CISA CYBERSECURITY MISSION AND RESOURCE BRIEF

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

Cyber Protective Visit: Agenda

- About CISA
- Cybersecurity Resources & Services
  - Cybersecurity State Coordinator and Cybersecurity Advisors
  - Cybersecurity Assessments, Exercises, and Workshops
- Cybersecurity Information Sharing
- Cybersecurity Education and Training
- Incident Reporting
- Next Steps: Establishing a Cybersecurity Partnership with CISA

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

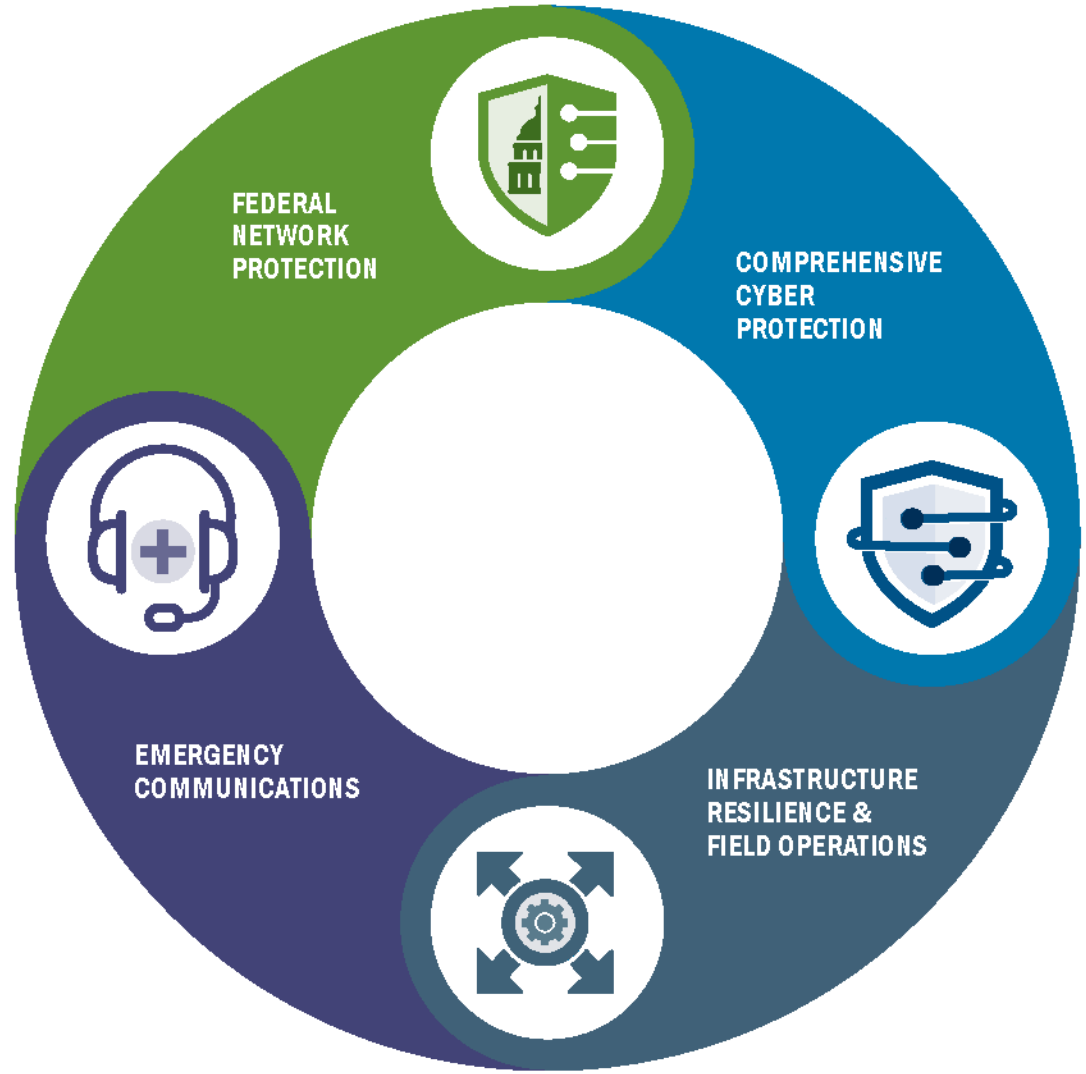
Strengthen critical infrastructure and address long-term risks

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

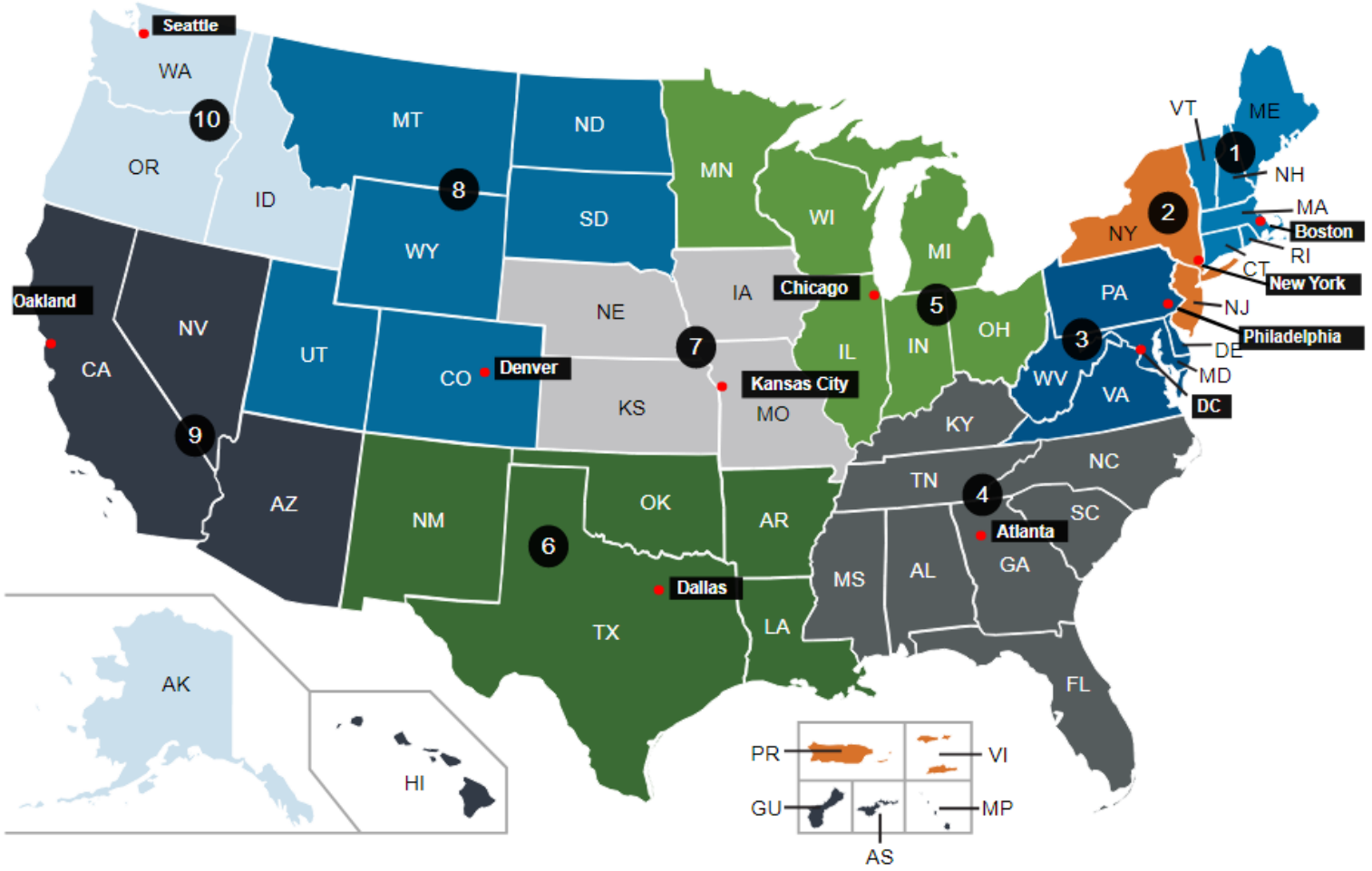


Critical Infrastructure Sectors

CISA assists the public and private sectors to secure their networks and focuses on organizations in the following 16 critical infrastructure sectors.

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)

State Cybersecurity Coordinator

The role of the State Cybersecurity Coordinator is to build strategic public and private sector relationships in Texas to facilitate the development and maintenance of secure and resilient infrastructure, pursuant to 6 United States Code, Section 665(c) (2021).

- Build strategic public and private sector relationships;
- Serve as the Federal cybersecurity risk advisor;
- Facilitate the sharing of cyber threat information;
- Raise awareness of cyber resources from the Federal Government to non-Federal entities;
- Support training, exercises, and planning for continuity of operations from cyber incidents;
- Serve as a principal point of contact for non-Federal entities to engage the Federal Government on preparing, managing, and responding to cyber incidents;
- Assist State, local, Tribal, and territorial governments in development of State cyber plans;
- Coordinate with appropriate officials within the Agency (CISA).

Cybersecurity Advisors (CSAs)

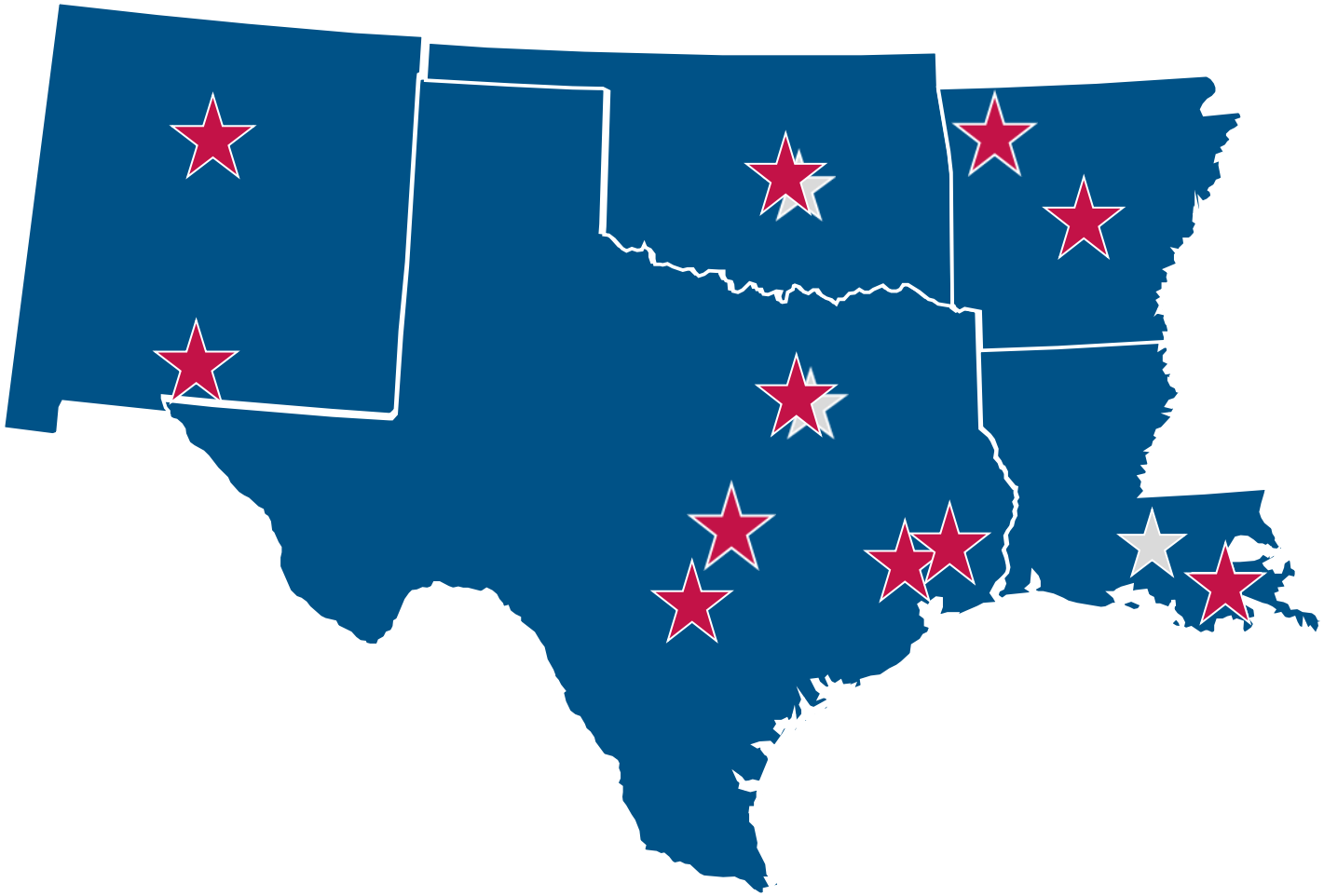
To provide direct coordination, outreach, and regional support in order to protect cyber components essential to the sustainability, preparedness, and protection of the Nation's Critical Infrastructure and Key Resources (CIKR) and State, Local, Tribal, and Territorial (SLTT) governments.

- **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.

On-Hand / Projected Cyber Personnel

On-Hand

Projected



Cybersecurity Resources and Services

CISA Cybersecurity Resources Snapshot

Regional Cybersecurity Resources:

- Cybersecurity Assessments (*Performed by Cybersecurity Advisors*)
  - Introductory Level:
    - Ransomware Readiness Assessment (RRA)
    - Cybersecurity Performance Goals Assessment (CPG)
  - Intermediate Level:
    - Cyber Infrastructure Survey (CIS)
  - Advanced Level:
    - Cyber Resilience Review (CRR)
    - External Dependencies Management (EDM)
    - Incident Management Review (IMR)
- Cybersecurity Exercises and Workshops (*Performed by Cybersecurity Advisors*)
  - Cyber Resilience Workshop (CRW)
  - Incident Management Workshop (IMW)
  - Vulnerability Management Workshop (VMW)
  - Intro to Digital Forensics Workshop (DFW)
  - Facilitated Cyber Exercise (FCE)

National/Automated Cybersecurity Resources:

- Vulnerability Scanning Service (CyHy)

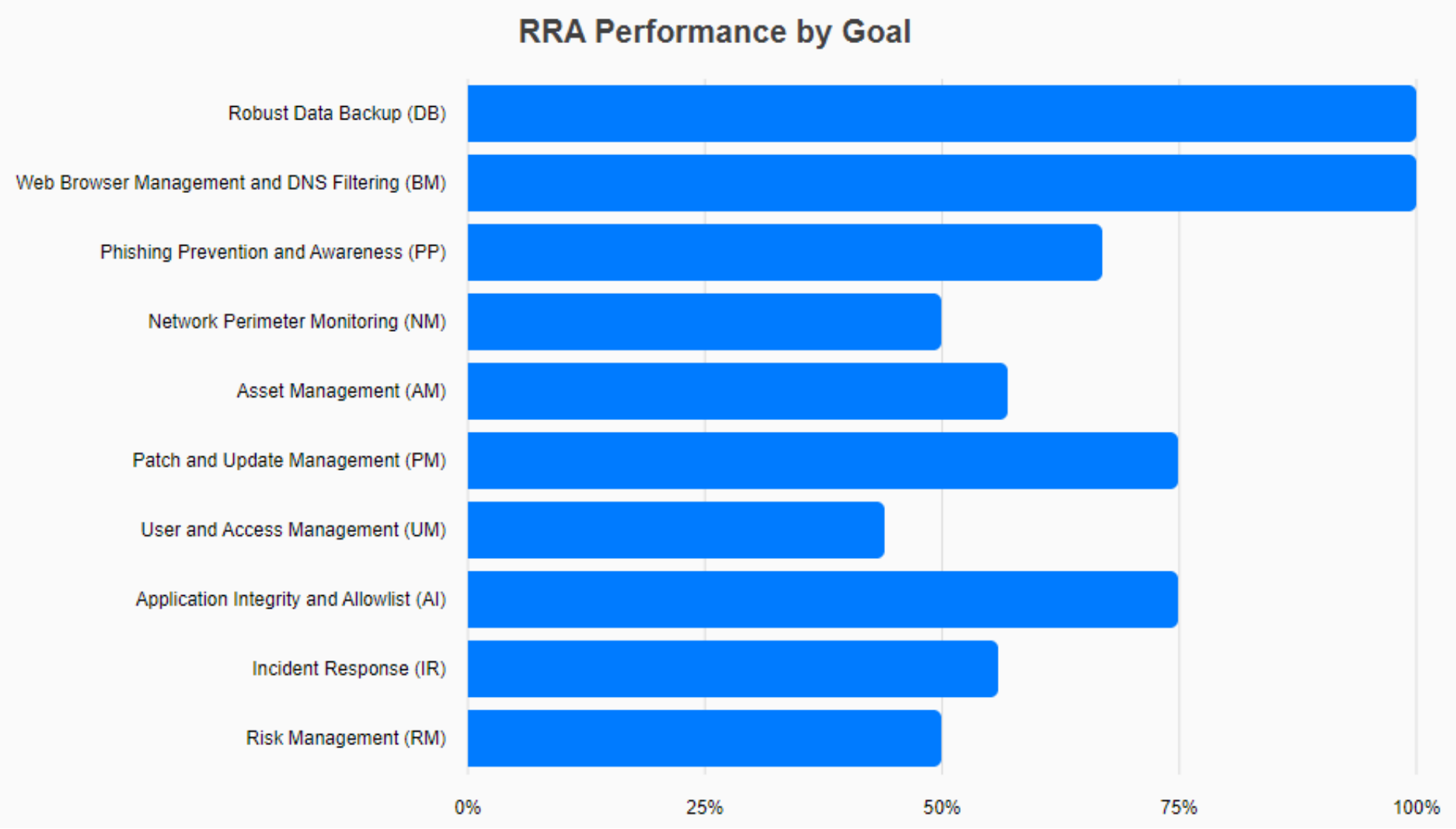
Cybersecurity Assessments

CSET Ransomware Readiness Assessment (RRA)

- **Purpose**: The RRA is an interview-based assessment on a tiered set of practices to help organizations better assess how well they are equipped to defend and recover from a ransomware incident.
- **Time to Complete**: ~2 hours
- **Delivery**: Facilitated by a CISA Cybersecurity Advisor (CSA)
- **Benefits**:
  - Helps organizations evaluate their cybersecurity posture against recognized standards and best practice.
  - 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.

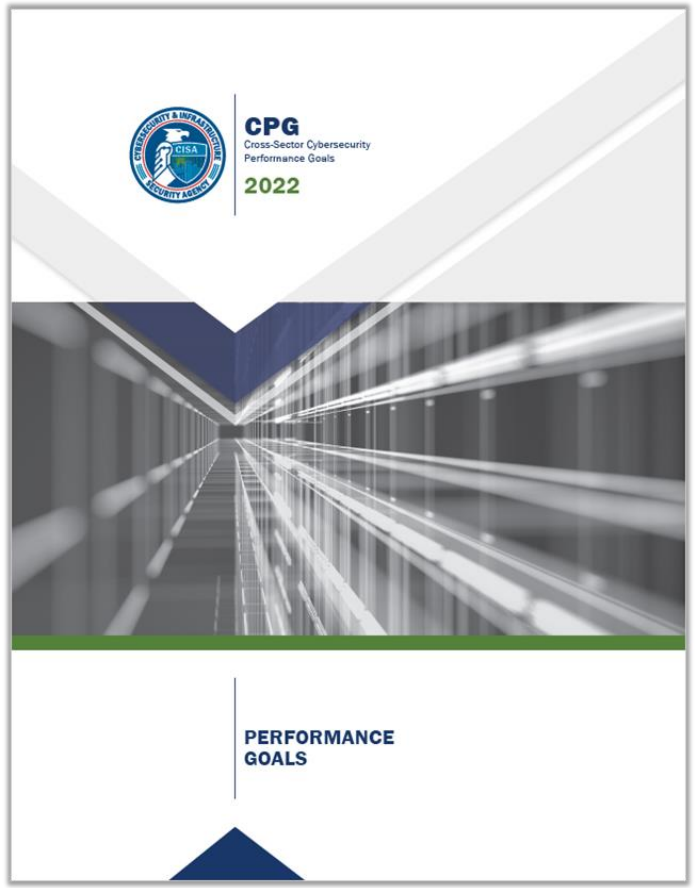
https://github.com/cisagov/cset/releases/

Goal Completion Summary Example

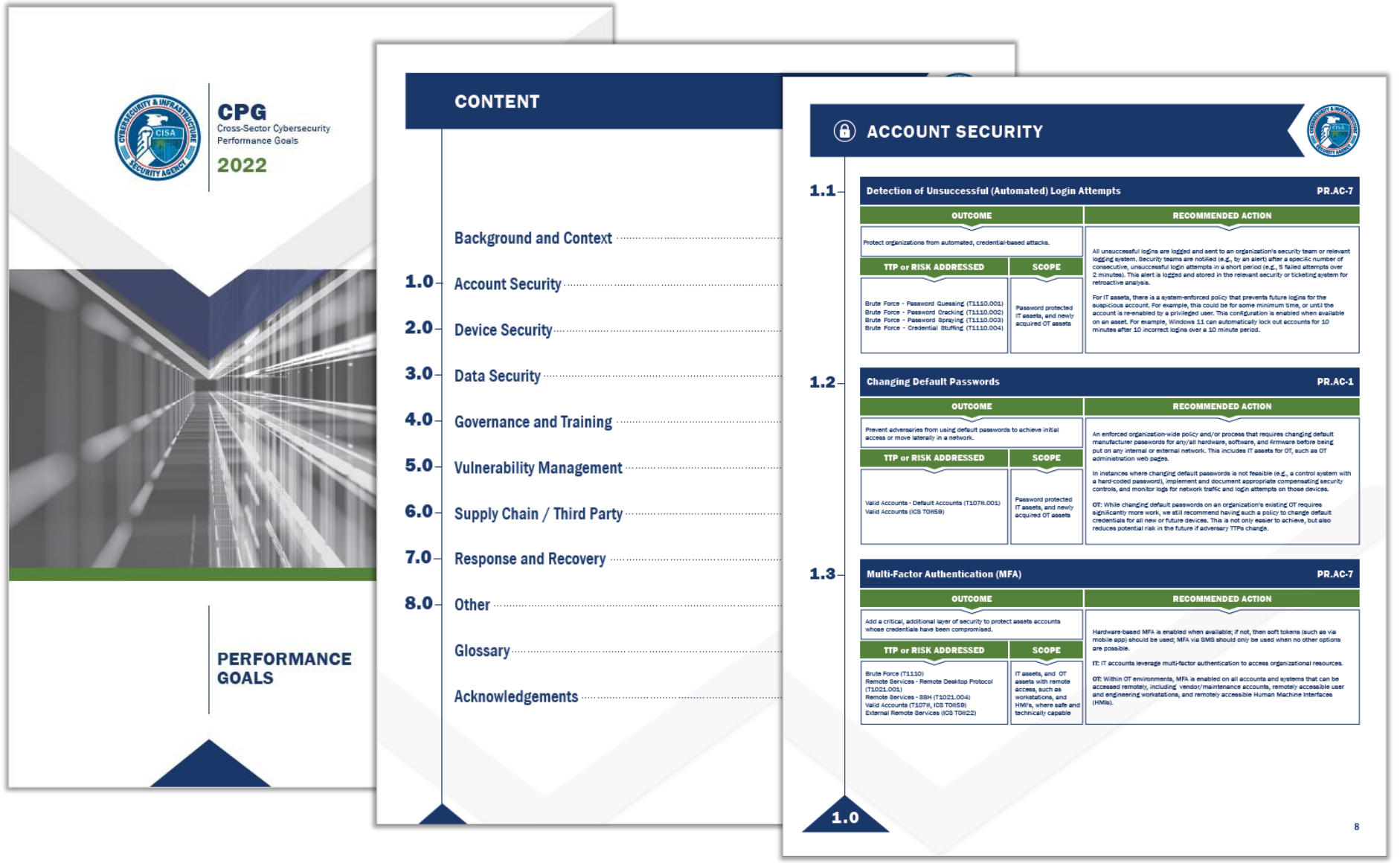


Cyber Performance Goals (CPG) Assessment

- **Purpose**: The CPG is an interview-based assessment of essential cybersecurity practices that critical infrastructure owners and operators can implement to meaningfully reduce the likelihood and impact of known risks and adversary techniques.
- **Time to Complete**: ~1-2 hours
- **Delivery**: Facilitated by a CISA Cybersecurity Advisor (CSA)
- **Benefits**:
  - An inventory of practices and goals that owners and operators can implement to reduce risk to their organization's critical infrastructure operations.

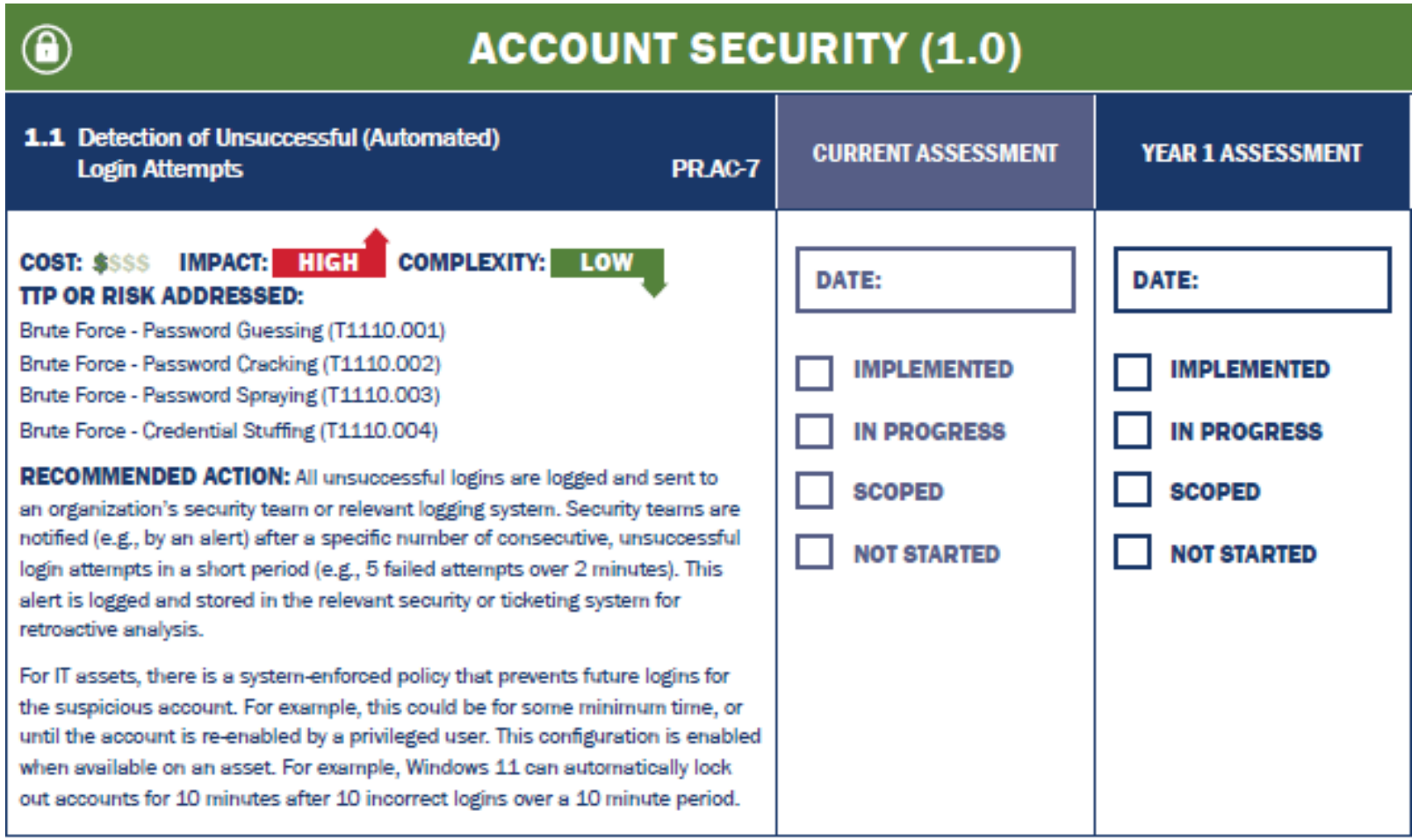


CPG Guide


CPG
Cross-Sector Cybersecurity Performance Goals
2022
PERFORMANCE GOALS
CONTENT
Background and Context
1.0 Account Security
2.0 Device Security
3.0 Data Security
4.0 Governance and Training
5.0 Vulnerability Management
6.0 Supply Chain / Third Party
7.0 Response and Recovery
8.0 Other
Glossary
Acknowledgements
ACCOUNT SECURITY
1.1 Detection of Unsuccessful (Automated) Login Attempts PR.AC-7
OUTCOME
Protect organizations from automated, credential-based attacks.
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.
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)
SCOPE
Password protected IT assets, and newly acquired OT assets
1.2 Changing Default Passwords PR.AC-1
OUTCOME
Prevent adversaries from using default passwords to achieve initial access or move laterally in a network.
RECOMMENDED ACTION
An enforced organization-wide policy and/or process that requires changing default manufacturer passwords for any/all hardware, software, and firmware before being put on any internal or external network. This includes IT assets for OT, such as OT administration web pages.
In instances where changing default passwords is not feasible (e.g., a control system with a hard-coded password), implement and document appropriate compensating security controls, and monitor logs for network traffic and login attempts on those devices.
OT: While changing default passwords on an organization's existing OT requires significantly more work, we still recommend having such a policy to change default credentials for all new or future devices. This is not only easier to achieve, but also reduces potential risk in the future if adversary TTPs change.
TTP or RISK ADDRESSED
Valid Accounts - Default Accounts (T1078.001)
Valid Accounts (ICS T0859)
SCOPE
Password protected IT assets, and newly acquired OT assets
1.3 Multi-Factor Authentication (MFA) PR.AC-7
OUTCOME
Add a critical, additional layer of security to protect assets accounts whose credentials have been compromised.
RECOMMENDED ACTION
Hardware-based MFA is enabled when available; if not, then soft tokens (such as via mobile app) should be used; MFA via SMS should only be used when no other options are possible.
IT: IT accounts leverage multi-factor authentication to access organizational resources.
OT: Within OT environments, MFA is enabled on all accounts and systems that can be accessed remotely, including vendor/maintenance accounts, remotely accessible user and engineering workstations, and remotely accessible Human Machine Interfaces (HMIs).
TTP or RISK ADDRESSED
Brute Force (T1110)
Remote Services - Remote Desktop Protocol (T1021.001)
Remote Services - SSH (T1021.004)
Valid Accounts (T1078, ICS T0859)
External Remote Services (ICS T0822)
SCOPE
IT assets, and OT assets with remote access, such as workstations, and HMIs, where safe and technically capable
1.0
8

Example CPG Question

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

Cybersecurity Infrastructure Survey (CIS)

- **Purpose**: The CIS is an interview-based assessment of essential cybersecurity practices in-place for critical services within critical infrastructure organizations.
- **Time to Complete**: ~3-4 hours
- **Delivery**: Facilitated by a CISA Cybersecurity
- **Benefits**:
  - Anonymized comparative data that public and private sector partners can use to understand and measure its ability to manage cybersecurity risk, per domain.
  - An interactive data-rich dashboard, which can be used as an interactive support resource.

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 Security & Communications

Cyber IST Survey

Home | Logout

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

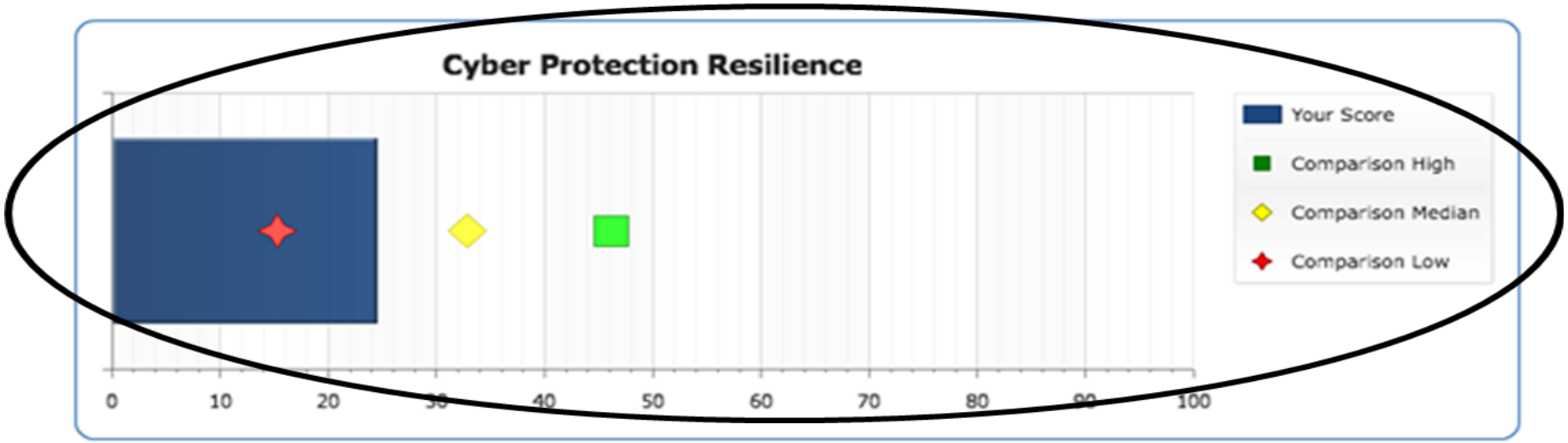
Cyber Protection Resilience Index
- Point Of Contact and Participants
- Critical Service Information
- **Cybersecurity Management**
- Cybersecurity Leadership
- Inventory
- System Architecture
- Security Architecture
- Change Management
- Lifecycle Tracking
- Accreditation and Assessment
- Cybersecurity Plan
- Cybersecurity Exercises
- External Information Sharing

Cyber IST Survey for

Threat Overlay: General

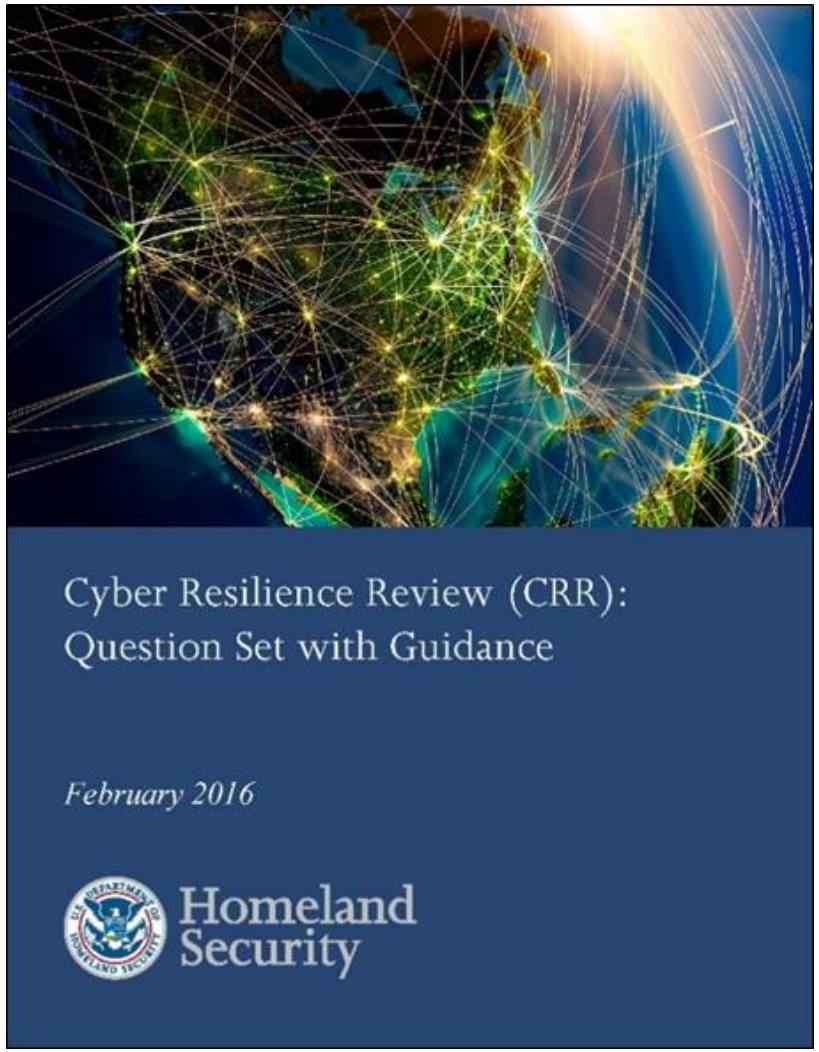
Scenario: General

Cyber Protection Resilience



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
- **Time to Complete**: ~6-8 hours
- **Delivery**: Facilitated by a CISA Cybersecurity Advisor (CSA)
- **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)



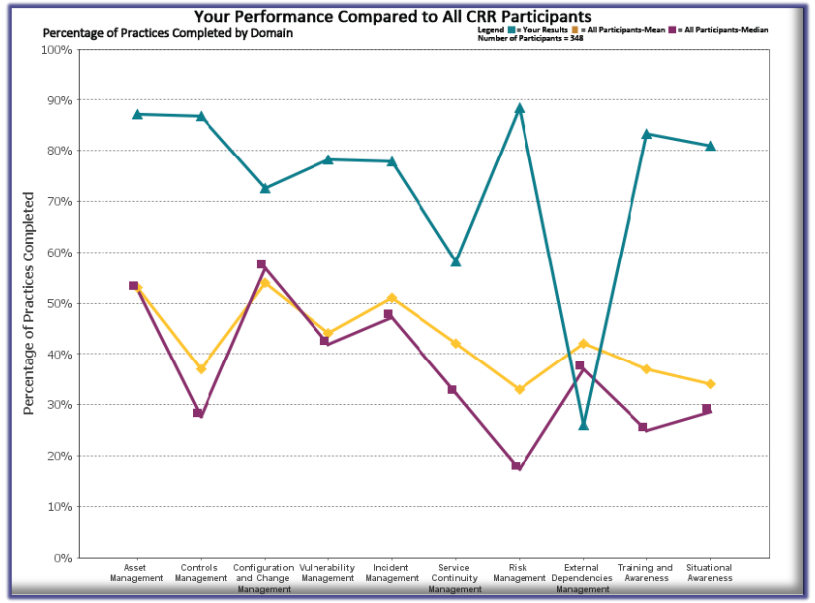
Cyber Resilience Review (CRR) | Domains

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*

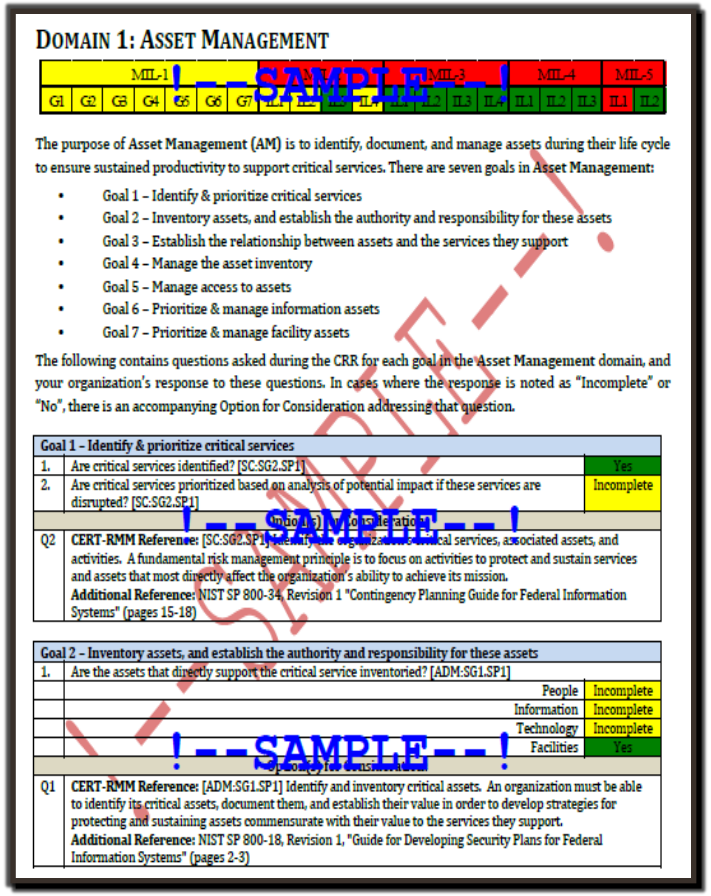
Benefits of CRR



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 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)	

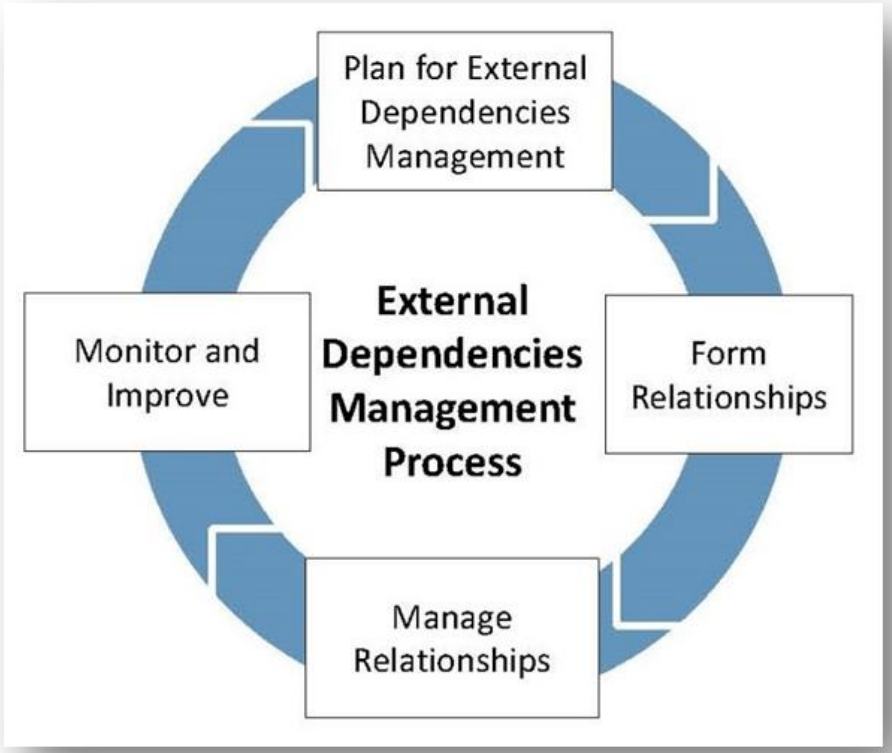
CRR Mappings to Other Frameworks

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 Dependency Management (EDM)



EDM process outlined in the External Dependencies Management Resource Guide

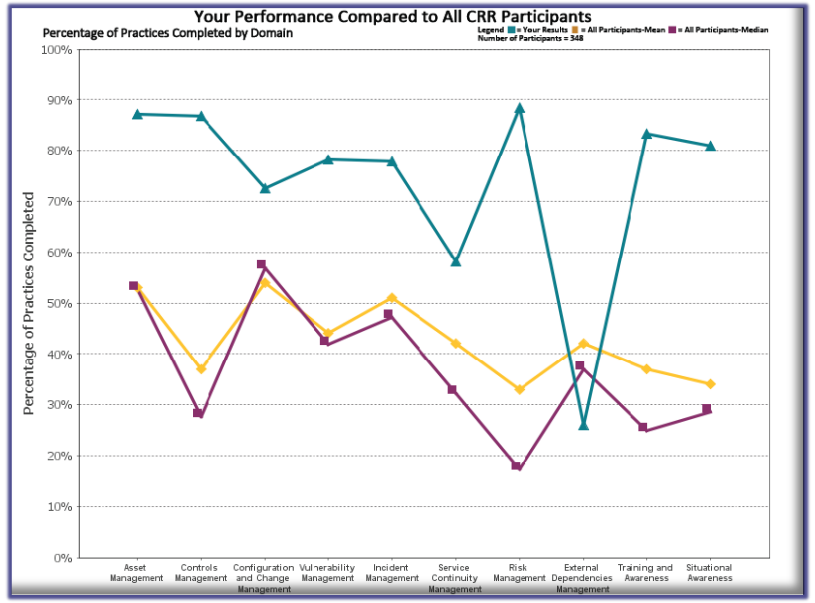
- **Purpose**: The EDM is an interview-based assessment of the management activities and practices utilized to identify, analyze, and reduce risks arising from third parties.
- **Time to Complete**: ~3-4 hours
- **Delivery**: Facilitated by a CISA Cybersecurity Advisor (CSA)
- **Benefits**:
  - The EDM Assessment measures essential external dependency cybersecurity capabilities and behaviors to provide meaningful indicators of an organization's resilience during normal operations and during times of operational stress.
  - Provides comparative data across each domain.

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

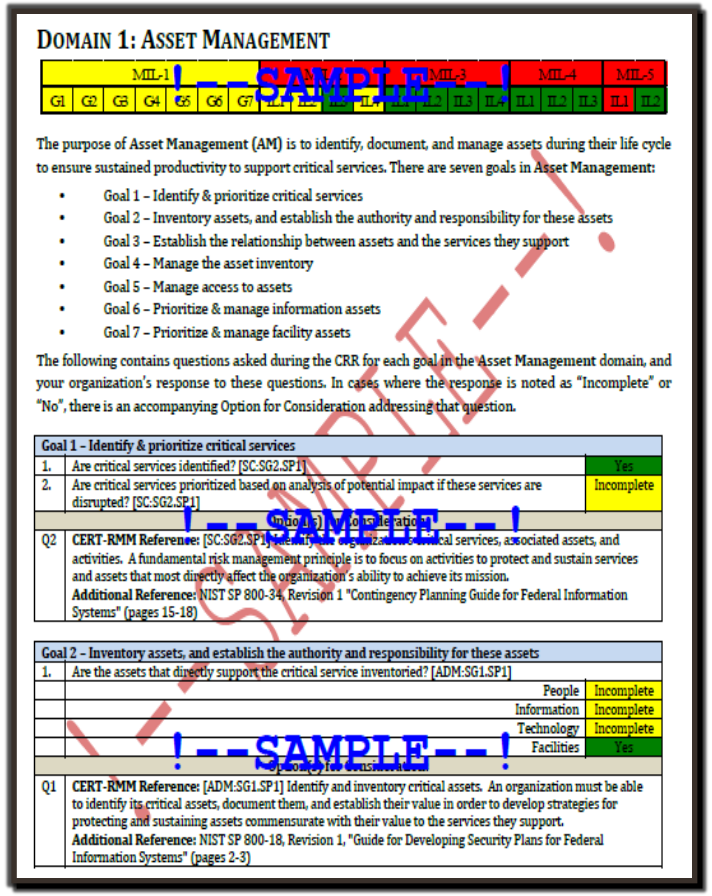
Benefits of EDM



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

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)	

Cybersecurity Workshops & Exercises

Cyber Resilience Workshop (CRW)

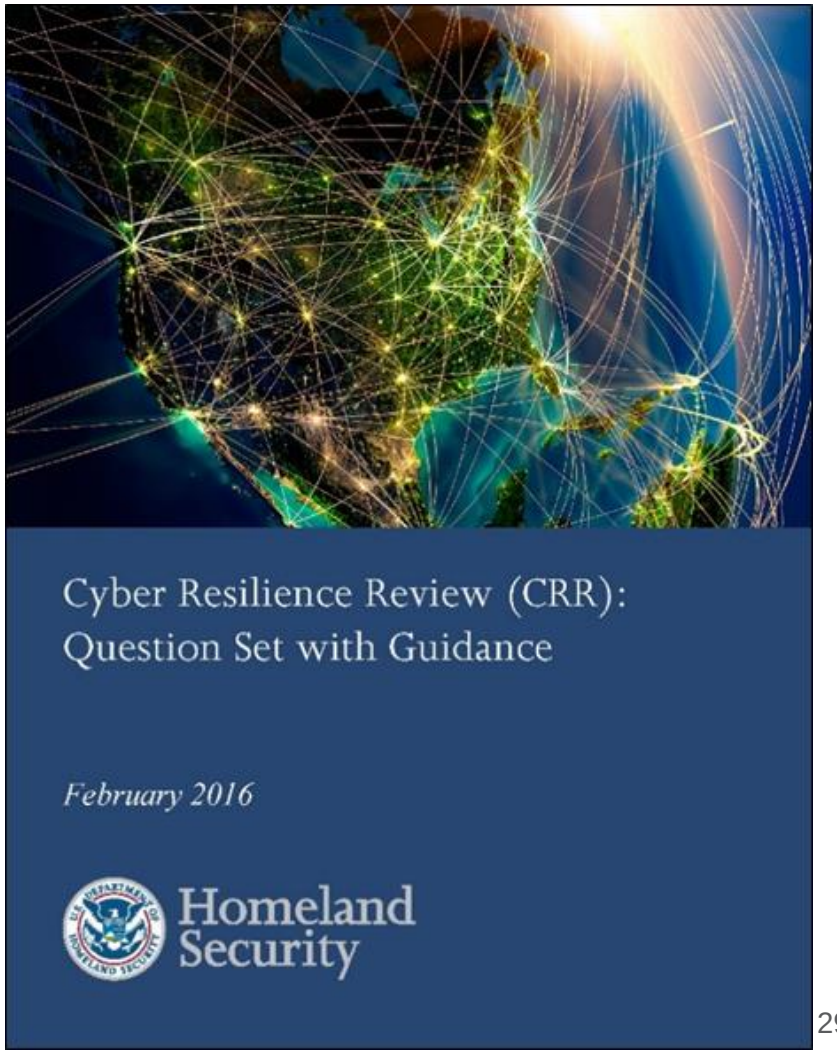
Description: A 2-hour or 4-hour non-technical and informative session designed to help organizations understand cyber resilience concepts and ways to improve management of cyber resilience.

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



Incident Management Workshop (IMW)

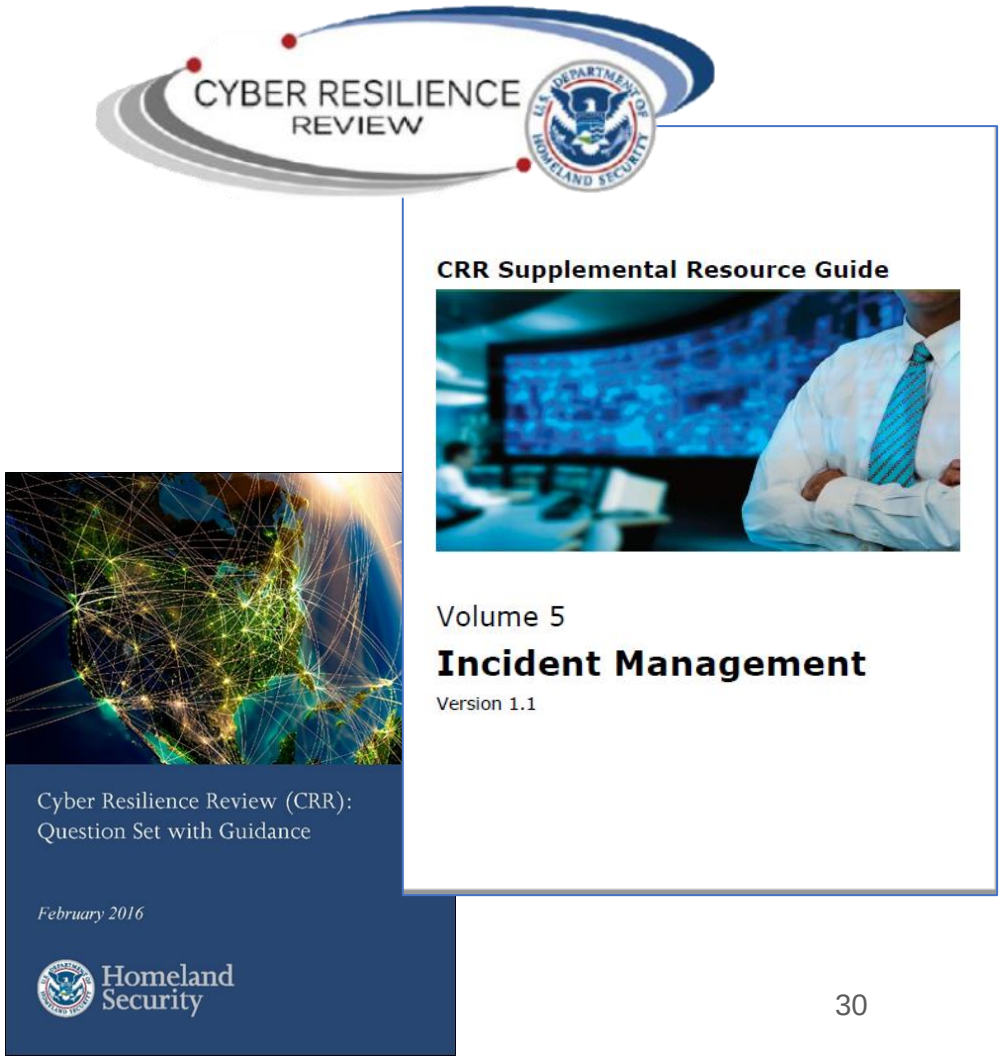
Description: A 2-hour non-technical and informative session designed to help organizations understand incident management concepts, key elements, planning and implementation.

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)

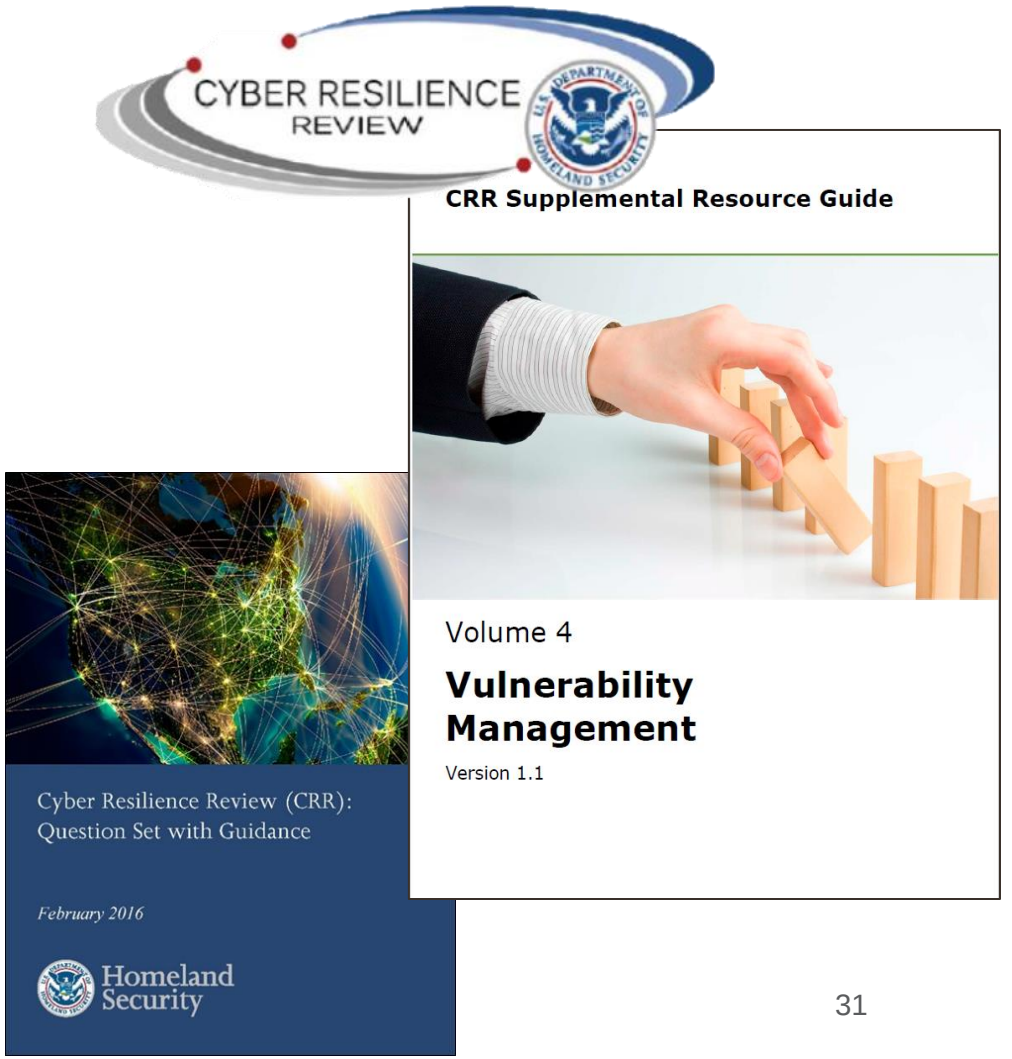
Description: A 2-hour non-technical and informative session designed to help organizations understand vulnerability management concepts, key elements, planning and implementation.

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



Facilitated Cyber Exercise (FCE)

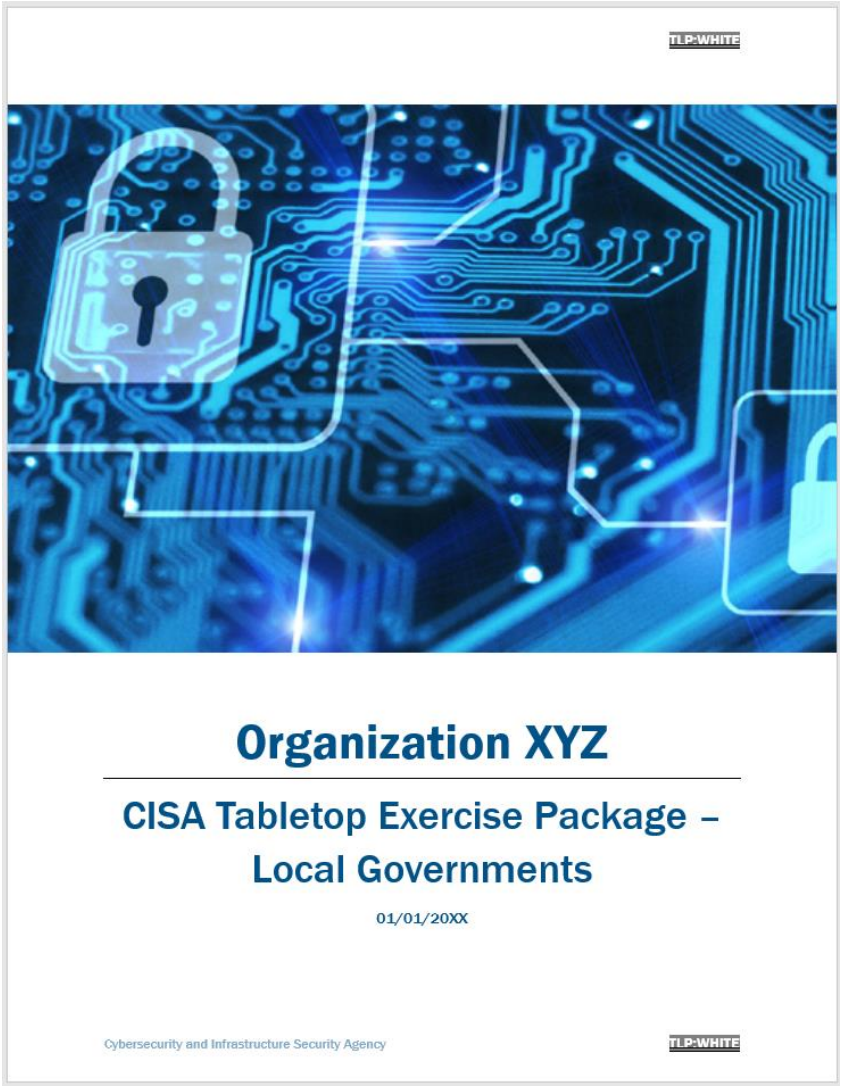
Description: A 2-hour or 4-hour non-technical facilitated cybersecurity tabletop exercise, where organizations are presented with a cyber threat-based scenario and are challenged to consider how their organization would respond, based on existing incident response plans.

Goal: The goal of the workshop 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

Cyber Hygiene Services

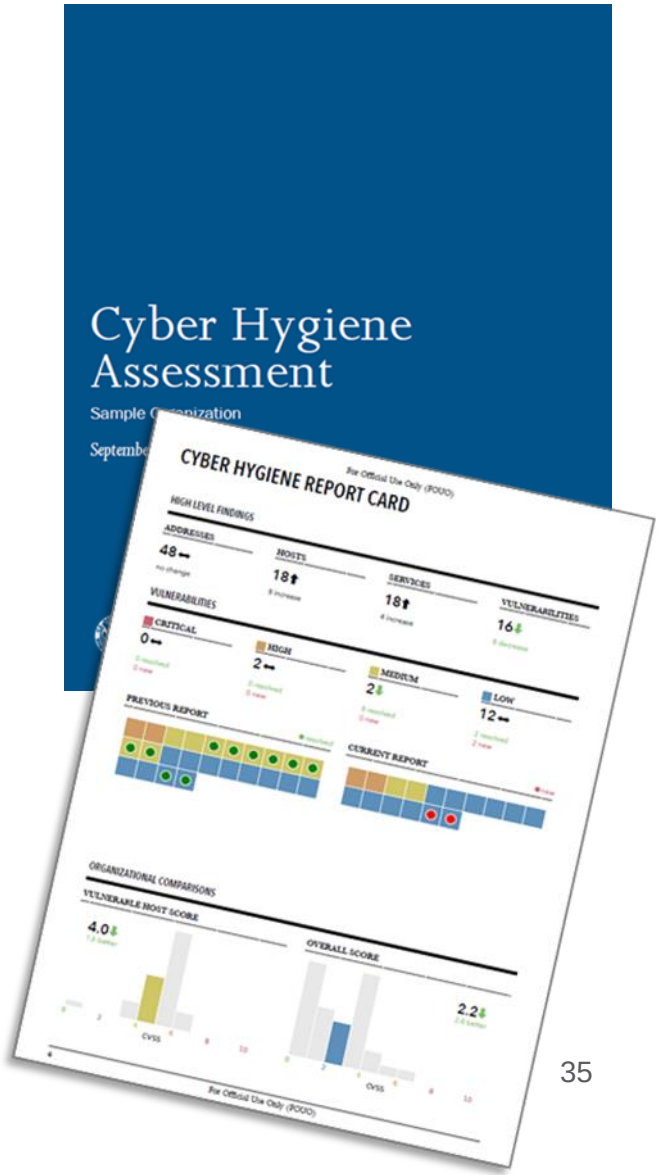
Vulnerability Scanning Service (CyHy)

Assess Internet accessible systems for known vulnerabilities and configuration errors

Work with organization to proactively mitigate threats and risks to systems

Activities include:

- Network Mapping
  - Identify public IP address space
  - Identify hosts that are active on IP address space
  - Determine the O/S and Services running
  - Re-run scans to determine any changes
  - Graphically represent address space on a map
- Network Vulnerability & Configuration Scanning
  - Identify network vulnerabilities and weakness



Contact vulnerability@cisa.dhs.gov to get started.

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

Information Sharing

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.

Contact cyberservices@cisa.dhs.gov for more information.

Multi-State 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 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

Cybersecurity Education & 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

Phishing and Incident Reporting / Malware Analysis

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

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.

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.

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: Cybersecurity Partnership Formation

Next Steps: Cybersecurity Partnership Formation

Would you like to partners with CISA and leverage our no-cost cybersecurity assessments, workshops, education, training, and information sharing resources?

Next Steps:

1. Visit https://www.cisa.gov/cisa-regions;
2. Identify your region (Texas is in Region 6); and
3. Request to speak/meet with your Cybersecurity State Coordinator (CSC) or Cybersecurity Advisor (CSA) to discuss cybersecurity partnership opportunities.

Region 6 Office: CISARegion6@hq.dhs.gov
Cybersecurity State Coordinator of Texas: ernesto.ballesteros@cisa.dhs.gov

48

CISA REGION 6

Ernesto Ballesteros, JD, MS, CISSP, CISA, Security+

Cybersecurity State Coordinator of Texas (Region 6)
Cybersecurity & Infrastructure Security Agency

EMAIL: ernesto.ballesteros@cisa.dhs.gov
CELL: (210) 202-6646

CISA Region 6 Offices
Central@cisa.dhs.gov

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


DEFEND TODAY,
SECURE TOMORROW
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA