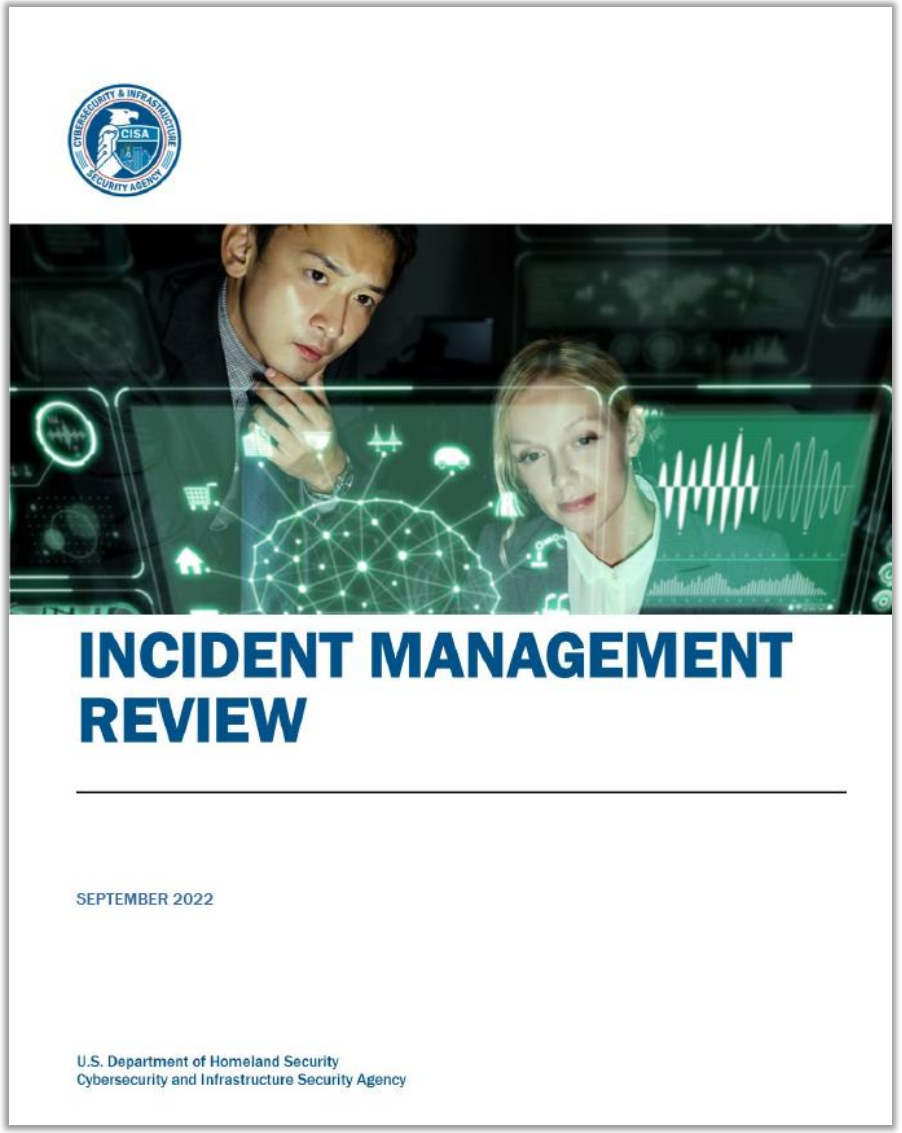


Incident Management Review (IMR)

Purpose: An interview-based assessment of an organization's event and incident handling practices.

Goal: Provides an organization with a more robust awareness of its event and incident handling and response activities.

- Reviews the activities essential to managing events and incidents to an organization's suite of critical services
- Provides a baseline of practice
- Assists an organization with identifying areas for improvement to strengthen incident handling and response activities
- Provides a comprehensive final report that includes options for consideration

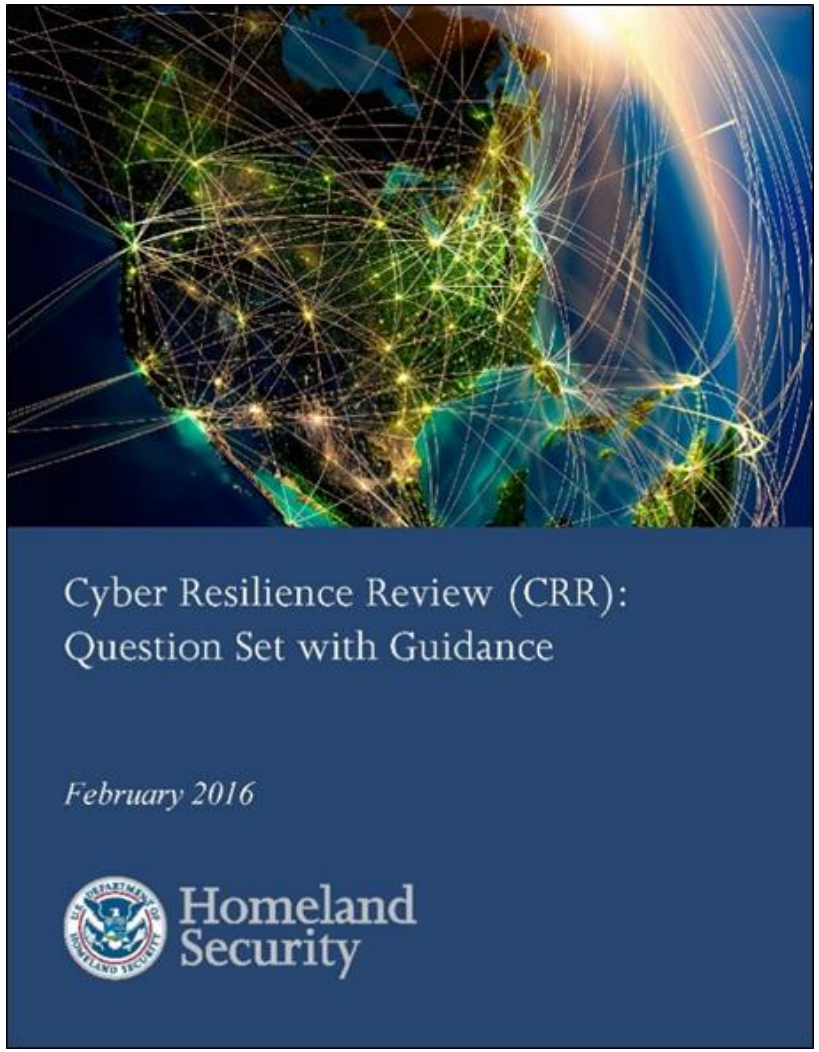


Cyber Resilience Review (CRR)

Purpose: The CRR is an assessment intended to evaluate an organization's operational resilience and cybersecurity practices of its critical services

Goal: Helps partners understand and measure cyber security capabilities as they relate to operational resilience and cyber risk

- Evaluates the maturity of an organization's capacities and capabilities in performing, planning, managing, measuring, and defining cybersecurity capabilities
- Based on the CERT ® Resilience Management Model (CERT® RMM)



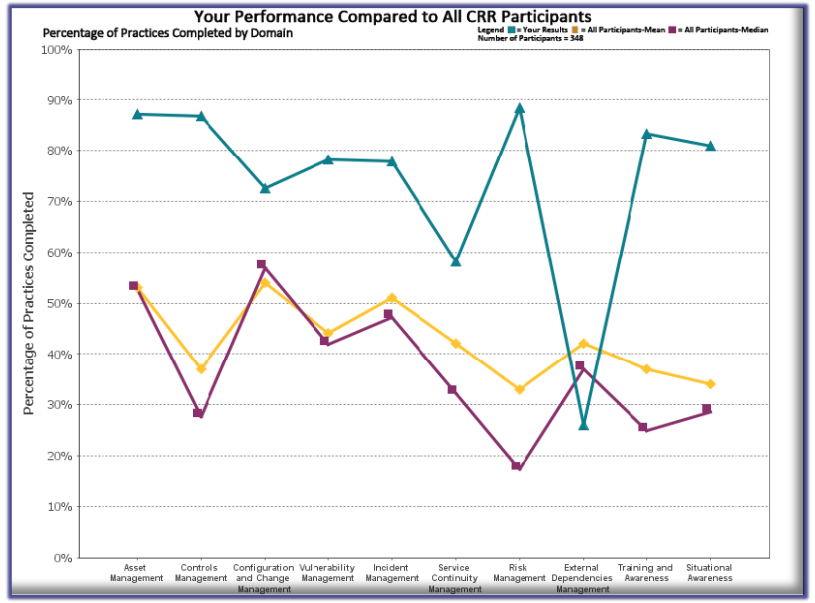
Cyber Resilience Review (CRR) | Domains

These represent key areas that typically contribute to an organization's cyber resilience— each domain focuses on:

- Documentation in place, and periodically reviewed & updated
- Communication and notification to all those who need to know
- Execution/Implementation & analysis in a consistent, repeatable manner
- Alignment of goals and practices within and across CRR domains

AM	**Asset Management** *identify, document, and manage assets during their life cycle*	SCM	**Service Continuity Management** *ensure continuity of IT operations in the event of disruptions*
CCM	**Configuration and Change Management** *ensure the integrity of IT systems and networks*	RISK	**Risk Management** *identify, analyze, and mitigate risks to services and IT assets*
CNTL	**Controls Management** *identify, analyze, and manage IT and security controls*	EXD	**External Dependency Management** *manage IT, security, contractual, and organizational controls that are dependent on the actions of external entities*
VM	**Vulnerability Management** *identify, analyze, and manage vulnerabilities*	TRNG	**Training and Awareness** *promote awareness and develop skills and knowledge*
IM	**Incident Management** *identify and analyze IT events, detect cyber security incidents, and determine an organizational response*	SA	**Situational Awareness** *actively discover and analyze information related to immediate operational stability and security*

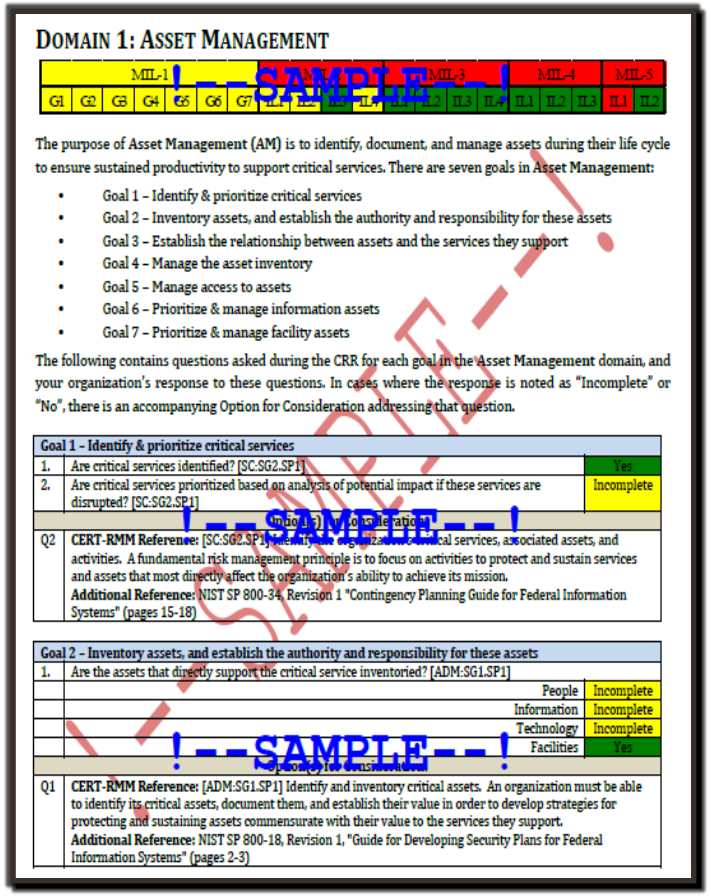
Benefits of CRR



Comparison data with other CRR participants

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

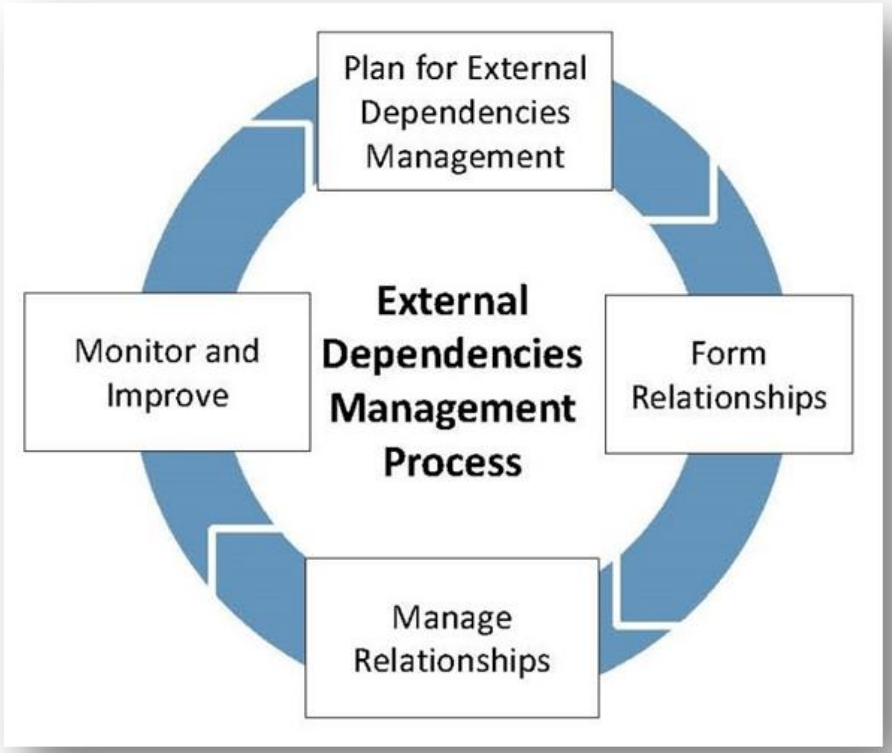
CRR Mappings to Other Frameworks

The Cyber Resilience Review has been mapped to:

- NIST Cybersecurity Framework (CSF)
- Health Insurance Portability and Accountability Act (HIPAA) Security Rule
- Federal Financial Institutions Examination Council's (FFIEC) Cybersecurity Assessment Tool (CAT)
- NIST Special Pub 800-53 rev 4 (This mapping has not yet been published)

Most Cybersecurity Frameworks are being mapped to the NIST Cybersecurity Framework as a result that mapping can be used to indirectly map them to the CRR

External Dependencies Management (EDM)



EDM process outlined in the External Dependencies Management Resource Guide

Overview: In 2016, DHS launched the External Dependencies Management (EDM) Assessment, focusing specifically on ensuring the protection and sustainment of services and assets that are dependent on the actions of third-party entities.

Background: External Dependencies Management is a domain covered by the CRR. However, EDM and associated issues (e.g., supply-chain management, vendor management) are not addressed at a comprehensive level within the CRR, resulting in the creation of a separate assessment.

Linkages to CRR: Despite operating at a more granular level than the CRR, the EDM Assessment borrows heavily from the CRR's methodological architecture and scoring system but remains a CISA facilitated assessment.

External Dependency Management (EDM)

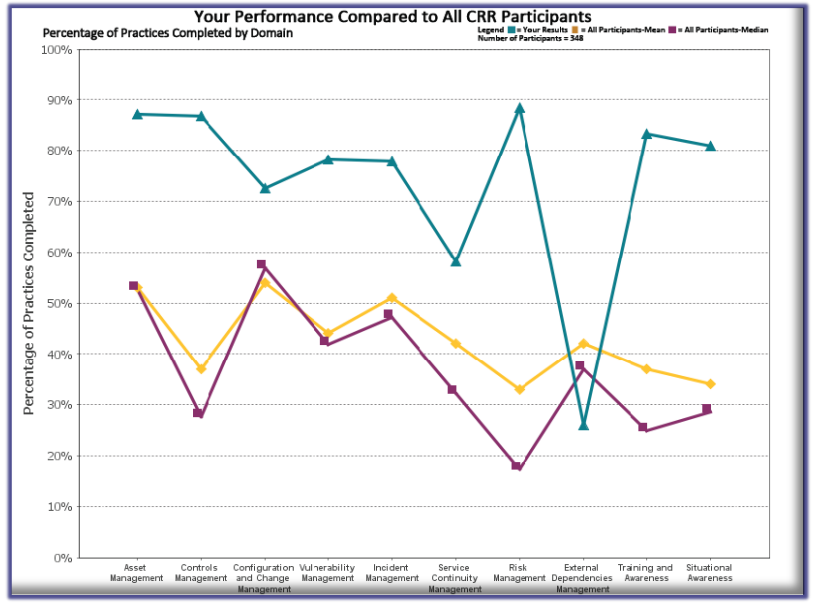
To provide the organization with an understandable and useful structure for the evaluation, the EDM Assessment is divided into three distinct areas (domains):

1. **RELATIONSHIP FORMATION** – how the organization considers third party risks, selects external entities, and forms relationships with them so that risk is managed from the start

2. **RELATIONSHIP MANAGEMENT AND GOVERNANCE** – how the organization manages ongoing relationships with external entities to support and strengthen its critical services at a managed level of risk and cost

3. **SERVICE PROTECTION AND SUSTAINMENT** – how the organization plans for, anticipates, and manages disruption or incidents related to external entities

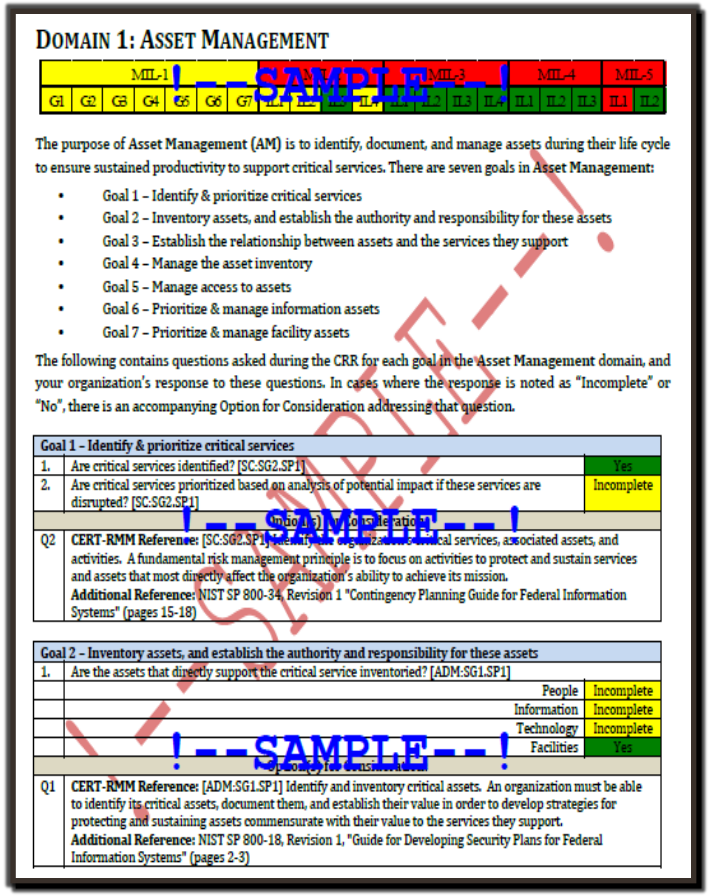
Benefits of EDM



Comparison data with other EDM participants

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

!--SAMPLE--!

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 your 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)	

!--SAMPLE--!

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)	

!--SAMPLE--!

Cybersecurity Workshops & Exercises

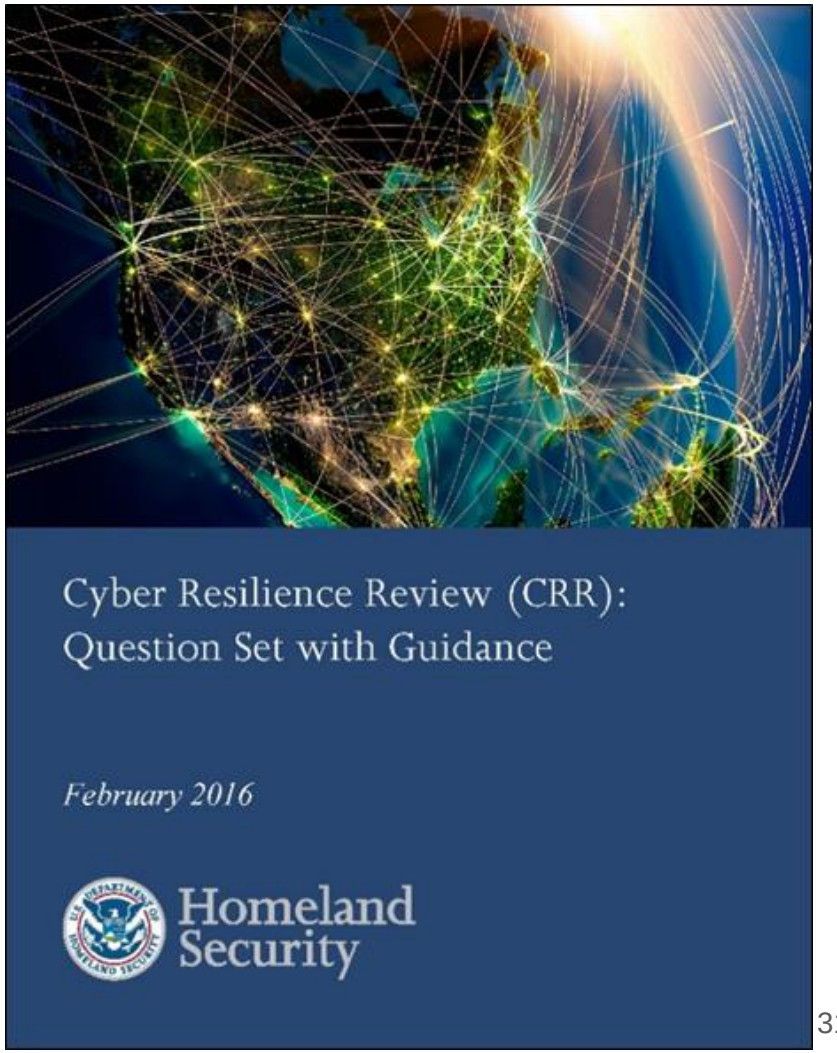
Cyber Resilience Workshop (CRW)

Description: A 2- or 4-hour non-technical and informative session designed to help organizations understand cyber resilience concepts and ways to improve management of cyber resilience.

Goal: The goal of the workshop is to provide your organization with tangible takeaway information related to risk-based decision making and security planning for critical services.

Audience: Organizations that want to learn about an approach to developing repeatable cybersecurity capabilities and practices to protect and sustain their organization's operating environment.

Format: In-Person or Virtual



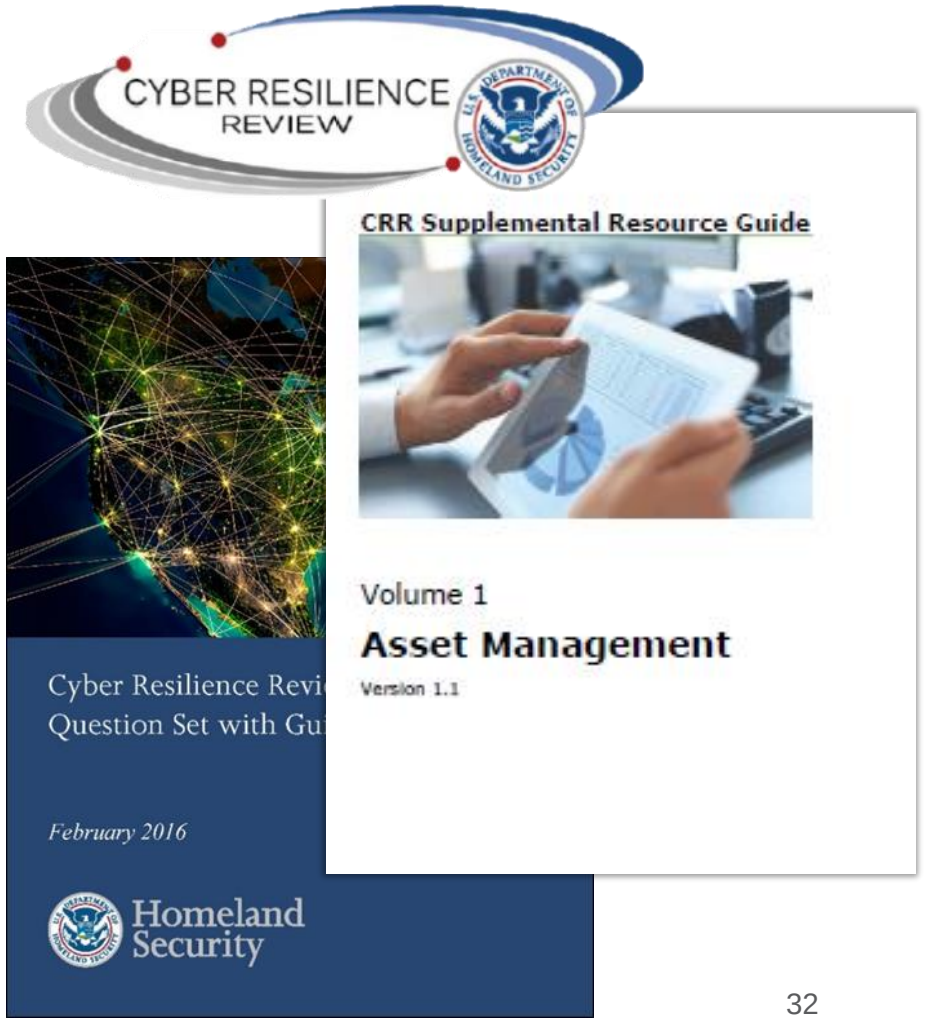
Asset Management Workshop (AMW)

Description: A 2-hour non-technical and informative session designed to help organizations understand asset management concepts and key elements for effective planning and implementation.

Goal: The goal of the workshop is to provide your organization with tangible takeaway information on how to establish inventory of high-value assets and defines how to ensure their productivity in support of the organization's critical services.

Audience: Organizations that want to learn about an approach to developing an asset management plan to identify, document, and manage their assets.

Format: In-Person or Virtual



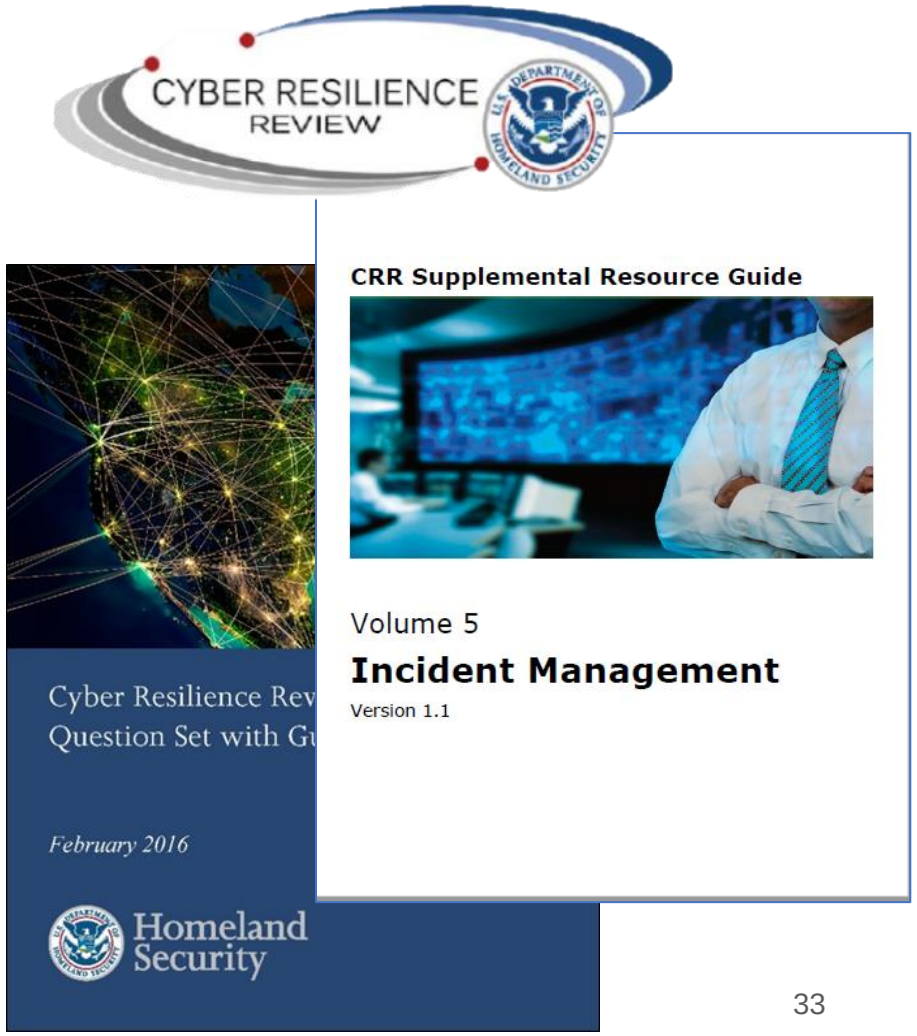
Incident Management Workshop (IMW)

Description: A 2-hour non-technical and informative session designed to help organizations understand incident management concepts, key elements, planning and implementation.

Goal: The goal of the workshop is to provide organizations with tangible, useful takeaway information on how to manage cybersecurity incidents effectively and, ultimately, achieve operational resilience.

Audience: Organizations that want to learn about an approach to developing a cyber incident management capability.

Format: In-Person or Virtual



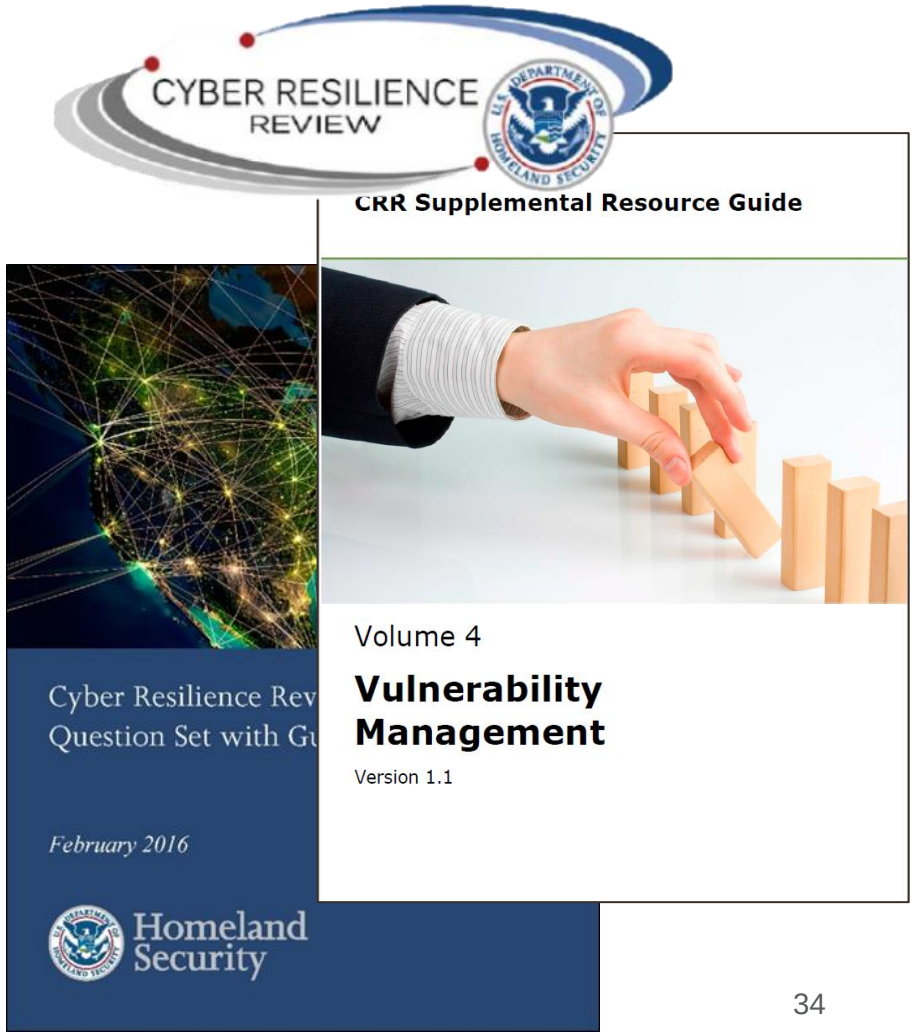
Vulnerability Management Workshop (VMW)

Description: A 2-hour non-technical and informative session designed to help organizations understand vulnerability management concepts, key elements, planning and implementation.

Goal: The goal of the workshop is to provide your organization with tangible takeaway information on how to manage cybersecurity vulnerabilities effectively and ultimately achieve operational resilience.

Audience: Organizations that want to learn about an approach to developing a cyber vulnerability management program to identify, analyze, and manage vulnerabilities in their operating environment.

Format: In-Person or Virtual



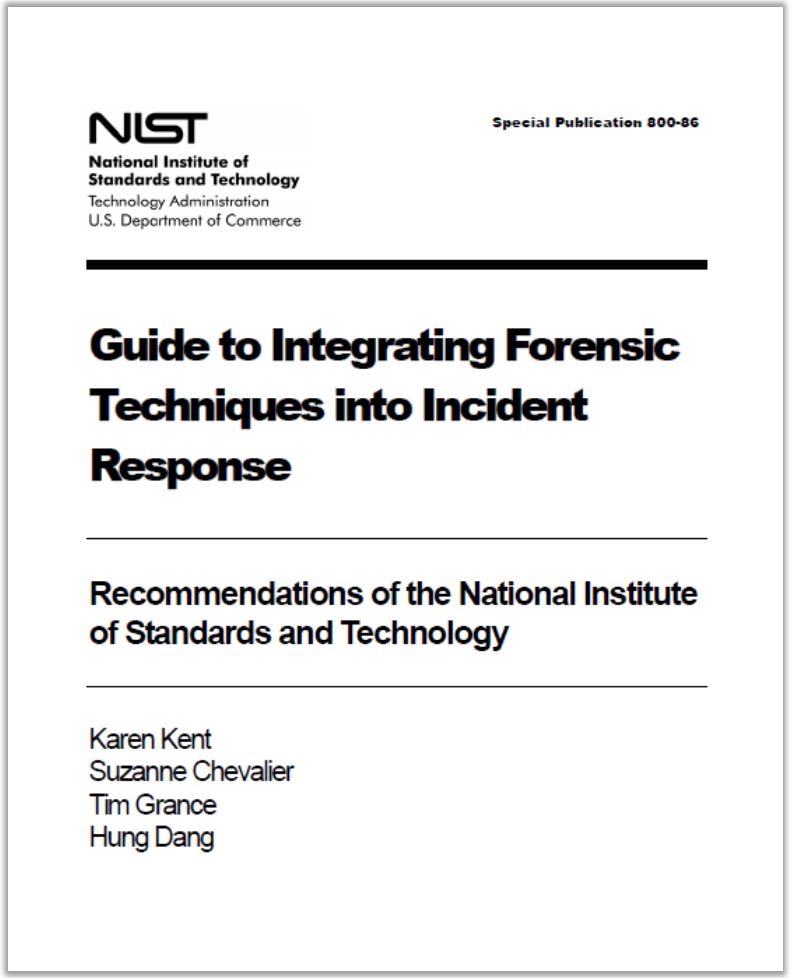
Introduction to Digital Forensics Workshop (DFW)

Description: A 3-hour informative and hands-on session designed to help organizations understand digital forensics concepts, key elements, planning and implementation.

Goal: The goal of the workshop is to provide your organization with tangible takeaway information on how to manage digital forensics effectively.

Audience: Tailored for incident response teams; forensic analysts; system, network, and security administrators; and computer security program managers who are responsible for performing forensics for investigative, incident response, or troubleshooting purposes.

Required: A laptop is required for the hands-on portion of the workshop.


NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-86

Guide to Integrating Forensic Techniques into Incident Response

Recommendations of the National Institute of Standards and Technology

Karen Kent
Suzanne Chevalier
Tim Grance
Hung Dang

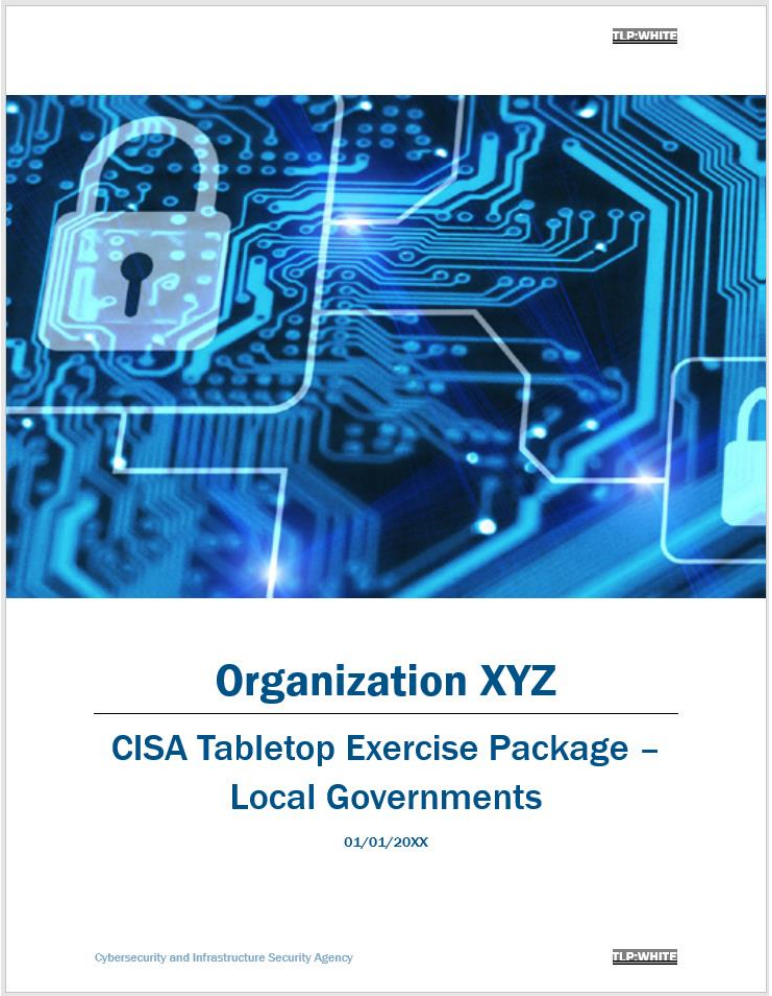
Facilitated Cyber Exercise (FCE)

Description: A 2-hour or 4-hour non-technical facilitated cybersecurity tabletop exercise, where organizations are presented with a cyber threat-based scenario and are challenged to consider how their organization would respond, based on existing incident response plans.

Goal: The goal of the exercise is to provide organizations an opportunity to assess their level of readiness to respond to and recover from a cybersecurity incident impacting their operating environment.

Audience: Organizations that want to assess their level of readiness to respond to and recover from a cybersecurity incident.

Format: In-Person or Virtual



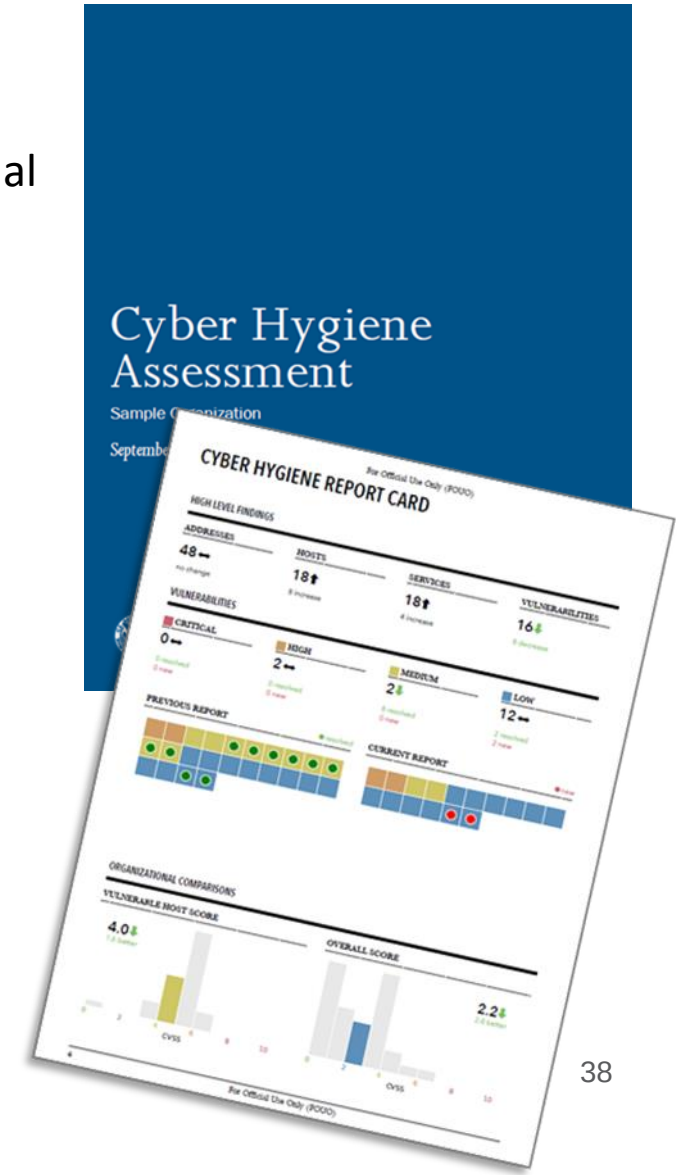
National Resources

Vulnerability Scanning Service (CyHy)

CISA's Vulnerability Scanning (VS) is persistent "internet scanning-as-a-service". VS service continuously assesses the health of your internet-accessible assets by checking for known vulnerabilities, weak configurations—or configuration errors—and suboptimal security practices. VS service also recommends ways to enhance security through modern web and email standards.

VS service includes:

- **Target Discovery** identifies all active internet-accessible assets (networks, systems, and hosts) to be scanned.
- **Vulnerability Scanning** initiates non-intrusive checks to identify potential vulnerabilities and configuration weaknesses.
- **Weekly Report** of known vulnerabilities detected on Internet-facing hosts for your organization, as well as recommended remediations.



Web Application Scanning (WAS)

CISA's Cyber Hygiene Web Application Scanning is "internet scanning-as-a-service."

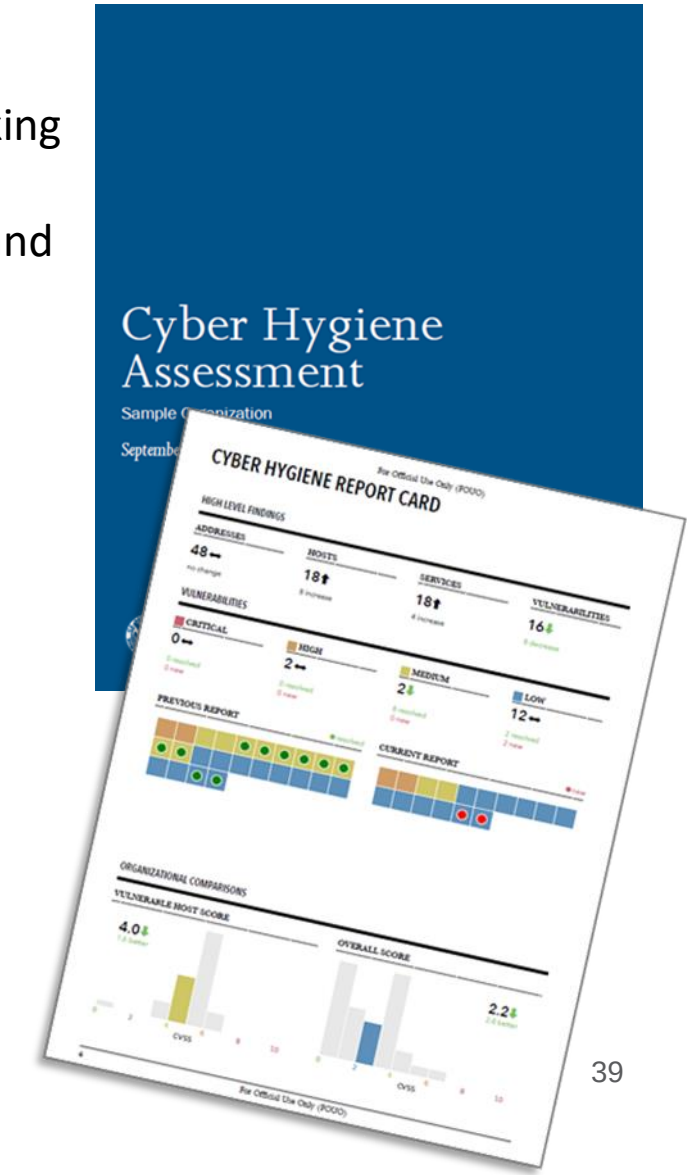
This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards.

Scanning Objectives:

- Maintain enterprise awareness of your publicly accessible web-based assets
- Provide insight into how systems and infrastructure appear to potential attackers
- Drive proactive mitigation of vulnerabilities to help reduce overall risk

Scanning Phases

- Discovery Scanning: identify active, internet-facing web applications
- Vulnerability Scanning: Initiate non-intrusive checks to identify potential vulnerabilities and configuration weaknesses



Known Exploited Vulnerabilities Catalog

Show 10 entries

Search:

CVE	Vendor/Project	Product	Vulnerability Name	Date Added to Catalog	Short Description	Action	Due Date	Notes
CVE-2022-0847	Linux	Kernel	Linux Kernel Privilege Escalation Vulnerability	2022-04-25	Linux kernel contains an improper initialization vulnerability where an unprivileged local user could escalate their privileges on the system. This vulnerability has the moniker of "Dirty Pipe."	Apply updates per vendor instructions.	2022-05-16	
CVE-2021-41357	Microsoft	Win32k	Microsoft Win32k Privilege Escalation Vulnerability	2022-04-25	Microsoft Win32k contains an unspecified vulnerability that allows for privilege escalation.	Apply updates per vendor instructions.	2022-05-16	
CVE-2021-40450	Microsoft	Win32k	Microsoft Win32k Privilege Escalation Vulnerability	2022-04-25	Microsoft Win32k contains an unspecified vulnerability that allows for privilege escalation.	Apply updates per vendor instructions.	2022-05-16	
CVE-2019-1003029	Jenkins	Script Security Plugin	Jenkins Script Security Plugin Sandbox Bypass Vulnerability	2022-04-25	Jenkins Script Security Plugin contains a protection mechanism failure, allowing an attacker to bypass the sandbox.	Apply updates per vendor instructions.	2022-05-16	

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

Cyber Exercise & Planning Program

CISA provides end-to-end exercise planning and conduct support, including planning meetings, document and scenario development, facilitation, and after-action report development.

CISA offers the following services at no-cost on an as-needed and as-available basis:

- Cyber Storm Exercise (CISA's flagship national level cyber exercise)
- End-to-End Cyber Exercise Planning
- Cyber Exercise Consulting
- Cyber Planning Support
- Exercise-In-A-Box
- Virtual CTTX

Situational Awareness & Information Sharing Resources

Cybersecurity Alerts & Advisories

Filters

What are you looking for?

Sort by (optional)

Release Date

APPLY

Advisory Type —

- Alert
- Analysis Report
- Cybersecurity Advisory
- ICS Advisory
- ICS Medical Advisory

Release Year +

MAR 01, 2023 ■ ALERT

CISA Releases Decider Tool to Help with MITRE ATT&CK Mapping

FEB 28, 2023 ■ ICS ADVISORY | ICSA-23-059-01

Hitachi Energy Gateway Station

FEB 28, 2023 ■ ICS ADVISORY | ICSA-23-059-02

Hitachi Energy Gateway Station

FEB 28, 2023 ■ ICS ADVISORY | ICSA-22-139-01

Mitsubishi Electric MELSEC iQ-F Series (Update B)

FEB 28, 2023 ■ ALERT

CISA Releases Three Industrial Control Systems Advisories

FEB 28, 2023 ■ ALERT

CISA Red Team Shares Key Findings to Improve Monitoring and Hardening of Networks

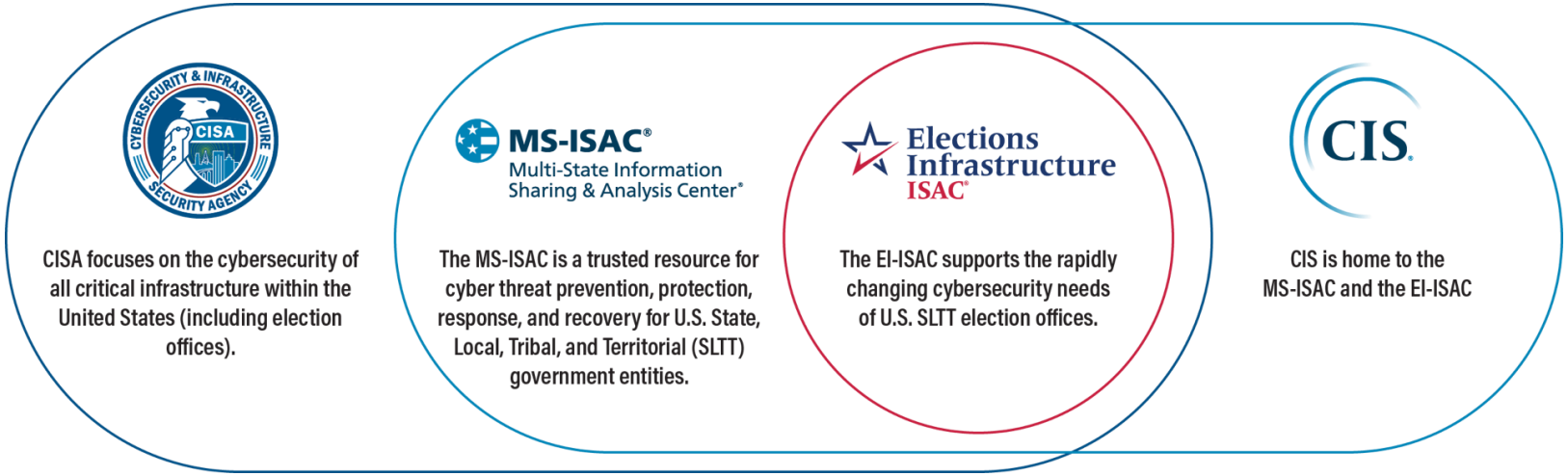
https://www.cisa.gov/news-events

Automated Indicator Sharing (AIS)

- **Automated Indicator Sharing (AIS)**: Rapid and wide sharing of machine-readable cyber threat indicators and defensive measures at machine-speed for network defense purposes
- AIS is about volume and velocity of sharing indicators, ***not*** human validation.

Link: [Automated Indicator Sharing (AIS) | CISA]

Muti-State Information Sharing and Analysis Center (MS-ISAC)



- The MS-ISAC is designated by the U.S. Department of Homeland Security as the focal point for cyber threat prevention, protection, response and recovery for the nation's state, local, tribal and territorial (SLTT) governments including chief information security officers, homeland security advisors and fusion centers.
- Includes representatives from all 50 states, U.S. territories, hundreds of local governments (including all 50 state capital cities), and tribal governments.
- Operates a 24-hour Integrated Intelligence Center that provides real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification and mitigation and incident response for the nation's SLTT governments.

Cybersecurity Education and Training Resources

Federal Virtual Training Environment (FedVTE)

Cyber professionals can continue to improve their skills through hands-on training opportunities.

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

Example Content:

- Cloud Computing Security
- Cloud Security - What Leaders Need to Know
- Cryptocurrency for Law Enforcement for the Public
- Cyber Supply Chain Risk Management for the Public
- Cyber-essentials
- Understanding DNS Attack
- Understanding Web and Email Server Security
- Don’t Wake Up to a Ransomware Attack
- Foundations of Cybersecurity for Managers
- Fundamentals of Cyber Risk Management
- Introduction to Cyber Intelligence
- Securing Internet-Accessible Systems
- 101 Coding for the Public
- 101 Reverse Engineering for the Public

https://fedvte.usalearning.gov

ICS Training Opportunities

ICS-CERT Virtual Learning Portal (VLP)

- Virtual & Instructor Led Training; No Cost

Courses:

- Introduction to Control Systems Cybersecurity (101) - 8 hrs
- Intermediate Cybersecurity for Industrial Control Systems (201) - 8 hrs
- Intermediate Cybersecurity for Industrial Control Systems (202) - 8 hrs
- ICS Cybersecurity (301V) - 12 hrs
- ICS Cybersecurity (301L) - 5 days
- ICS Cybersecurity (401) - 5 days

https://ics-training.inl.gov/learn/signin

IMR Training Series

The Identify, Mitigate, and Recover (IMR) incident response curriculum provides a range of training offerings encompassing cybersecurity awareness and best practices for organizations, live red/blue team network defense demonstrations emulating real-time incident response scenarios, and hands-on cyber range training courses for incident response practitioners.

Topics for Awareness Webinars & Cyber Range Training:

- Ransomware
- Cloud Security
- Business Email Compromise
- Vulnerabilities of Internet-Accessible Systems
- Web and Email Server Attacks
- DNS Infrastructure Attacks
- High Value Assets/Critical Assets
- Indicators of Compromise
- Incident Analysis with tool demo
- Investigating logs for incidents

Topics for Cyber Range Challenges & Observe the Attack Series:

- Ransomware
- Cloud Security
- Business Email Compromise

For more info: education@cisa.dhs.gov
Or visit: https://www.cisa.gov/incident-response-training

Cybersecurity Incident Reporting

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.

Incident Response Activities

Incident Triage: Process taken to scope the severity of an incident and determine required resources for action

Network Topology Review: Assessment of network ingress, egress, remote access, segmentation, and interconnectivity, with resulting recommendations for security enhancements

Infrastructure Configuration Review: Analysis of core devices on the network which are or can be used for network security (e.g., prevention, monitoring, or enforcement functions)

Log Analysis: Examination of logs from network and security devices to illuminate possible malicious activity

Incident Specific Risk Overview: Materials and in-person briefings for technical, program manager, or senior leadership audience; cover current cyber risk landscape, including classified briefings to cleared staff when appropriate

Hunt Analysis: Deployment of network hunting tools to proactively detect indicators of compromise (IOC)

Security Program Review: A review of the client's existing security roles, responsibilities, and policies to identify possible organizational or information-sharing gaps

Malware Analysis: Reverse engineering of malware artifacts to determine functionality and build indicators

Mitigation: Actionable guidance to improve the organization's security posture, including incident-specific recommendations, security best practices, and recommended tactical measures

Digital Media Analysis: Technical forensic examination of digital artifacts to detect malicious activity and develop further indicators

Control Systems Incident Analysis: Analysis of supervisory control and data acquisition devices, process control, distributed control, and any other systems that control, monitor, and manage critical infrastructure

Phishing and Incident Reporting / Malware Analysis

24x7 contact number: 888-282-0870 | central@cisa.dhs.gov

Where/How/When to Report Incidents: https://www.cisa.gov/forms/report

If there is a suspected or confirmed cyber attack or incident that affects core government or critical infrastructure functions and/or results in the loss of data, system availability or control of systems.

Report Phishing to: phishing-report@us-cert.gov

CISA partners with the Anti-Phishing Working Group (APWG) to collect phishing email messages and website locations to help people avoid becoming victims of phishing scams.

Advanced Malware Analysis Center: https://malware.us-cert.gov

Provides 24x7 dynamic analyses of malicious code. Stakeholders submit samples via an online website and receive a technical document outlining the results of the analysis. Experts will detail recommendations for malware removal and recovery activities.

Next Steps

Forming a Partnership with CISA on Cybersecurity Matters

CISA's No-Cost Cybersecurity Resources

CISA's Cybersecurity State Coordinators & Cybersecurity Advisors (CSAs)

- **Cybersecurity Assessments**
  - Baseline Assessments
    - Ransomware Readiness Assessment (RRA)
    - Cybersecurity Performance Goals (CPG)
  - Intermediate Assessments
    - Cyber Infrastructure Survey (CIS)
    - Cyber Resilience Essentials (CRE)
  - Advanced Assessments
    - External Dependencies Management (EDM)
    - Incident Management Review (IMR)
    - Cyber Resilience Review (CRR)
- **Cyber Hygiene Services**
  - External Vulnerability Scanning Service
  - Web Application Scanning Service
- **Workshops & Exercises**
  - Asset Management Workshop (AMW)
  - Cyber Resilience Workshop (CRW)
  - Incident Management Workshop (IMW)
  - Vulnerability Management Workshop (VMW)
  - Digital Forensics Workshop I (DFW I)
  - Digital Forensics Workshop II (DFW II)
  - Cyber Tabletop Exercise (CTTX)
- **Technical Assessments***
  - Remote Penetration Test (RPT)
  - Risk and Vulnerability Assessment (RVA)
  - Validated Architecture Design Review (VADR)

***Note:** Eligibility for technical assessments is contingent upon assessment of the stakeholder's capabilities by their Cybersecurity Advisor (CSA).

Cybersecurity State Coordinator (TX): ernesto.ballesteros@cisa.dhs.gov

CISA's No-Cost Cybersecurity Resources

CISA's Cybersecurity State Coordinators & Cybersecurity Advisors (CSAs)

STRATEGIC (HIGH-LEVEL)

- **Cybersecurity Assessments**
  - Baseline Assessments
    - Ransomware Readiness Assessment (RRA)
    - Cybersecurity Performance Goals (CPG)
  - Intermediate Assessments
    - Cyber Infrastructure Survey (CIS)
    - Cyber Resilience Essentials (CRE)
  - Advanced Assessments
    - External Dependencies Management (EDM)
    - Incident Management Review (IMR)
    - Cyber Resilience Review (CRR)
- **Cyber Hygiene Services**
  - External Vulnerability Scanning Service
  - Web Application Scanning Service

Request CISA's cybersecurity assessments to **identify your "current state" of cyber** and acquire guidance on how to improve.

Contact your CISA Cybersecurity State Coordinator (CSC) or Cybersecurity Advisor (CSA) to schedule these.

TECHNICAL (LOW-LEVEL)

Cybersecurity State Coordinator (TX): ernesto.ballesteros@cisa.dhs.gov

CISA's No-Cost Cybersecurity Resources

CISA's Cybersecurity State Coordinators & Cybersecurity Advisors (CSAs)

STRATEGIC (HIGH-LEVEL)

- **Cybersecurity Assessments**
  - Baseline Assessments
    - Ransomware Readiness Assessment (RRA)
    - Cybersecurity Performance Goals (CPG)
  - Intermediate Assessments
    - Cyber Infrastructure Survey (CIS)
    - Cyber Resilience Essentials (CRE)
  - Advanced Assessments
    - External Dependencies Management (EDM)
    - Incident Management Review (IMR)
    - Cyber Resilience Review (CRR)
- **Cyber Hygiene Services**
  - External Vulnerability Scanning Service
  - Web Application Scanning Service

Request CISA's external vulnerability scanning service to continuously **identify and address vulnerabilities on internet-facing assets**!

Contact your CISA Cybersecurity State Coordinator or Cybersecurity Advisor (CSA) to get signed up!

TECHNICAL (LOW-LEVEL)

Cybersecurity State Coordinator (TX): ernesto.ballesteros@cisa.dhs.gov

CISA's No-Cost Cybersecurity Resources

CISA's Cybersecurity State Coordinators & Cybersecurity Advisors (CSAs)

- Build new or mature existing cyber capabilities with our workshops.

  Exercise your incident response, business continuity, and disaster recovery plans with our Cyber Tabletop Exercise.

  Contact your CISA Cybersecurity State Coordinator (CSC) or Cybersecurity Advisor (CSA) to schedule these.

- **Workshops & Exercises**
  - Asset Management Workshop (AMW)
  - Cyber Resilience Workshop (CRW)
  - Incident Management Workshop (IMW)
  - Vulnerability Management Workshop (VMW)
  - Digital Forensics Workshop I (DFW I)
  - Digital Forensics Workshop II (DFW II)
  - Cyber Tabletop Exercise

Cybersecurity State Coordinator (TX): ernesto.ballesteros@cisa.dhs.gov

CISA's No-Cost Cybersecurity Resources

CISA's Cybersecurity State Coordinators & Cybersecurity Advisors (CSAs)

- **Cybersecurity Assessments**
  - Baseline Assessments
    - Ransomware Readiness Assessment (RRA)
    - Cybersecurity Performance Goals (CPG)
  - Intermediate Assessments
    - Cyber Infrastructure Survey (CIS)

- **Workshops & Exercises**
  - Asset Management Workshop (AMW)
  - Cyber Resilience Workshop (CRW)
  - Incident Management Workshop (IMW)
  - Vulnerability Management Workshop (VMW)
  - Digital Forensics Workshop I (DFW I)
  - Digital Forensics Workshop II (DFW II)

Work with your CISA Cybersecurity State Coordinator (CSC) or Cybersecurity Advisor (CSA) to eligibility for our technical assessments, including the RPT, RVA, VADR, and more.

- **Technical Assessments***
  - Remote Penetration Test (RPT)
  - Risk and Vulnerability Assessment (RVA)
  - Validated Architecture Design Review (VADR)

***Note:** Eligibility for technical assessments is contingent upon assessment of the stakeholder's capabilities by their Cybersecurity Advisor (CSA).

Cybersecurity State Coordinator (TX): ernesto.ballesteros@cisa.dhs.gov

Next Steps: Partnership Formation

Would you like to know more about CISA's no-cost cyber resources (cyber assessments, workshops, exercises, and more) and partnership opportunities?

Next Steps:

1. Contact your CISA Region 6 Office (CISARegion6@hq.dhs.gov) or your **Cybersecurity State Coordinator**;
2. Request an initial Cyber Protective Visit (CPV) from your Cybersecurity Advisor (CSA) or **Cybersecurity State Coordinator (CSC)**; and
3. Discuss how CISA and your organization can partner on cybersecurity matters.

Cybersecurity State Coordinator (TX): ernesto.ballesteros@cisa.dhs.gov

Additional Resources

- CISA's Shields Ready Webpage
- CISA Shields Up Webpage
- CISA's Cross-Sector Cybersecurity Performance Goals
- CISA Catalog of Free Cybersecurity Services
- CISA Cyber Resource Hub
- CISA's Free Cybersecurity Services and Tools Webpage
- CISA's Top Cyber Actions for Securing Water Systems

https://www.cisa.gov/free-cybersecurity-services-and-tools

Cybersecurity State Coordinator (TX): ernesto.ballesteros@cisa.dhs.gov

CISA REGION 6 | Texas

Ernesto Ballesteros, JD, MS, CISSP, CISA, Security+
Cybersecurity State Coordinator of Texas
Region 6 | State of Texas
Cybersecurity and Infrastructure Security Agency
EMAIL: ernesto.ballesteros@cisa.dhs.gov
CELL: (210) 202-6646

CISA INCIDENT REPORTING SYSTEM

https://www.cisa.gov/forms/report

CISA CENTRAL - 24/7 Watch

(888) 282-0870;Central@cisa.dhs.gov

FBI's 24/7 Cyber Watch (CyWatch)

(855) 292-3937; CyWatch@fbi.gov

MS-ISAC/EI-ISAC's SOC

(866) 787-4722; soc@cisecurity.org