

CYBERSECURITY SERVICES FOR BUILDING CYBER RESILIENCE

Rachael Han
Regional Analyst, Region 2
Cybersecurity & Infrastructure Security Agency

Jon Easton
Cybersecurity Advisor, Region 2
Cybersecurity and Infrastructure Security Agency



Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient infrastructure for the American people.

MISSION

Lead the national effort to understand, manage, and reduce risk to the nation's cyber and physical infrastructure.



Serving Critical Infrastructure

KEY ACTIVITIES:



16 CRITICAL INFRASTRUCTURE SECTORS:

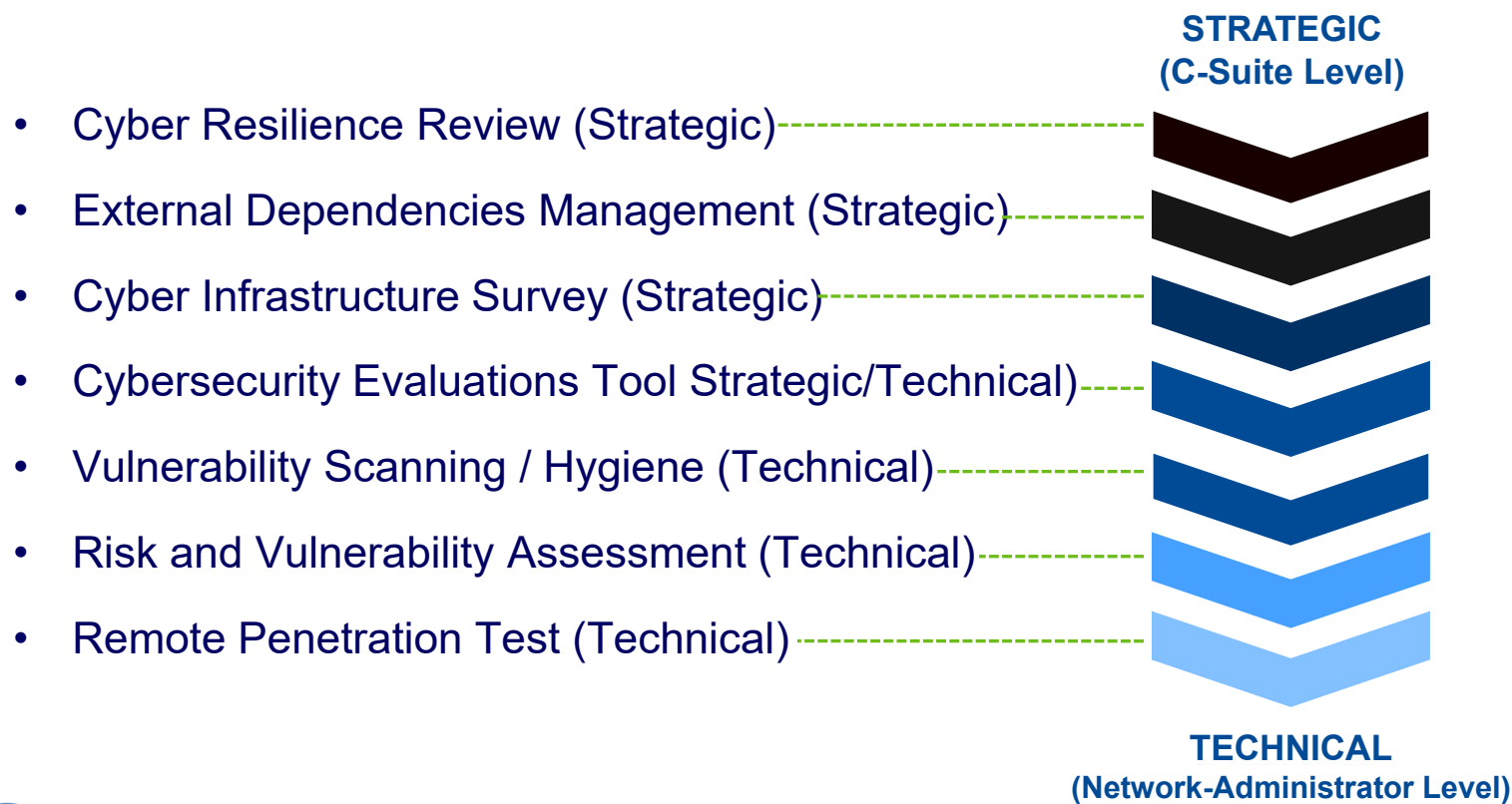


CISA CYBERSECURITY SERVICES



Jon Easton
July 24, 2024

Range of Cybersecurity Assessments



NIST Cybersecurity Framework

- All CRR and EDM practices are mapped to the subcategories of the CSF
 - After performing a CRR or EDM, organizations can compare the results to the criteria of the NIST CSF to identify gaps and where appropriate improvement efforts are needed
- The Cybersecurity Framework
 - Establishes a common perspective and vernacular,
 - Provides risk-based guidelines,
 - Is collaboration-oriented, and
 - Is internationally recognized.
- For more information, visit nist.gov/cyberframework

<i>Functions</i>	<i>Categories</i>
IDENTIFY (ID)	Asset Management (AM)
	Business Environment (BE)
	Governance (GV)
	Risk Assessment (RA)
PROTECT (PR)	Risk Management Strategy (RM)
	Access Control (AC)
	Awareness and Training (AT)
	Data Security (DS)
	Information Protection Processes and Procedures (IP)
	Maintenance (MA)
DETECT (DE)	Protective Technology (PT)
	Anomalies and Events (AE)
	Security Continuous Monitoring (CM)
RESPOND (RS)	Detection Processes (DP)
	Incident Response Planning (RP)
	Communications (CO)
	Analysis (AN)
	Mitigation (MI)
RECOVER (RC)	Improvements (IM)
	Recovery Planning (RP)
	Improvements/Gap Remediation (IM)
	Communications (CO)



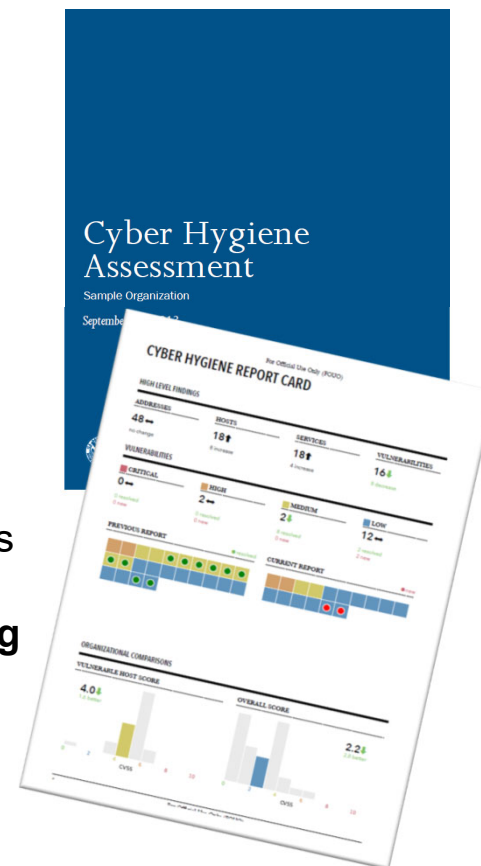
Vulnerability Scanning

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

Delivery: Online by CISA

Benefits:

- Continual review of system to identify potential problems
- Weekly reports detailing current and previously mitigated vulnerabilities
- Recommended mitigation for identified vulnerabilities
- **Network Vulnerability & Configuration Scanning**
 - Identify network vulnerabilities and weakness



Jon Easton
July 24, 2024

Cyber Security Evaluation Tool (CSET)

- **Purpose:** Assesses control system and information technology network security practices against industry standards.
- **Facilitated:** Self-Administered, undertaken independently
- **Benefits:**
 - Immediately available for download upon request
 - Understanding of operational technology and information technology network security practices
 - Ability to drill down on specific areas and issues
 - Helps to integrate cybersecurity into current corporate risk management strategy

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



<https://cset-download.inl.gov/>



Jon Easton
July 24, 2024

Cybersecurity Performance Goals

a **prioritized** subset of IT and OT cybersecurity practices aimed at meaningfully reducing risks.

This subset was selected using these criteria:

- Demonstrated value in reducing the risk or impact of commonly observed, cross-sector threats and cyber threat actor TTPs.
- Clear, actionable, and easily definable.
- Reasonably straightforward and not cost-prohibitive for even small- and medium-sized entities to successfully implement.

The cover of the "Cybersecurity Performance Goals" document. It features a central image of a server room with rows of server racks. The top left corner has the CISA logo. The top right corner contains the text "CPG Cross-Sector Cybersecurity Performance Goals March 2023 Update". The bottom right corner has the text "PERFORMANCE GOALS Version: 1.0.1". At the very bottom right, the author's name "Jon Easton" and the date "July 24, 2024" are listed.

CPG
Cross-Sector Cybersecurity
Performance Goals
March 2023 Update

PERFORMANCE
GOALS
Version: 1.0.1

Jon Easton
July 24, 2024

Logging Made Easy (LME)

In 2023, CISA introduced LME on GitHub. LME is a government-vetted, intuitive log management tool



Designed for small to midsize organizations with limited resources, LME offers unified logging and proactive threat detection



LME enables organizations to monitor their network, identify users and enhances security



LME Snapshot

- Creates a centralized repository of Windows Sysmon logs to detect incidents or suspicious events, aiding in incident response, account, device, and monitoring
- Uses open source technology alongside CISA-developed configurations and scripts
- Works in conjunction with threat reports, queries for the presence of an attacker in the form of Indicators of Compromise (IOCs) and Tools, Techniques and Procedures (TTPs).

Key Benefits

- No cost to users
- Quick setup and guided implementation for simplified log management
- Integrated monitoring for real-time threat visibility
- Trusted and transparent operations
- Tailored dashboards to fit users' needs
- Community Collaboration (GitHub discussions)
- No information is collected or sent back to CISA

Easy Installation

- User-friendly instructions for downloading and installing LME are available at [LME's GitHub Repo](#)
- LME's instructions provide detailed steps organized by chapters and explain how the tool uses endpoint agents for thorough event data collection and analysis.

Jon Easton

Contact LME:



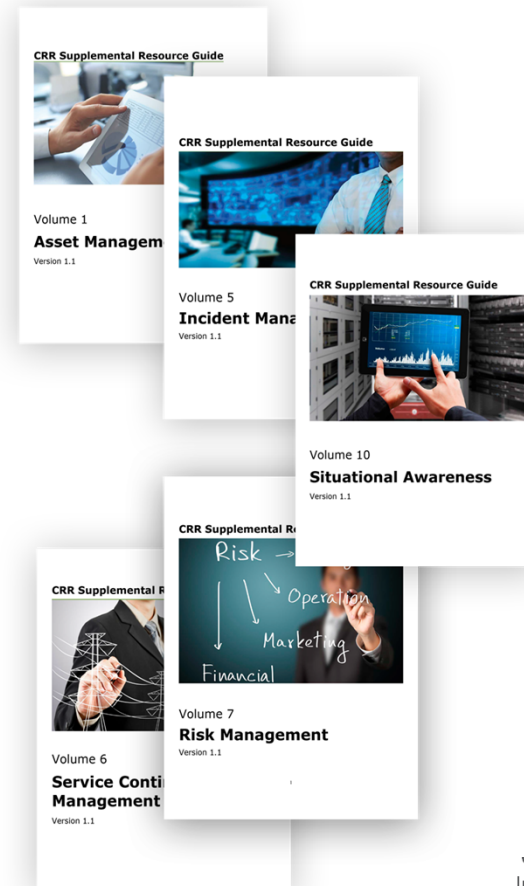
[CSSO Email](#)



[LME's GitHub Repo](#)

Resource Guides

- **Resource Guides:** Created to help organizations enhance their resilience in specific Cyber Resilience Review (CRR) domains.
- **CRR Tools:** Helps move organizations from initial capability to well-defined capability in security management areas
- **CRR Domains:** Includes the CRR 10 “domains” each representing a capability area foundational to an organization’s cyber resilience.
- **Content:** While the guides were developed for organizations to utilize after conducting a CRR, these publications provide content useful for all organizations with cybersecurity equities.
- **Flexibility in Use:** Moreover, the guides can be utilized as a full set or as individual components, depending on organizational preference and/or need.
- For more information, visit <https://www.cisa.gov/cyber-resource-hub>





Jon Easton
July 24, 2024

Federal Ransomware Website

An official website of the United States government [Here's how you know](#) ▾

STOP RANSOMWARE

Search 



WHAT IS RANSOMWARE?

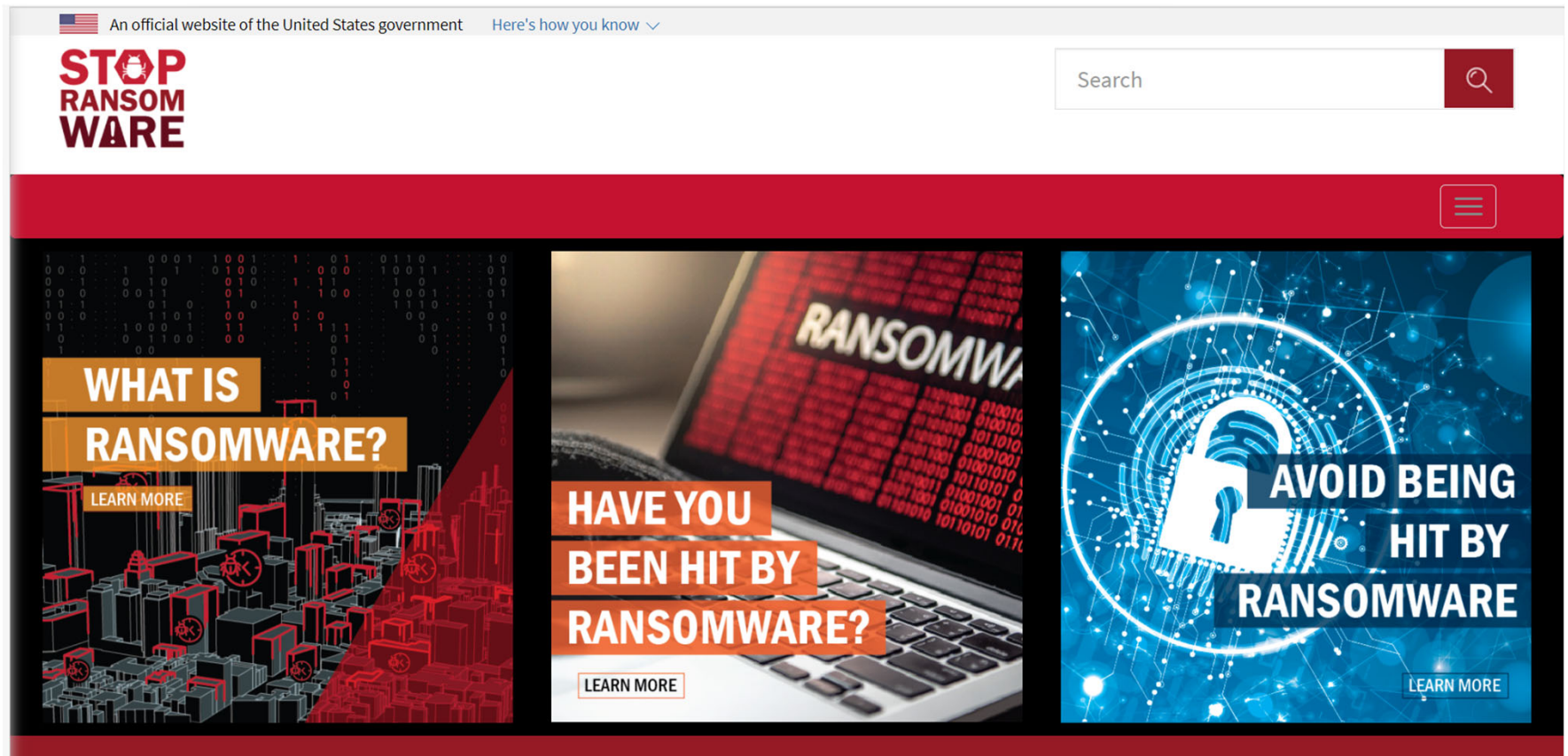
[LEARN MORE](#)

HAVE YOU BEEN HIT BY RANSOMWARE?

[LEARN MORE](#)

AVOID BEING HIT BY RANSOMWARE

[LEARN MORE](#)



Visit StopRansomware.gov today!

Free Federal Cyber Training

FedVTE enables cyber professionals to continue growing skills.

FedVTE is an online, on-demand training center that provides **free** cybersecurity training for U.S. veterans and federal, state, local, tribal, and territorial government employees. **As of January 2017**, there are:

- Over 140,000 registered users, including employees at all levels of government
- Over 18,000 veteran users (through non-profit partner, Hire Our Heroes™)
- Over 5,000 SLTT registered users

<https://fedvte.usalearning.gov/>



Cybersecurity Performance Goals

- CISA's Cybersecurity Performance Goals (CPGs) are a subset of cybersecurity practices, selected through a thorough process of industry, government, and expert consultation, aimed at meaningfully reducing risks to both critical infrastructure operations and the American people.
- **The CPGs are intended to be:**
 - A baseline set of cybersecurity practices broadly applicable across critical infrastructure with known risk-reduction value.
 - A benchmark for critical infrastructure operators to measure and improve their cybersecurity maturity.
 - A combination of recommended practices for information technology (IT) and operational technology (OT) owners, including a prioritized set of security practices.

The cover page of the CPG Performance Goals document. It features a central image of a server room aisle with perspective lines. The top left corner has the CISA logo. The top right corner has the text "CPG Cross-Sector Cybersecurity Performance Goals March 2023 Update". The bottom right corner has the text "PERFORMANCE GOALS Version: 1.0.1" and a blue triangle. The bottom right corner also has the text "Jon Easton July 24, 2024".

CPG
Cross-Sector Cybersecurity
Performance Goals
March 2023 Update

PERFORMANCE
GOALS
Version: 1.0.1

Jon Easton
July 24, 2024

Cyber Security Evaluation Tool (CSET)

The screenshot displays the CSET web application interface. At the top, there is a navigation bar with the CSET logo, a search bar, and buttons for 'New Assessment' and 'My Assessments'. Below the navigation bar, there is a section titled 'Popular Assessments' which contains four assessment cards. The first card, 'CISA Cross-Sector Cybersecurity Performance Goals (CPG)', is highlighted with a green border. Below this section is another section titled 'CISA Sponsored (Resilience and Maturity)' which contains four more assessment cards: 'CISA Cyber Infrastructure Survey (CIS)', 'CISA Cyber Resilience Review (CRR)', 'CISA External Dependencies Management (EDM)', and 'CISA Ransomware Readiness'.

Local Installation

File Edit View Window

CSET Tools Resource Library

New Assessment My Assessments

Search

To start a new assessment, click on a card. To view additional details click the **i** icon.

Popular Assessments

- CISA Cross-Sector Cybersecurity Performance Goals (CPG)**
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 know...
- CISA Ransomware Readiness Assessment (RRA)**
Ransomware poses an increasing threat and continues to rise as a top cyber threat impacting both businesses and government agencies. Ransomware is a type of malicious attack where attackers encrypt an or...
- NIST CSF: Framework for Improving Critical Infrastructure Cybersecurity v1.1**
This approach is a voluntary risk-based Cybersecurity Framework – a set of industry standards and best practices to help organizations manage cybersecurity risks. The resulting Framework, created through collabora...
- Network Diagram/Component**
A Network Architecture and Diagram assessment requires that you build a network diagram and creates a question set specific...

CISA Sponsored (Resilience and Maturity)

- CISA Cyber Infrastructure Survey (CIS)**
The CIS goal is to assess the foundational and essential cybersecurity practices of an organization's critical service to identify dependencies, capabilities and emerging effects of the current cybersecurity posture. C...
- CISA Cyber Resilience Review (CRR)**
The CRR is a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. The CRR may be conducted as a self-assessment or as a facilitated assess...
- CISA External Dependencies Management (EDM)**
The External Dependencies Management (EDM) Assessment evaluates an organization's management of external dependencies. This assessment focuses on the relationship between an organization's high...
- CISA Ransomware Readiness**
Ransomware poses an increasing th...
cyber threat impacting both business...
Ransomware is a type of malicious a...



Assessment Items (Goals)

The screenshot displays the CSET application interface. At the top, there is a menu bar with 'File', 'Edit', 'View', and 'Window'. Below this is a yellow header with 'Local Installation'. The main navigation bar includes the CSET logo, 'Tools', and 'Resource Library'. A secondary navigation bar has three tabs: 'Prepare', 'Assessment' (which is highlighted with a white background and a question mark icon), and 'Results'. On the left, a dark blue sidebar contains a home icon and a list of menu items: 'Prepare' (with a dropdown arrow), 'Assessment Configuration', 'Assessment Information', 'Assessment' (with a dropdown arrow), 'Results' (with a dropdown arrow), 'Performance Summary', and 'Security Practice Checklist'. The 'Security Practices' item under the 'Assessment' dropdown is highlighted with a white box and a yellow arrow pointing to it from the left. The main content area shows the title 'Security Practices - CPG' and a sub-header 'Unanswered questions are calculated as a 'Not' response'. Below this is a section titled 'CPG Answer Key' with a bulleted list of four items: 'Implemented', 'In Progress', 'Scoped', and 'Not Implemented', each with a brief description.



Format in CSET

1.C Security Practice

OT Cybersecurity Leadership



Outcome

A single leader is responsible and accountable for OT-specific cybersecurity within an organization with OT assets.



Scope

N/A

Recommended Action

A named role/position/title is identified as responsible and accountable for planning, resourcing, and execution of OT-specific cybersecurity activities. In some organizations this may be the same position as identified in 1.B.



Format in CSET - References



NIST Cybersecurity Framework (CSF) Reference

ID.GV-1, ID.GV-2

TTP or Risk Addressed

Lack of accountability, investment, or effectiveness of OT cybersecurity program.

Additional External References

NIST SP 800-53: PM-2, PM-29

ISA 62443-2-1:2009 4.3.2.3.3, 4.3.2.6

ISO/IEC 27001:2013 A.5.1.1, A.6.1.1, A.7.2.1, A.15.1.1

Source Documents

CISA Cross-Sector Cybersecurity Performance Goals (CPG): [1.C](#)

Additional Documents

NIST Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations: [document](#)

NIST CSF: Framework for Improving Critical Infrastructure Cybersecurity v1.1: [ID.GV-1](#), [ID.GV-2](#)

NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations (September 2020, includes updates as of Dec. 10, 2020): [document](#)



Format in Checklist

1.C OT Cybersecurity Leadership	ID.GV-1, ID.GV-2	CURRENT ASSESSMENT
<p>COST: \$\$\$\$ IMPACT: HIGH COMPLEXITY: LOW</p> <p>TTP OR RISK ADDRESSED:</p> <p>Lack of accountability, investment, or effectiveness of OT cybersecurity program.</p> <p>RECOMMENDED ACTION: A named role/position/title is identified as responsible and accountable for planning, resourcing, and execution of OT-specific cybersecurity activities. In some organizations this may be the same position as identified in 1.B.</p>	<p>DATE: <input type="text"/></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>	

1.C OT Cybersecurity Leadership



ID.GV-1, ID.GV-2

CURRENT ASSESSMENT

COST: \$\$\$\$

IMPACT: **HIGH**



COMPLEXITY: **LOW**



TTP OR RISK ADDRESSED:

Lack of accountability, investment, or effectiveness of OT cybersecurity program.

RECOMMENDED ACTION: A named role/position/title is identified as responsible and accountable for planning, resourcing, and execution of OT-specific cybersecurity activities. In some organizations this may be the same position as identified in 1.B.

DATE:



IMPLEMENTED



IN PROGRESS



SCOPED

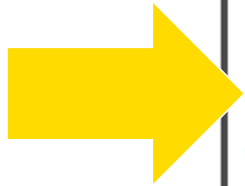


NOT STARTED



1.C OT Cybersecurity Leadership

ID.GV-1, ID.GV-2



COST: \$\$\$\$

IMPACT: HIGH



COMPLEXITY: LOW



TTP OR RISK ADDRESSED:

Lack of accountability, investment, or effectiveness of OT cybersecurity program.

RECOMMENDED ACTION: A named role/position/title is identified as responsible and accountable for planning, resourcing, and execution of OT-specific cybersecurity activities. In some organizations this may be the same position as identified in 1.B.



1.C OT Cybersecurity Leadership

ID.GV-1, ID.GV-2

COST: \$\$\$\$ **IMPACT:** **HIGH** **COMPLEXITY:** **LOW**

TTP OR RISK ADDRESSED:

Lack of accountability, investment, or effectiveness of OT cybersecurity program.

RECOMMENDED ACTION: A named role/position/title is identified as responsible and accountable for planning, resourcing, and execution of OT-specific cybersecurity activities. In some organizations this may be the same position as identified in 1.B.



1.C OT Cybersecurity Leadership

ID.GV-1, ID.GV-2

COST: \$\$\$\$ **IMPACT:** **HIGH** **COMPLEXITY:** **LOW**

TTP OR RISK ADDRESSED:

Lack of accountability, investment, or effectiveness of OT cybersecurity program.

RECOMMENDED ACTION: A named role/position/title is identified as responsible and accountable for planning, resourcing, and execution of OT-specific cybersecurity activities. In some organizations this may be the same position as identified in 1.B.

Recommended Action

A named role/position/title is identified as responsible and accountable for planning, resourcing, and execution of OT-specific cybersecurity activities. In some organizations this may be the same position as identified in 1.B.



1.C OT Cybersecurity Leadership

ID.GV-1, ID.GV-2

CURRENT ASSESSMENT

COST: \$\$\$\$

IMPACT:

HIGH

COMPLEXITY:

LOW

TTP OR RISK ADDRESSED:

Lack of accountability, investment, or effectiveness of OT cybersecurity program.

RECOMMENDED ACTION: A named role/position/title is identified as responsible and accountable for planning, resourcing, and execution of OT-specific cybersecurity activities. In some organizations this may be the same position as identified in 1.B.

DATE:

IMPLEMENTED

IN PROGRESS

SCOPED

NOT STARTED



1.C OT Cybersecurity Leadership

ID.GV-1, ID.GV-2

CURRENT ASSESSMENT

COST: \$\$\$\$ **IMPACT:** **HIGH** **COMPLEXITY:** **LOW**

TTP OR RISK ADDRESSED:

Lack of accountability, investment, or effectiveness of OT cybersecurity program.

RECOMMENDED ACTION: A named role/position/title is identified as responsible and accountable for planning, resourcing, and execution of OT-specific cybersecurity activities. In some organizations this may be the same position as identified in 1.B.

DATE:

- IMPLEMENTED**
- IN PROGRESS**
- SCOPED**
- NOT STARTED**



1.C OT Cybersecurity Leadership

ID.GV-1, ID.GV-2

CURRENT ASSESSMENT

COST: \$\$\$\$

IMPACT: HIGH 

COMPLEXITY: LOW 

TTP OR RISK ADDRESSED:

Lack of accountability, investment, or effectiveness of OT cybersecurity program.

RECOMMENDED ACTION: A named role/position/title is identified as responsible and accountable for planning, resourcing, and execution of OT-specific cybersecurity activities. In some organizations this may be the same position as identified in 1.B.

DATE:

- IMPLEMENTED**
- IN PROGRESS**
- SCOPED**
- NOT STARTED**



1.C OT Cybersecurity Leadership

ID.GV-1, ID.GV-2

CURRENT ASSESSMENT

COST: \$\$\$\$ **IMPACT:** **HIGH** **COMPLEXITY:** **LOW**

TTP OR RISK ADDRESSED:

Lack of accountability, investment, or effectiveness of OT cybersecurity program.

RECOMMENDED ACTION: A named role/position/title is identified as responsible and accountable for planning, resourcing, and execution of OT-specific cybersecurity activities. In some organizations this may be the same position as identified in 1.B.

DATE:

- IMPLEMENTED**
- IN PROGRESS**
- SCOPED**
- NOT STARTED**



Questions?



CPG - Identity

1.A Asset Inventory

ID.AM-1, ID.AM-2, ID.AM-4,
DE.CM-1, DE.CM-7

COST: \$\$\$\$ **IMPACT:** **HIGH** **COMPLEXITY:** **MEDIUM**

TACTIC, TECHNIQUE, AND PROCEDURE (TTP) OR RISK ADDRESSED:

Hardware Additions (T1200)

Exploit Public-Facing Application (T0819, ICS T0819)

Internet-accessible device (ICS T0883)

RECOMMENDED ACTION: Maintain a regularly updated inventory of all organizational assets with an IP address (including IPv6), including OT. This inventory is updated on a recurring basis, no less than monthly for both IT and OT.

FREE SERVICES AND REFERENCES: [Cyber Hygiene Services](#), "[Stuff Off Search](#)" [Guide](#) or email vulnerability@cisa.DHS.gov



CPG - Identity

1.B Organizational Cybersecurity Leadership ID.GV-1, ID.GV-2

COST: \$\$\$\$

IMPACT: HIGH

COMPLEXITY: LOW

TTP OR RISK ADDRESSED:

Lack of sufficient cybersecurity accountability, investment, or effectiveness.

RECOMMENDED ACTION: A named role/position/title is identified as responsible and accountable for planning, resourcing, and execution of cybersecurity activities. This role may undertake activities, such as managing cybersecurity operations at the senior level, requesting and securing budget resources, or leading strategy development to inform future positioning.



CPG - Identity

1.E Mitigating Known Vulnerabilities

ID.RA-1, PR.IP-12,
DE.CM-8, RS.MI-3,
ID.RA-6, RS.AN-5

COST: \$\$\$\$ **IMPACT:** **HIGH** **COMPLEXITY:** **MEDIUM**

TTP OR RISK ADDRESSED:

Active Scanning - Vulnerability Scanning (T1595.002)
Exploit Public-Facing Application (T1190, ICS T0819)
Exploitation of Remote Service (T1210, ICS T0866)
Supply Chain Compromise (T1195, ICS T0862)
External Remote Services (T1133, ICS T0822)

RECOMMENDED ACTION: All known exploited vulnerabilities (listed in CISA's [KEV Catalog](#)) in internet-facing systems are patched or otherwise mitigated within a risk-informed span of time, prioritizing more critical assets first.

OT: For assets where patching is either not possible or may substantially compromise availability or safety, compensating controls are applied (e.g. segmentation, monitoring) and recorded. Sufficient controls either make the asset inaccessible from the public internet, or they reduce the ability of adversaries to exploit the vulnerabilities in these assets.



CPG - Identity

1.F Third-Party Validation of Cybersecurity Control Effectiveness

ID.RA-1, ID.RA-3,
ID.RA-4, ID.RA-5,
ID.RA-6

COST: \$\$\$\$ **IMPACT:** **HIGH** **COMPLEXITY:** **HIGH**

TTP OR RISK ADDRESSED:

Gaps in cyber defenses or a false sense of security in existing protections.

RECOMMENDED ACTION: Third parties with demonstrated expertise in (IT and/or OT) cybersecurity should regularly validate the effectiveness and coverage of an organization's cybersecurity defenses. These exercises, which may include penetration tests, bug bounties, incident simulations, or table-top exercises, should include both unannounced and announced tests.

Exercises consider both the ability and impact of a potential threat actor to infiltrate the network from the outside, as well as the ability of a threat actor within the network (e.g., "assume breach") to pivot laterally to demonstrate potential impact on critical systems, including operational technology and industrial control systems.

High-impact findings from previous tests are mitigated in a timely manner and are not re-observed in future tests.



CPG - Identity

1.G Supply Chain Incident Reporting

ID.SC-1, ID.SC-3

COST: \$\$\$\$

IMPACT: HIGH 

COMPLEXITY: LOW 

TTP OR RISK ADDRESSED:

Supply Chain Compromise (T1195, ICS T0862)

RECOMMENDED ACTION: Procurement documents and contracts, such as service-level agreements (SLAs), stipulate that vendors and/or service providers notify the procuring customer of security incidents within a risk-informed time frame, as determined by the organization.



CPG - Identity

1.H Supply Chain Vulnerability Disclosure

ID.SC-1, ID.SC-3

COST: \$\$\$\$

IMPACT: HIGH



COMPLEXITY: LOW



TTP OR RISK ADDRESSED:

Supply Chain Compromise (T1195, ICS T0862)

RECOMMENDED ACTION: Procurement documents and contracts, such as SLAs, stipulate that vendors and/or service providers notify the procuring customer of confirmed security vulnerabilities in their assets within a risk-informed time frame, as determined by the organization.



CPG - Protect

2.A Changing Default Passwords

PR.AC-1

COST: \$\$\$\$ **IMPACT:** **HIGH** **COMPLEXITY:** **MEDIUM**

TTP OR RISK ADDRESSED:

Valid Accounts - Default Accounts (T1078.001)

Valid Accounts (ICS T0859)

RECOMMENDED ACTION: An enforced organization-wide policy and/or process that requires changing default manufacturer passwords for any/all hardware, software, and firmware before putting 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, CISA still recommends 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 threat actor TTPs change.



CPG - Protect

2.B Minimum Password Strength

PR.AC-1

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: Organizations have a system-enforced policy that requires a minimum password length of 15* or more characters for all password-protected IT assets, and all OT assets where technically feasible.** Organizations should consider leveraging passphrases and password managers to make it easier for users to maintain sufficiently long passwords. In instances where minimum password lengths are not technically feasible, compensating controls are applied and recorded, and all login attempts to those assets are logged. Assets that cannot support passwords of sufficient strength length are prioritized for upgrade or replacement.

This goal is particularly important for organizations that lack widespread implementation of MFA and capabilities to protect against brute-force attacks (such as web application firewalls and third-party content delivery networks) or are unable to adopt passwordless authentication methods.

* Modern attacker tools can crack eight-character passwords quickly. Length is a more impactful and important factor in password strength than complexity or frequent password rotations. Long passwords are also easier for users to create and remember.

** OT assets that use a central authentication mechanism (such as Active Directory) are most important to address. Examples of low-risk OT assets that may not be technically feasible include those in remote locations, such as on offshore rigs or wind turbines.

CPG - Protect

2.D Revoking Credentials for Departing Employees

PR.AC-1,
PR.IP-11

COST: \$\$\$\$ **IMPACT:** MEDIUM **COMPLEXITY:** LOW

TTP OR RISK ADDRESSED:

Valid Accounts (T1078, ICS T0859)

RECOMMENDED ACTION: A defined and enforced administrative process applied to all departing employees by the day of their departure that (1) revokes and securely returns all physical badges, key cards, tokens, etc., and (2) disables all user accounts and access to organizational resources.



CPG - Protect

2.E Separating User and Privileged Accounts

PR.AC-4

COST: \$\$\$\$

IMPACT:

HIGH

COMPLEXITY:

LOW

TTP OR RISK ADDRESSED:

Valid Accounts (T1078, ICS T0859)

RECOMMENDED ACTION: No user accounts always have administrator or super-user privileges. Administrators maintain separate user accounts for all actions and activities not associated with the administrator role (e.g., for business email, web browsing). Privileges are reevaluated on a recurring basis to validate continued need for a given set of permissions.



CPG - Protect

2.H Phishing-Resistant

Multi-Factor Authentication (MFA)

PR.AC-7, PR.AC-1

COST: \$\$\$\$ **IMPACT:** **HIGH** **COMPLEXITY:** **MEDIUM**

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)

RECOMMENDED ACTION: Organizations implement MFA for access to assets using the strongest available method for that asset (see below for scope). MFA options sorted by strength, high to low, are as follows:

1. Hardware-based, phishing-resistant MFA (e.g., FIDO/WebAuthn or PKI-based - see CISA guidance in "Resources");
2. If such hardware-based MFA is not available, then mobile app-based soft tokens (preferably push notification with number matching) or emerging technology such as FIDO passkeys are used;
3. MFA via SMS or voice only used when no other options are possible.

IT: All IT accounts leverage MFA to access organizational resources. Prioritize accounts with highest risk, such as privileged administrative accounts for key IT systems.

OT: Within OT environments, MFA is enabled on all accounts and systems that can be accessed remotely, including vendors/maintenance accounts, remotely accessible user and engineering workstations, and remotely accessible human-machine interfaces (HMIs).

CPG - Protect

2.1 Basic Cybersecurity Training

PR.AT-1

COST: \$\$\$\$

IMPACT: HIGH 

COMPLEXITY: LOW 

TTP OR RISK ADDRESSED:

User Training (M1017, ICS M0917)

RECOMMENDED ACTION: At least annual trainings for all organizational employees and contractors that cover basic security concepts, such as phishing, business email compromise, basic operational security (OPSEC), password security, etc., as well as foster an internal culture of security and cyber awareness.

New employees receive initial cybersecurity training within 10 days of onboarding and recurring training on at least an annual basis.



CPG - Protect

2.L Secure Sensitive Data

PR.DS-1, PR.DS-5

COST: \$\$\$\$ **IMPACT:** **HIGH** **COMPLEXITY:** **MEDIUM**

TTP OR RISK ADDRESSED:

- Unsecured Credentials (T1552)
- Steal or Forge Kerberos Tickets (T1558)
- OS Credential Dumping (T1003)
- Data from Information Repositories (ICS T0811)
- Theft of Operational Information (T0882)

RECOMMENDED ACTION: Sensitive data, including credentials, are not stored in plaintext anywhere in the organization and can only be accessed by authenticated and authorized users. Credentials are stored in a secure manner, such as with a credential/password manager or vault, or other privileged account management solution.



CPG - Protect

2.R System Backups

PR.IP-4

COST: \$\$\$\$ **IMPACT:** **HIGH** **COMPLEXITY:** **MEDIUM**

TTP OR RISK ADDRESSED:

Data Destruction (T1485, ICS T0809)
Data Encrypted for Impact (T1486)
Disk Wipe (T1561)
Inhibit System Recovery (T1490)
Denial of Control (ICS T0813)
Denial/Loss of View (ICS T0815, T0829)
Loss of Availability (T0826)
Loss/Manipulation of Control (T0828, T0831)

RECOMMENDED ACTION: All systems that are necessary for operations are backed up on a regular cadence, no less than once per year.

Backups are stored separately from the source systems and tested on a recurring basis, no less than once per year. Stored information for OT assets includes at a minimum: configurations, roles, PLC logic, engineering drawings, and tools.



CPG - Protect

2.S Incident Response (IR) Plans

PR.IP-9, PR.IP-10

COST: \$\$\$\$

IMPACT: HIGH

COMPLEXITY: LOW

TTP OR RISK ADDRESSED:

Inability to quickly and effectively contain, mitigate, and communicate about cybersecurity incidents.

RECOMMENDED ACTION: Organizations have, maintain, update, and regularly drill IT and OT cybersecurity incident response plans for both common and organization-specific (e.g., by sector, locality) threat scenarios and TTPs. When conducted, tests or drills are as realistic as feasible. IR plans are drilled at least annually and are updated within a risk-informed time frame following the lessons learned portion of any exercise or drill.



CPG - Protect

2.U Secure Log Storage

PR.PT-1

COST: \$\$\$\$

IMPACT: HIGH 

COMPLEXITY: LOW 

TTP OR RISK ADDRESSED:

Indicator Removal on Host - Clear Windows Event Logs (T1070.001)

Indicator Removal on Host - Clear Linux or Mac System Logs (T1070.002)

Indicator Removal on Host - File Deletion (T1070.004)

Indicator Removal on Host (ICS T0872)

RECOMMENDED ACTION: Logs are stored in a central system, such as a security information and event management (SIEM) tool or central database, and can only be accessed or modified by authorized and authenticated users. Logs are stored for a duration informed by risk or pertinent regulatory guidelines.



CPG - Respond

4.A Incident Reporting

RS.CO-2, RS.CO-4

COST: \$\$\$\$

IMPACT:

HIGH



COMPLEXITY:

LOW



TTP OR RISK ADDRESSED:

Without timely incident reporting CISA and other groups are less able to assist affected organizations and lack critical insight into the broader threat landscape (such as whether a broader attack is occurring against a specific sector).

RECOMMENDED ACTION: Organizations maintain codified policy and procedures on to whom and how to report all confirmed cybersecurity incidents to appropriate external entities (e.g., state/federal regulators or SRMAs as required, ISAC/ISAO, as well as CISA).

Known incidents are reported to CISA and other necessary parties within time frames directed by applicable regulatory guidance or in the absence of guidance, as soon as safely capable. This goal will be revisited following full implementation of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCA).



CPG - Recover

5.A Incident Planning and Preparedness

RC.RP-1, R.IP-9,
PR.IP-10

COST: \$\$\$\$ **IMPACT:** MEDIUM **COMPLEXITY:** LOW

TTP OR RISK ADDRESSED:

Disruption to availability of an asset, service, or system

RECOMMENDED ACTION: Develop, maintain, and execute plans to recover and restore to service business or mission-critical assets or systems that might be impacted by a cybersecurity incident.



CSET Tools Resource Library

Prepare Assessment Results

- Home
- Prepare
 - Assessment Configuration
 - Assessment Information
- Assessment
 - Security Practices
- Results
 - Performance Summary
 - Security Practice Checklist
 - Reports**
 - Feedback

Reports

Thank you for completing your assessment. The reports on this page capture organization's cybersecurity planning and growth going forward. The assessment is updated as you complete the assessment. Any reports run prior to that update may not reflect the current state of the assessment.

[Observations Tear-Out Sheets](#)

CISA Cybersecurity Performance Goals (CPG)

[CPG Report](#)

[CPG Deficiency](#)

Export

Reports and Summary

Questions?





Rachael Han

Regional Analyst
Region II (NY, NJ, PR, USVI)

Rachael.Han@cisa.dhs.gov

(202) 394-6453

Jon Easton

Cybersecurity Advisor
Region II (NY, NJ, PR, USVI)

Jonathan.Easton@cisa.dhs.gov

(771) 217-0640

