

CISA CYBERSECURITY MISSION & RESOURCE BRIEF



Andrew Buschbom
Cybersecurity State Coordinator
Region VI | New Mexico

AGENDA:

- About CISA
- Cybersecurity Resources & Services
- Information Sharing
- Training
- Incident Reporting

About CISA



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 secure its networks and focuses on organizations in the following 16 critical infrastructure sectors.



Cybersecurity Advisors (CSAs)

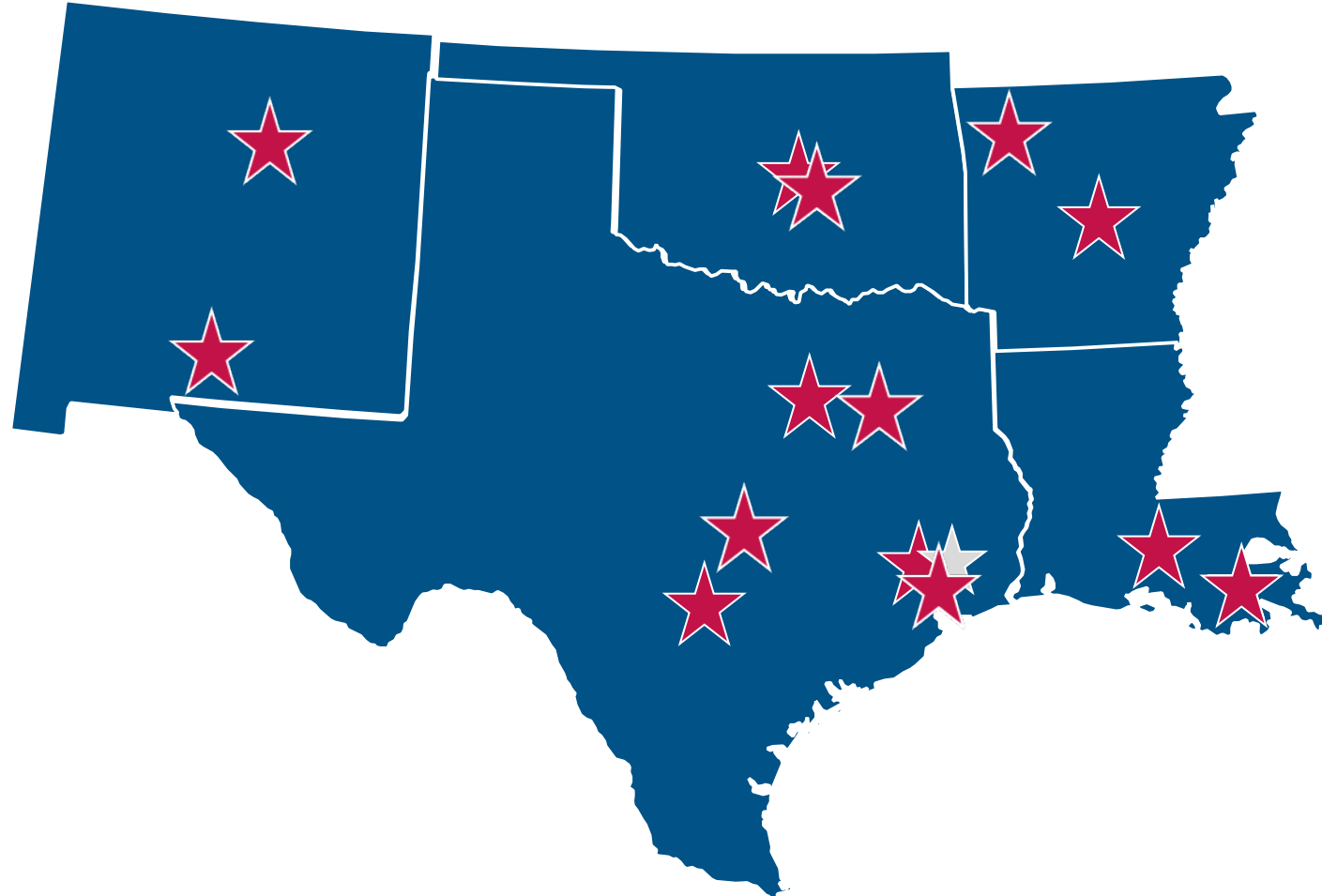
To provide direct coordination, outreach, and regional support in order to protect cyber components essential to the sustainability, preparedness, and protection of the Nation's Critical Infrastructure and Key Resources (CIKR) and State, Local, Tribal, and Territorial (SLTT) governments.

- **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 Resources and Services

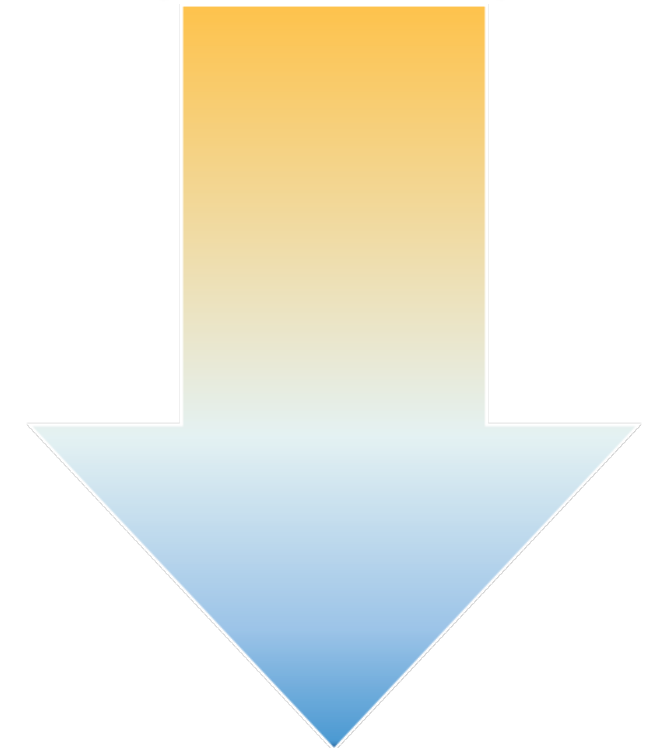


CISA Cybersecurity Resources

No-Cost/Federally-Funded Cybersecurity Resources:

- Cybersecurity Assessments
 - Cybersecurity Performance Goals (CPG)
 - Ransomware Readiness Assessment (RRA)
 - Cyber Infrastructure Survey (CIS)
 - Cyber Resilience Essentials (CRE)
 - External Dependencies Management (EDM)
 - Incident Management Review (IMR)
 - Cyber Resilience Review (CRR)
- Workshops
 - Cyber Resilience Workshop (CRW)
 - Asset Management Workshop (AMW)
 - Incident Management Workshop (IMW)
 - OEM Planning Considerations for Cyber Incidents Workshop (EMW)
 - Vulnerability Management Workshop (VMW)
 - Digital Forensics Workshop I & II (DFW)
 - Cyber Exercise (CYX)
- Cyber Hygiene Services
 - Vulnerability Scanning Service (CyHy)
 - Web Application Scan (WAS)

**STRATEGIC
(HIGH-LEVEL)**



**TECHNICAL
(LOW-LEVEL)**



CISA Cybersecurity Resources

No-Cost/Federally-Funded Cybersecurity Resources:

- Cybersecurity Assessments

Introductory Assessment →

- **Cybersecurity Performance Goals (CPG)**
- **Ransomware Readiness Assessment (RRA)**
- Cyber Infrastructure Survey (CIS)
- Cyber Resilience Essentials (CRE)
- External Dependencies Management (EDM)
- Incident Management Review (IMR)
- Cyber Resilience Review (CRR)

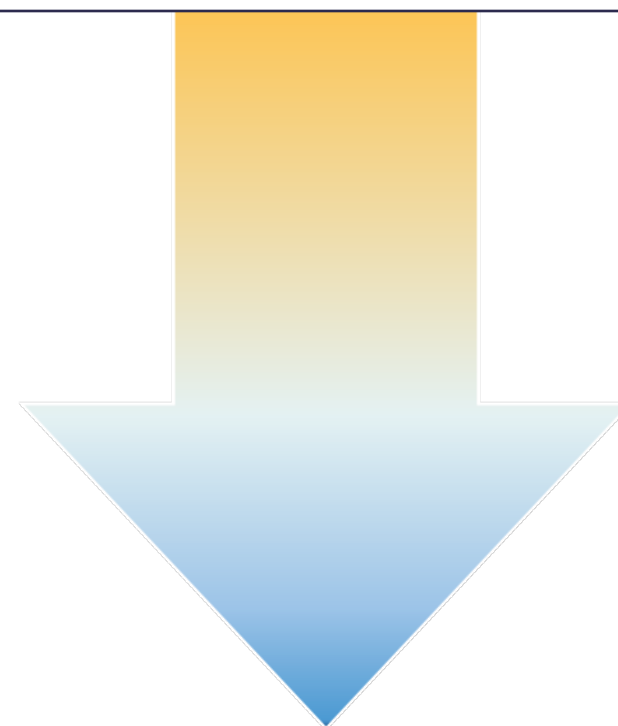
- Workshops

- Cyber Resilience Workshop (CRW)
- Asset Management Workshop (AMW)
- Incident Management Workshop (IMW)
- OEM Planning Considerations for Cyber Incidents Workshop (EMW)
- Vulnerability Management Workshop (VMW)
- Digital Forensics Workshop I & II (DFW)
- Cyber Exercise (CYX)

- Cyber Hygiene Services

- Vulnerability Scanning Service (CyHy)
- Web Application Scan (WAS)

Note: The RRA and CPG are recommended starter assessments.



**TECHNICAL
(LOW-LEVEL)**



CISA Cybersecurity Resources

No-Cost/Federally-Funded Cybersecurity Resources:

- Cybersecurity Assessments
 - Cybersecurity Performance Goals (CPG)
 - Ransomware Readiness Assessment (RRA)
 - **Cyber Infrastructure Survey (CIS)**
 - **Cyber Resilience Essentials (CRE)**
 - **External Dependencies Management (EDM)**
 - **Incident Management Review (IMR)**
 - Cyber Resilience Review (CRR)
- Workshops
 - Cyber Resilience Workshop (CRW)
 - Asset Management Workshop (AMW)
 - Incident Management Workshop (IMW)
 - OEM Planning Considerations for Cyber Incidents Workshop (EMW)
 - Vulnerability Management Workshop (VMW)
 - Digital Forensics Workshop I & II (DFW)
 - Cyber Exercise (CYX)
- Cyber Hygiene Services
 - Vulnerability Scanning Service (CyHy)
 - Web Application Scan (WAS)

Intermediate Assessments



**STRATEGIC
(HIGH-LEVEL)**

Note: The intermediate assessments are more specialized and focused.

**TECHNICAL
(LOW-LEVEL)**



CISA Cybersecurity Resources

No-Cost/Federally-Funded Cybersecurity Resources:

- Cybersecurity Assessments
 - Cybersecurity Performance Goals (CPG)
 - Ransomware Readiness Assessment (RRA)
 - Cyber Infrastructure Survey (CIS)
 - Cyber Resilience Essentials (CRE)
 - External Dependencies Management (EDM)
 - Incident Management Review (IMR)
 - **Cyber Resilience Review (CRR)**
- Workshops
 - Cyber Resilience Workshop (CRW)
 - Asset Management Workshop (AMW)
 - Incident Management Workshop (IMW)
 - OEM Planning Considerations for Cyber Incidents Workshop (EMW)
 - Vulnerability Management Workshop (VMW)
 - Digital Forensics Workshop I & II (DFW)
 - Cyber Exercise (CYX)
- Cyber Hygiene Services
 - Vulnerability Scanning Service (CyHy)
 - Web Application Scan (WAS)

Advanced Assessment →

**STRATEGIC
(HIGH-LEVEL)**

Note: Our most comprehensive assessment that focuses on a variety of aspects of your cybersecurity program.

**TECHNICAL
(LOW-LEVEL)**



CISA Cybersecurity Resources

No-Cost/Federally-Funded Cybersecurity Resources:

- Cybersecurity Assessments
 - Cybersecurity Performance Goals (CPG)
 - Ransomware Readiness Assessment (RRA)
 - Cyber Infrastructure Survey (CIS)
 - Cyber Resilience Essentials (CRE)
 - External Dependencies Management (EDM)
 - Incident Management Review (IMR)
 - Cyber Resilience Review (CRR)
- Workshops
 - Cyber Resilience Workshop (CRW)
 - Asset Management Workshop (AMW)
 - Incident Management Workshop (IMW)
 - OEM Planning Considerations for Cyber Incidents Workshop (EMW)
 - Vulnerability Management Workshop (VMW)
 - Digital Forensics Workshop I & II (DFW)
 - Cyber Exercise (CYX)
- Cyber Hygiene Services
 - Vulnerability Scanning Service (CyHy)
 - Web Application Scan (WAS)

Series of Workshops →

STRATEGIC
(HIGH-LEVEL)



Note: The workshops are great follow-on activities that helps to reinforce gaps in your cybersecurity program.

TECHNICAL
(LOW-LEVEL)



CISA Cybersecurity Resources

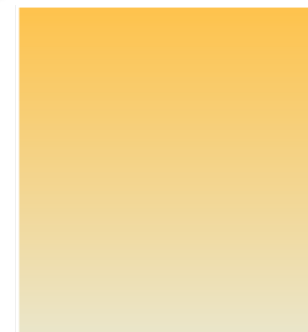
No-Cost/Federally-Funded Cybersecurity Resources:

- Cybersecurity Assessments
 - Cybersecurity Performance Goals (CPG)
 - Ransomware Readiness Assessment (RRA)
 - Cyber Infrastructure Survey (CIS)
 - Cyber Resilience Essentials (CRE)
 - External Dependencies Management (EDM)
 - Incident Management Review (IMR)
 - Cyber Resilience Review (CRR)
- Workshops
 - Cyber Resilience Workshop (CRW)
 - Asset Management Workshop (AMW)
 - Incident Management Workshop (IMW)
 - OEM Planning Considerations for Cyber Incidents Workshop
 - Vulnerability Management Workshop (VMW)
 - Digital Forensics Workshop I & II (DFW)
 - **Cyber Exercise (CYX)**
- Cyber Hygiene Services
 - Vulnerability Scanning Service (CyHy)
 - Web Application Scan (WAS)

Cyber Exercise →



**STRATEGIC
(HIGH-LEVEL)**



Note: Cyber Exercises are recommended opportunities to assess the organization's readiness to respond to and recover from a cybersecurity incident.

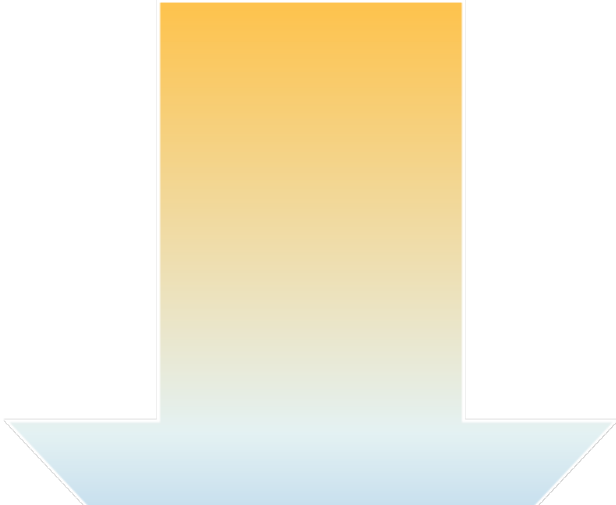
**TECHNICAL
(LOW-LEVEL)**

CISA Cybersecurity Resources

No-Cost/Federally-Funded Cybersecurity Resources:

- Cybersecurity Assessments
 - Cybersecurity Performance Goals (CPG)
 - Ransomware Readiness Assessment (RRA)
 - Cyber Infrastructure Survey (CIS)
 - Cyber Resilience Essentials (CRE)
 - External Dependencies Management (EDM)
 - Incident Management Review (IMR)
 - Cyber Resilience Review (CRR)
- Workshops
 - Cyber Resilience Workshop (CRW)
 - Asset Management Workshop (AMW)
 - Incident Management Workshop (IMW)
 - OEM Planning Considerations for Cyber Incidents Workshop
 - Vulnerability Management Workshop (VMW)
 - Digital Forensics Workshop I & II (DFW)
 - Cyber Exercise (CYX)
- Cyber Hygiene Services
 - **Vulnerability Scanning Service (CyHy)**
 - **Web Application Scan (WAS)**

**STRATEGIC
(HIGH-LEVEL)**



Note: Both the CyHy External Vulnerability Scanning Service and Web Application Scans are recommended to detect vulnerabilities.



CISA Cybersecurity Resources

No-Cost/Federally-Funded Cybersecurity Resources:

- Cybersecurity Assessments
 - Cybersecurity Performance Goals (CPG)
 - Ransomware Readiness Assessment (RRA)
 - Cyber Infrastructure Survey (CIS)
 - Cyber Resilience Essentials (CRE)
 - External Dependencies Management (EDM)
 - Incident Management Review (IMR)
 - Cyber Resilience Review (CRR)
- Workshops
 - Cyber Resilience Workshop (CRW)
 - Asset Management Workshop (AMW)
 - Incident Management Workshop (IMW)
 - OEM Planning Considerations for Cyber Incidents Workshop (EMW)
 - Vulnerability Management Workshop (VMW)
 - Digital Forensics Workshop I & II (DFW)
 - Cyber Exercise (CYX)
- Cyber Hygiene Services
 - Vulnerability Scanning Service (CyHy)
 - Web Application Scan (WAS)

*Technical Assessments

- Remote Penetration Testing
- Risk and Vulnerability Assessment
- Validated Architecture Design Review

***Note:** Eligibility for technical assessments is contingent upon assessment of the stakeholder's capabilities.

**STRATEGIC
(HIGH-LEVEL)**

**TECHNICAL
(LOW-LEVEL)**



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 <small>PR.AC-7</small>	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT
<p>COST: \$\$\$\$ IMPACT: HIGH COMPLEXITY: LOW</p> <p>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)</p> <p>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.</p> <p>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.</p>	<p>DATE:</p> <p><input type="checkbox"/> IMPLEMENTED</p> <p><input type="checkbox"/> IN PROGRESS</p> <p><input type="checkbox"/> SCOPED</p> <p><input type="checkbox"/> NOT STARTED</p>	<p>DATE:</p> <p><input type="checkbox"/> IMPLEMENTED</p> <p><input type="checkbox"/> IN PROGRESS</p> <p><input type="checkbox"/> SCOPED</p> <p><input type="checkbox"/> NOT STARTED</p>



Ransomware Readiness Assessment (RRA)

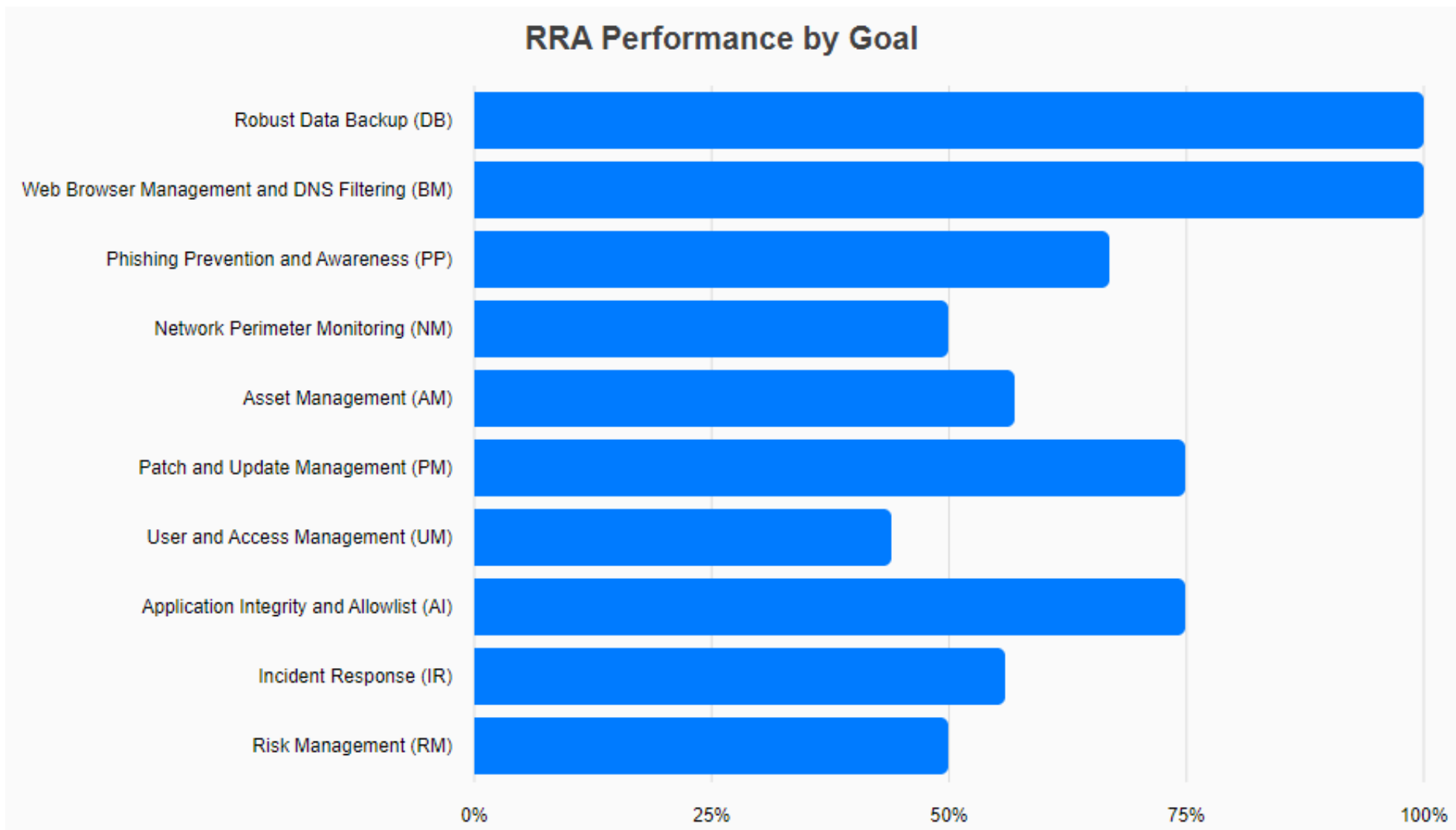
To understand your cybersecurity posture and assess how well your organization is equipped to defend and recover from a ransomware incident, take the Ransomware Readiness Assessment (RRA). The RRA is a self-assessment based on a tiered set of practices to help organizations better assess how well they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

Home

Logout

Threat-based PMI:

- Natural Disaster
- Distributed Denial-of-Service
- Remote Access Compromise
- System Integrity Compromise

Scenario:

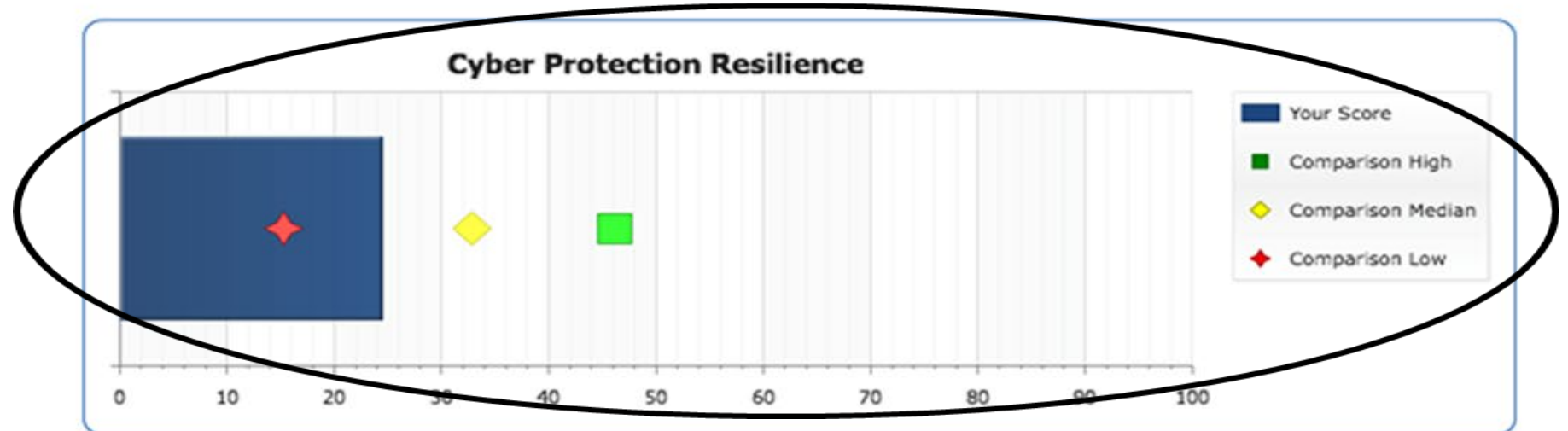
- Where should we to invest?
- Weakest area in comparison to peers
- Show management improvement

Cyber IST Survey for

Threat Overlay: General

Scenario: General

Cyber Protection Resilience



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

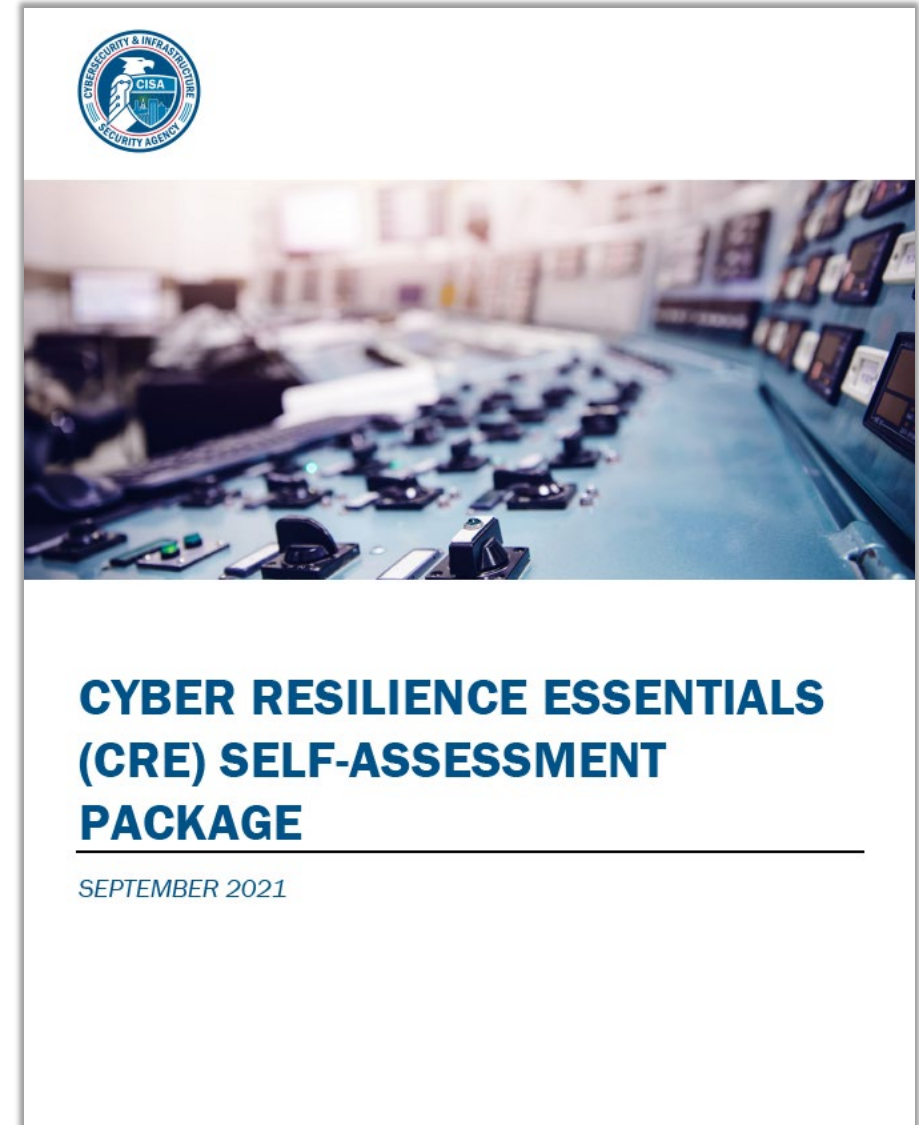
Cyber Resilience Essentials (CRE)

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

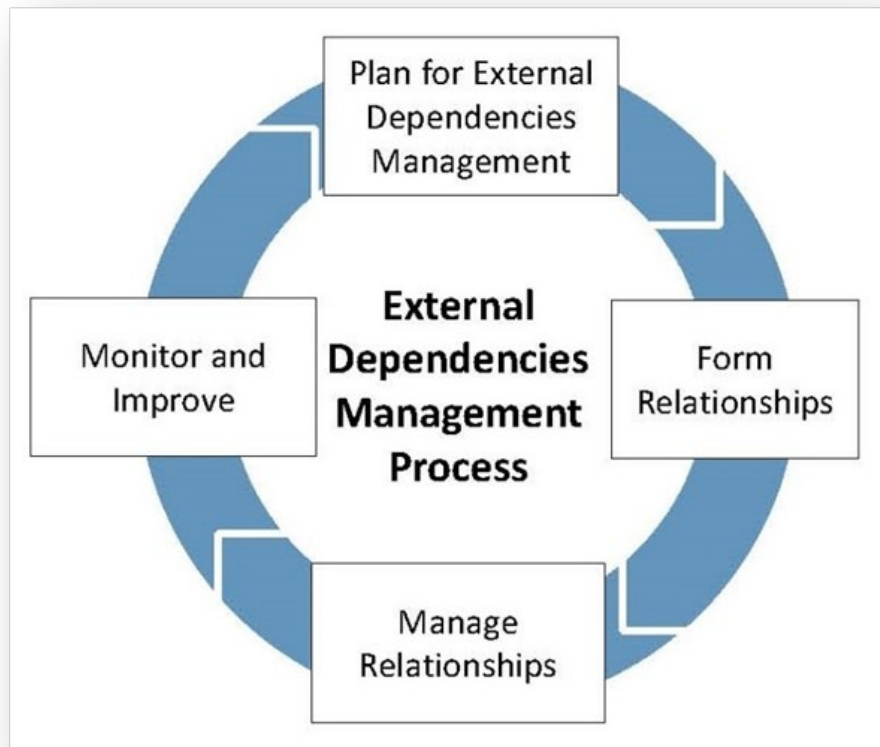
Evaluates the maturity of an organization's capacities and capabilities in performing, planning, managing, measuring, and defining cybersecurity capabilities.

Goal: Identify Cybersecurity Strengths & Weaknesses

- 11 Domains
- 103 Practices



External Dependency 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

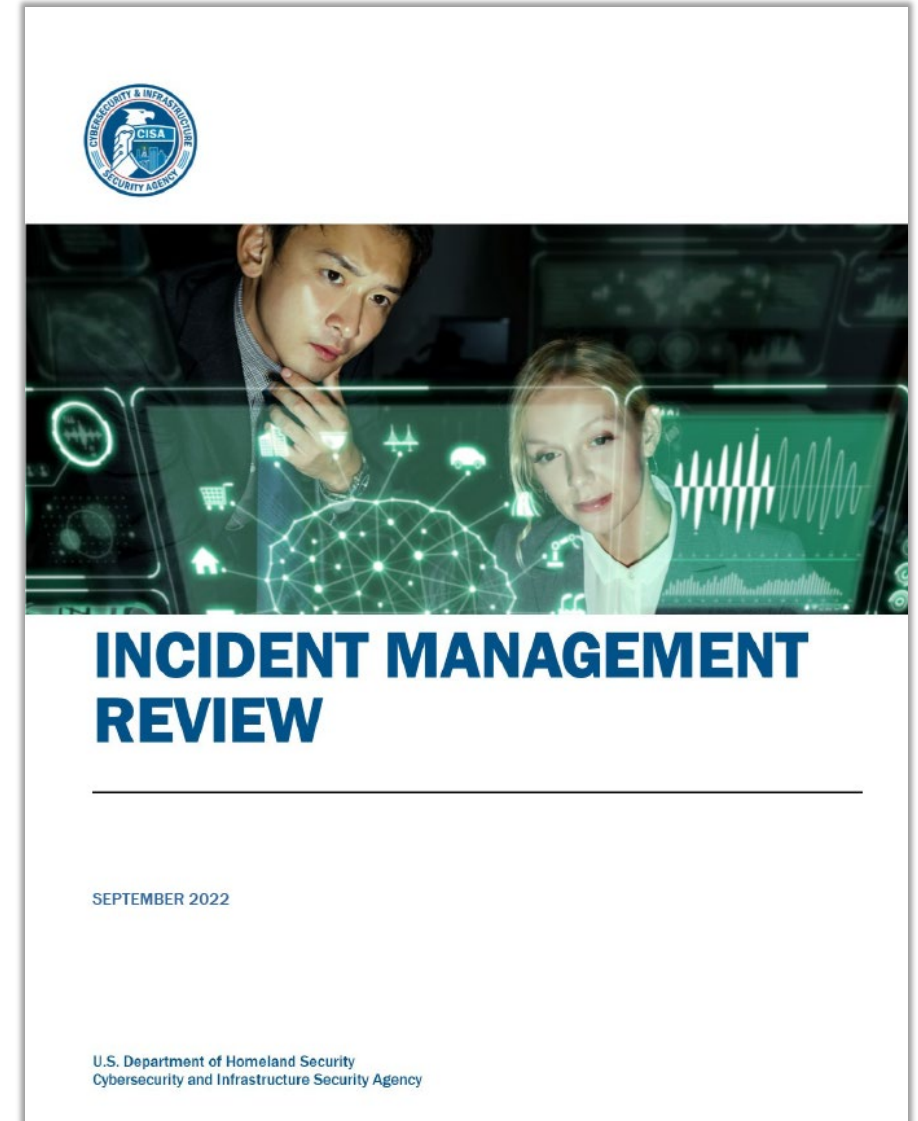


Incident Management Review (IMR)

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):
Question Set with Guidance

February 2016



Department of
Homeland
Security

Cyber Resilience Review (CRR) | Domains

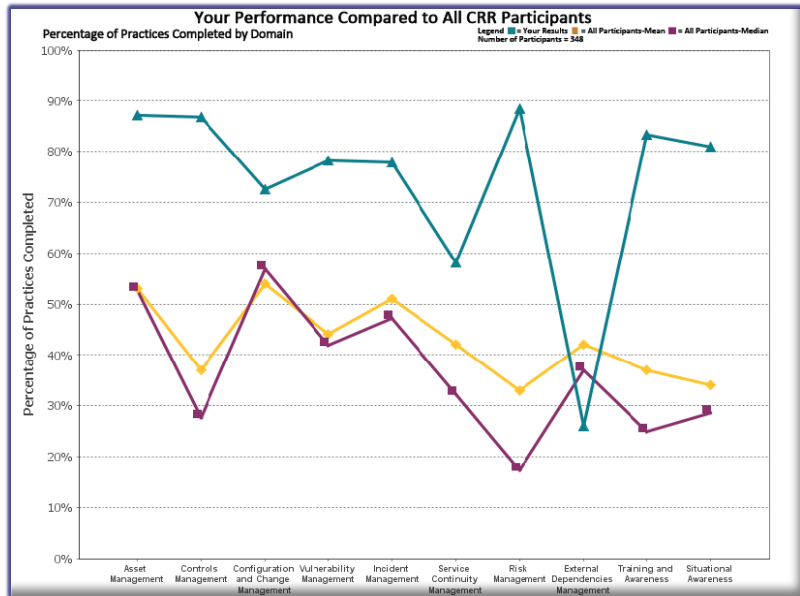
These represent key areas that typically contribute to an organization’s cyber resilience— each domain focuses on:

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



Benefits of CRR



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																										
ML-1			ML-2			ML-3			ML-4			ML-5														
G1	G2	G3	G4	G5	G6	G7	IL1	IL2	IL3	IL4	IL5	IL6	IL7	IL8												
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:																										
<ul style="list-style-type: none"> 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 an analysis of potential impact if these services are disrupted? [SC.SG2.SP1] Incomplete																										
Q2 CERT-RMM Reference: [SC.SG2.SP1] Identify and inventory 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]																										
<table border="1" style="width:100%; border-collapse: collapse;"> <tr> <td style="width:80%;"></td> <td style="width:10%;">People</td> <td style="width:10%;">Incomplete</td> </tr> <tr> <td></td> <td>Information</td> <td>Incomplete</td> </tr> <tr> <td></td> <td>Technology</td> <td>Incomplete</td> </tr> <tr> <td></td> <td>Facilities</td> <td>Yes</td> </tr> </table>																People	Incomplete		Information	Incomplete		Technology	Incomplete		Facilities	Yes
	People	Incomplete																								
	Information	Incomplete																								
	Technology	Incomplete																								
	Facilities	Yes																								
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



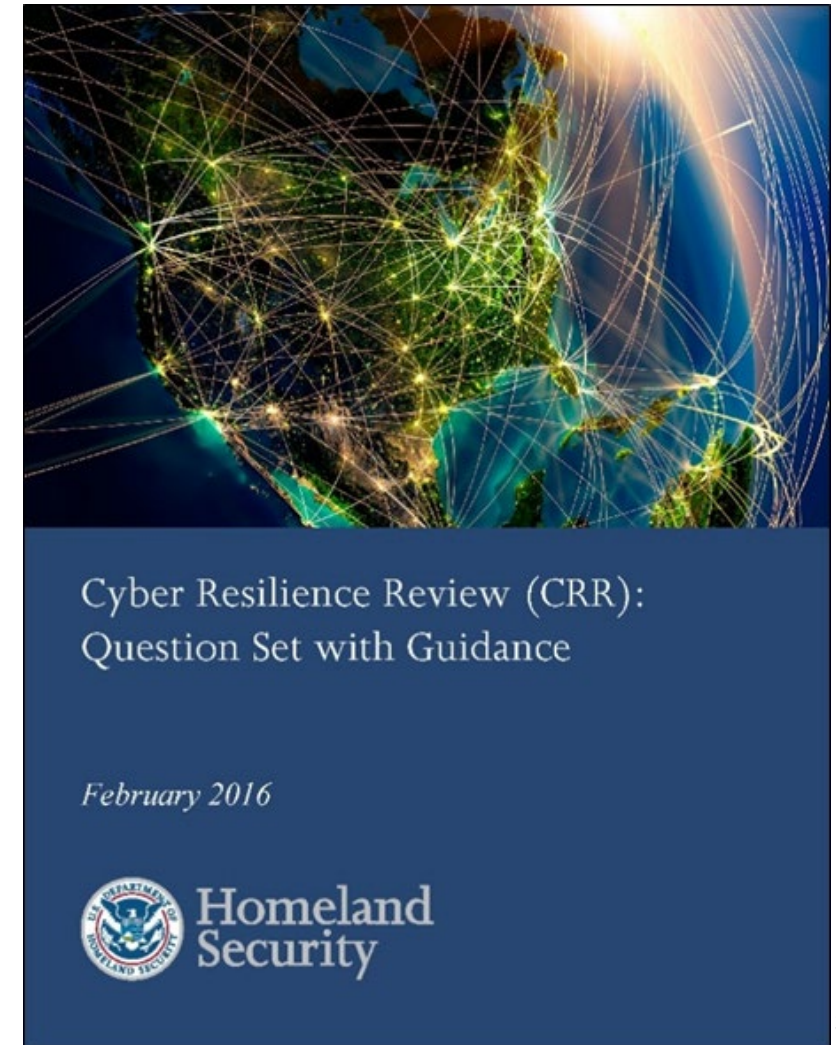
Cyber Resilience Workshop (CRW)

Description: A 2-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



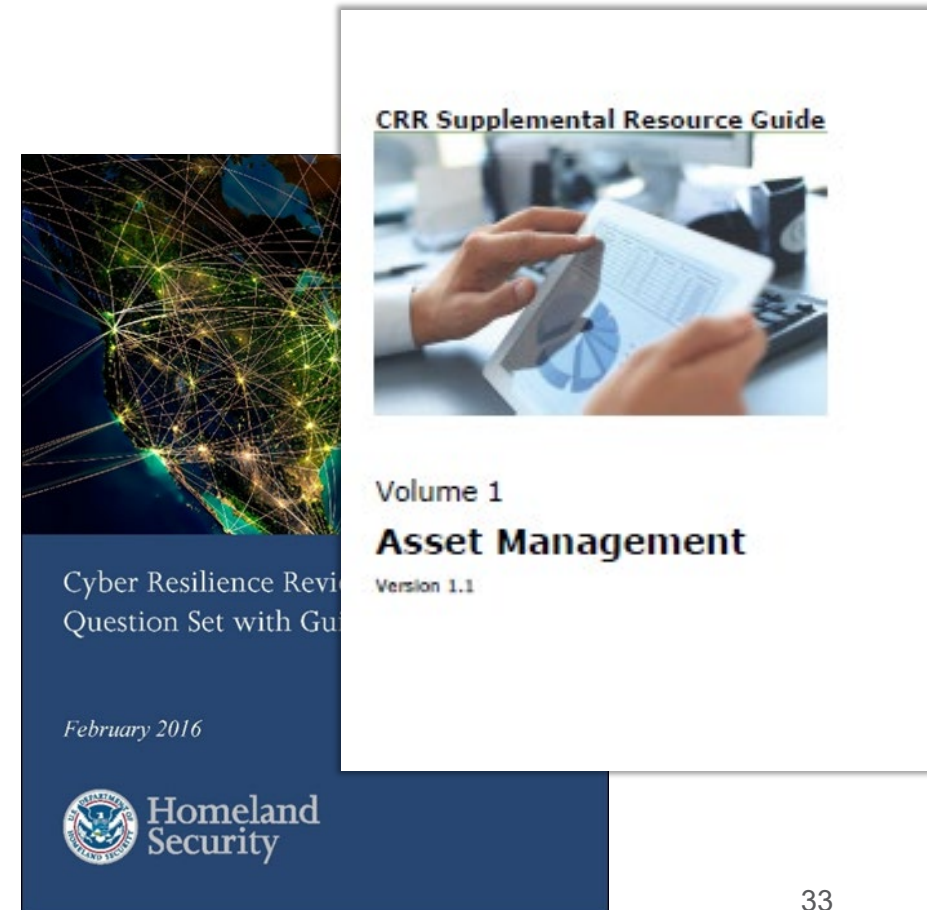
Asset Management Workshop (AMW)

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 2.5-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



Cyber Resilience Review
Question Set with Guidance

February 2016



CRR Supplemental Resource Guide



Volume 5

Incident Management

Version 1.1

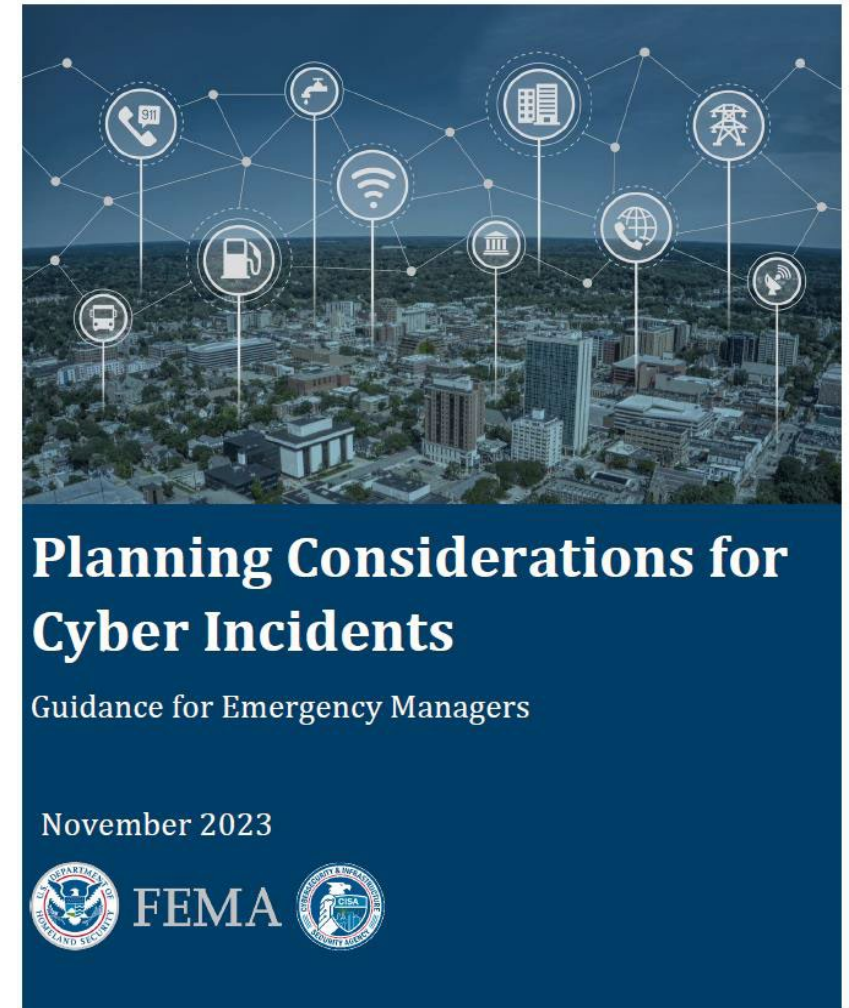
OEM Planning Considerations for Cyber Incidents Workshop

For Emergency Managers managing or taking part in responding to incidents caused by a cybersecurity incident on critical infrastructure.

This is a 2.5 hour non-technical and informative session designed to assist state, local, tribal, and territorial (SLTT) emergency management personnel to collaboratively prepare for a cyber incident and support the development of a cyber incident response plan or annex.

Audience: Individuals with responsibilities for -

- Emergency Management in Government
- Emergency Management in Academia, Nonprofits, Private Sector
- Jurisdiction Planning Teams



Vulnerability Management Workshop (VMW)

Description: A 1.5-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



The image shows the cover of a document titled "CYBER RESILIENCE REVIEW" with the "U.S. DEPARTMENT OF HOMELAND SECURITY" logo. Below this is the subtitle "CRR Supplemental Resource Guide". The cover is split into two main sections. The left section features a network of glowing green nodes and lines on a dark background, with the text "Cyber Resilience Review Question Set with Guidance" and "February 2016" at the bottom. The right section features a hand placing a wooden block on a bar chart, with the text "Volume 4", "Vulnerability Management", and "Version 1.1". At the bottom right, the "U.S. DEPARTMENT OF HOMELAND SECURITY" logo and the text "Homeland Security" are visible.

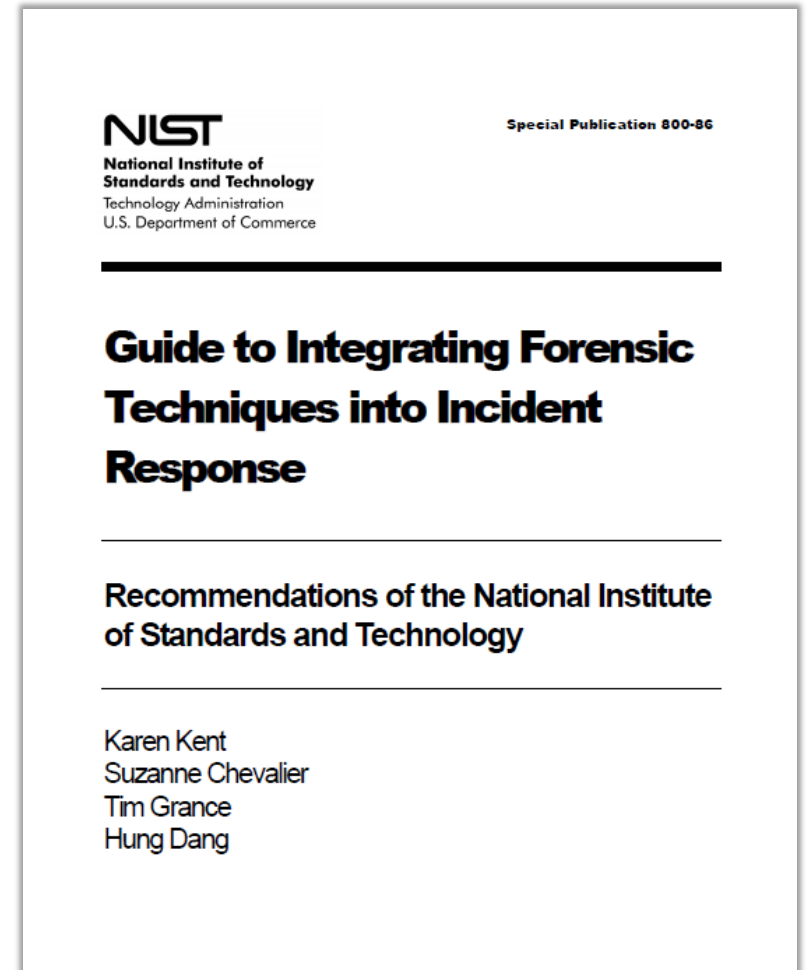
Introduction to Digital Forensics Workshop (DFW)

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.



Digital Forensics Workshop II (DFW2) | Autopsy

Description: A 3 hour informative and hands-on session designed to introduce the Autopsy digital forensic toolkit.

Goal: To provide an overview of an easy to use, GUI-based program that allows you to efficiently analyze hard drives and smart phones.

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.



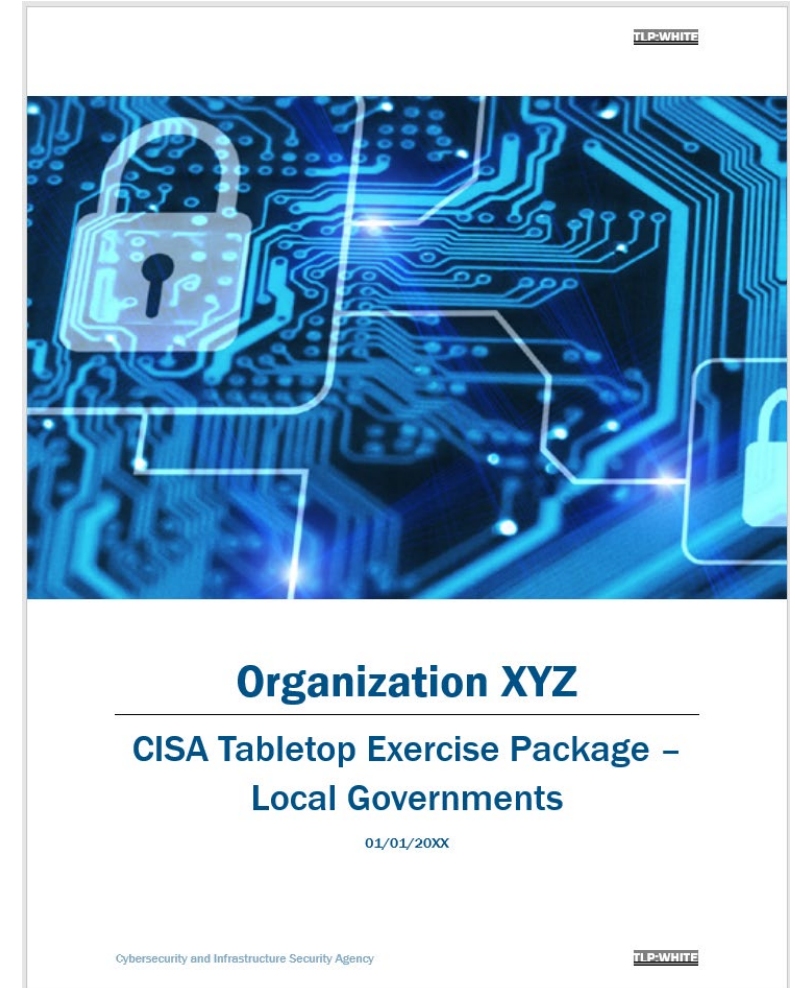
Cyber Exercise (CYX)

Description: A customizable 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



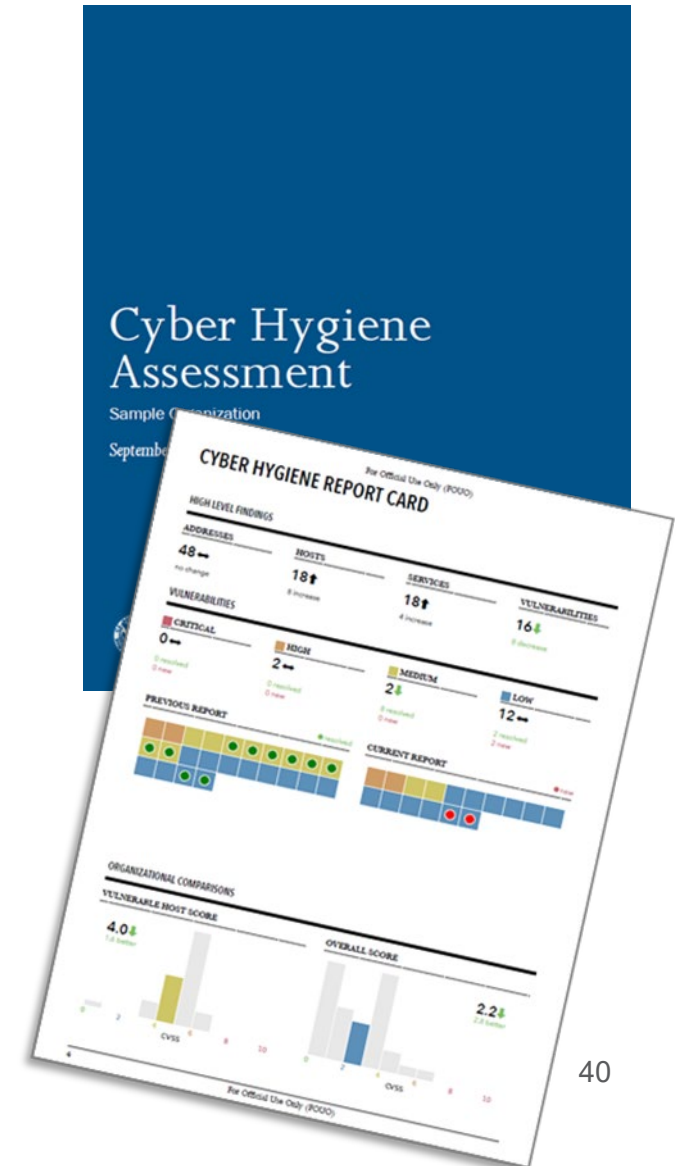
Vulnerability Scanning Service (CyHy)

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



Web Application Scanning (WAS)

An Internet based scanning service to assess 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



Information Sharing



Cybersecurity Alerts & Advisories

Filters

What are you looking for?

Sort

Rel

APP

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](#)

Subscribe to CISA Alerts and Advisories



SUBSCRIBE NOW



<https://public.govdelivery.com/accounts/USDHSCISA/subscriber/new?>

Advisory Type

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

Release Year



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-advisories>

Known Exploited Vulnerabilities Catalog

Filters

What are you looking for?

Sort by (optional)

Publish Date



Items per page (optional)

20



APPLY

Vendor/Project



QUALCOMM | MULTIPLE CHIPSETS



[CVE-2022-22071](#)

Qualcomm Multiple Chipsets Use-After-Free Vulnerability

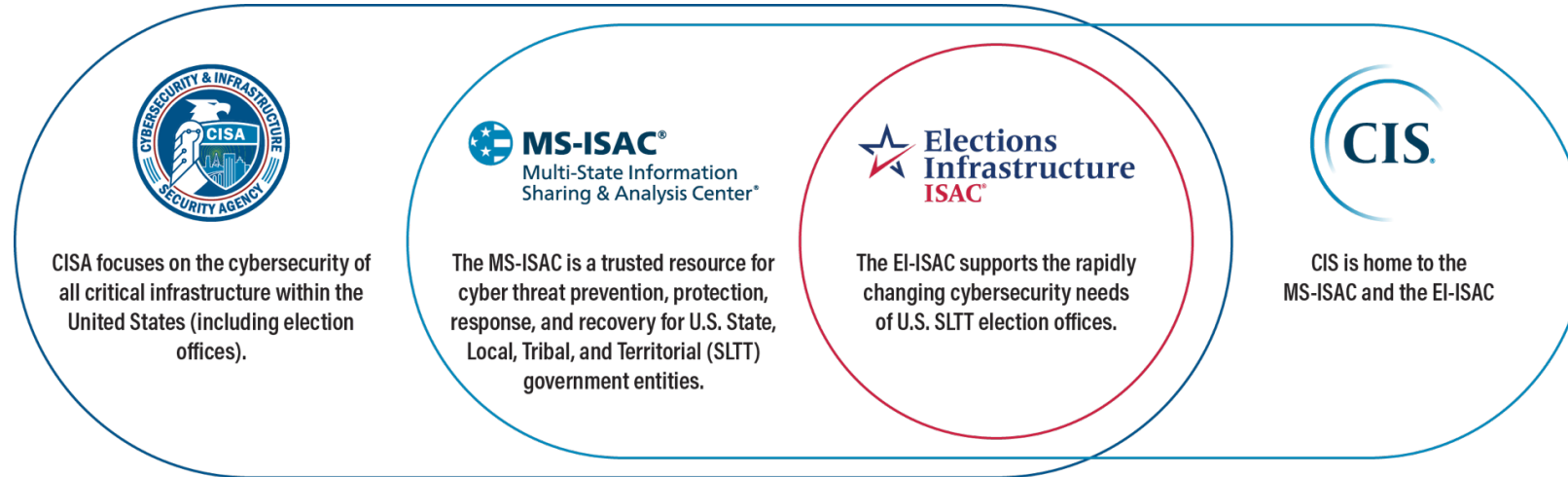
Multiple Qualcomm chipsets contain a use-after-free vulnerability when process shell memory is freed using IOCTL munmap call and process initialization is in progress.

- **Action:** Apply remediations or mitigations per vendor instructions or discontinue use of the product if remediation or mitigations are unavailable.
- **Known To Be Used in Ransomware Campaigns?:** Unknown
- **Date Added:** 2023-12-05
- **Due Date:** 2023-12-26

Resources and Notes +

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

Multi-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.



Logging Made Easy

[CISA's Logging Made Easy \(LME\)](#) is a no-cost log management solution for small to medium-sized organizations with limited resources that would otherwise have little to no functionality to detect attacks. LME offers centralized logging, proactive threat detection and enhanced security by allowing organizations to monitor their network, identify users, and actively analyze Sysmon data to quickly identify potential malicious activity. As a locally run application, CISA cannot access LME data, ensuring the privacy and security of organizations' information.

LME is dedicated to evolving with the cybersecurity needs of its community. Available to the public, LME serves organizations across private, public and non-profit sectors, especially those operating Windows-based, on-premises networks.

To get started with LME, download it directly from [CISA's GitHub page](#). For any questions, please contact CyberSharedServices@cisa.dhs.gov



SCuBA Overview

What is SCuBA? The Secure Cloud Business Applications (SCuBA) project provides guidance and capabilities to secure entities' cloud business application environments and protect information created, accessed, shared, and stored in those environments.

What are SCuBA's Benefits? SCuBA will enhance the security of cloud business application environments through additional configurations, settings, and security products.

[Secure Cloud Business Applications \(SCuBA\) Project | CISA](#)



Cyber Training



CISA Learning

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

CISA Learning 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://learning.cisa.gov/>



ICS Training Opportunities

ICS-CERT Virtual Learning Portal (VLP)

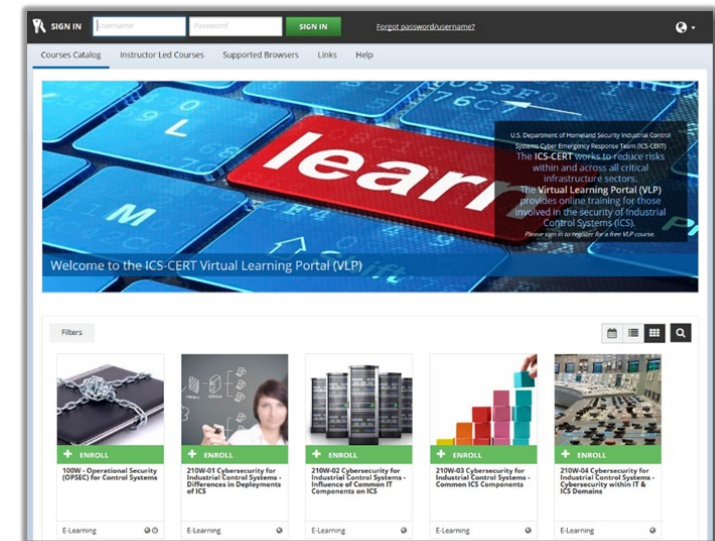
- Virtual & Instructor Led Training
- No Cost

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.



The graphic illustrates the IMR training series across three phases: IDENTIFY, MITIGATE, and RECOVER. Each phase is associated with specific training offerings, their target audience, capacity, and duration.

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

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>

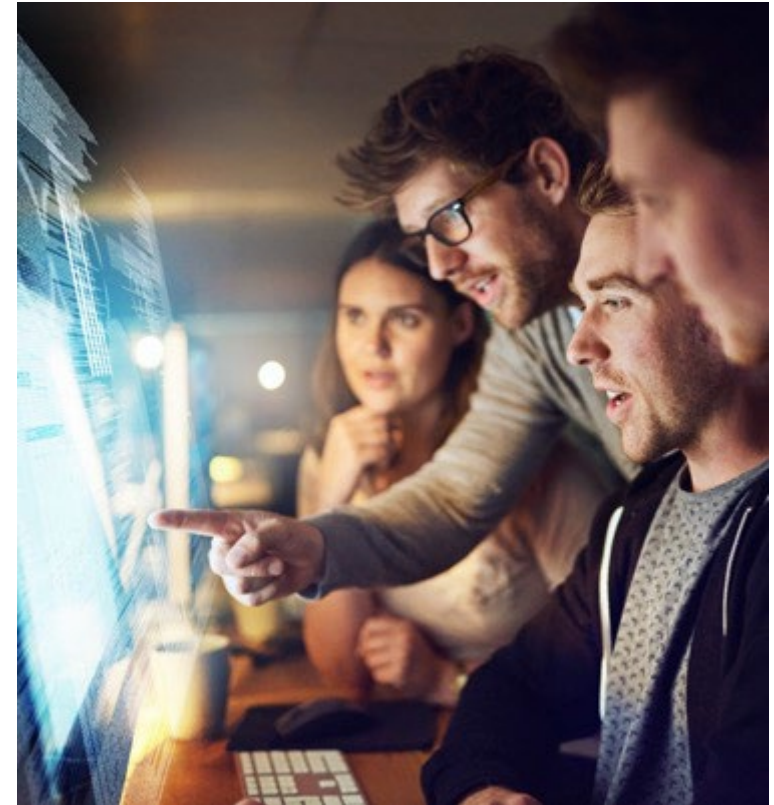
Incident Reporting



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.



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/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.cisa.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.





CISA REGION 6

Andrew Buschbom

State Cybersecurity Coordinator

Region 6 | New Mexico

Cybersecurity and Infrastructure Security Agency

EMAIL: andrew.buschbom@cisa.dhs.gov

CELL: (505) 302-4299

Felix Villa

Cybersecurity Advisor

Region 6 | El Paso, TX & Las Cruces, NM

Cybersecurity and Infrastructure Security Agency

EMAIL: felix.villa@cisa.dhs.gov

CELL: (575) 446-2749

CISA INCIDENT REPORTING SYSTEM

<https://www.cisa.gov/report>

CISA CENTRAL - 24/7 Watch

(888) 282-0870; report@cisa.gov

FBI's 24/7 Cyber Watch (CyWatch)

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