CYBERSECURITY SERVICES FOR BUILDING CYBER RESILIENCE

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

Eddie Harmon
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.

CISA
CYBERSECURITY SERVICES

Range of Cybersecurity Assessments

- Cyber Resilience Review (Strategic)
- External Dependencies Management (Strategic)
- Cyber Infrastructure Survey (Strategic)
- Cybersecurity Evaluations Tool Strategic/Technical)
- Vulnerability Scanning / Hygiene (Technical)
- Risk and Vulnerability Assessment (Technical)
- Remote Penetration Test (Technical)

Remote Penetration Testing

SCENARIOS

- **External Penetration Test:** Verifying if the stakeholder network is accessible from the public domain by an unauthorized user by assessing open ports, protocols, and services.
- **External Web Application Test:** Evaluating web applications for potential exploitable vulnerabilities; the test can include automated scanning, manual testing, or a combination of both methods.
- **Phishing Assessment:** Testing the stakeholder email infrastructure through carefully crafted phishing emails containing a variety of malicious payloads to the trusted point of contact.
- **Open-Source Information Gathering:** Identify publicly available information about the stakeholder environment which may be useful in preparing for an attack.

ASSESSMENT OBJECTIVES

- Conduct assessments to identify vulnerabilities and work with customers to eliminate exploitable pathways.
- Simulate the tactics and techniques of real-world threats and malicious adversaries.
- Test centralized data repositories and externally accessible assets/resources.
- Avoid causing disruption to the customer's mission, operation, and network infrastructure.

ASSESSMENT TIMELINE

Pre-Planning
- Request RPT
- Receive RPT Capabilities Brief
- Sign and return RPT Rules of Engagement
- Determine RPT services, scope, and logistics during pre-assessment call(s)

Planning
- Confirm schedule
- Establish trusted points of contact

Execution (Up to Six Weeks)
- Dependent on resource availability
- Critical findings are immediately disclosed

Reporting
- Briefing and initial recommendations
- Final report review and receipt – 10 days

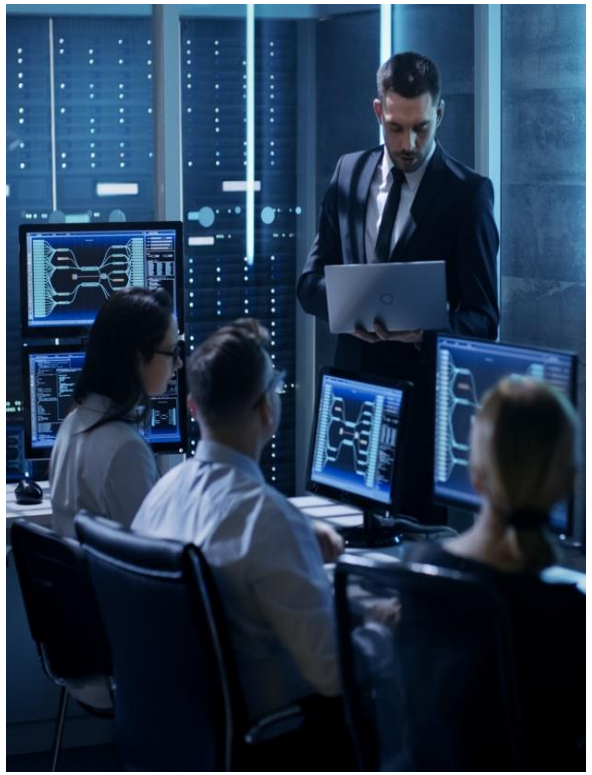
Validated Architecture Design Review

Purpose: Analyze network architecture, system configurations, log file review, network traffic and data flows to identify abnormalities in devices and communications traffic.

Delivery: CISA staff working with entity staff

Benefits:

- In-depth review of network and operating system
- Recommendations to improve an organization's operational maturity and enhancing their cybersecurity posture
- Evaluation of network architecture



Vulnerability Scanning

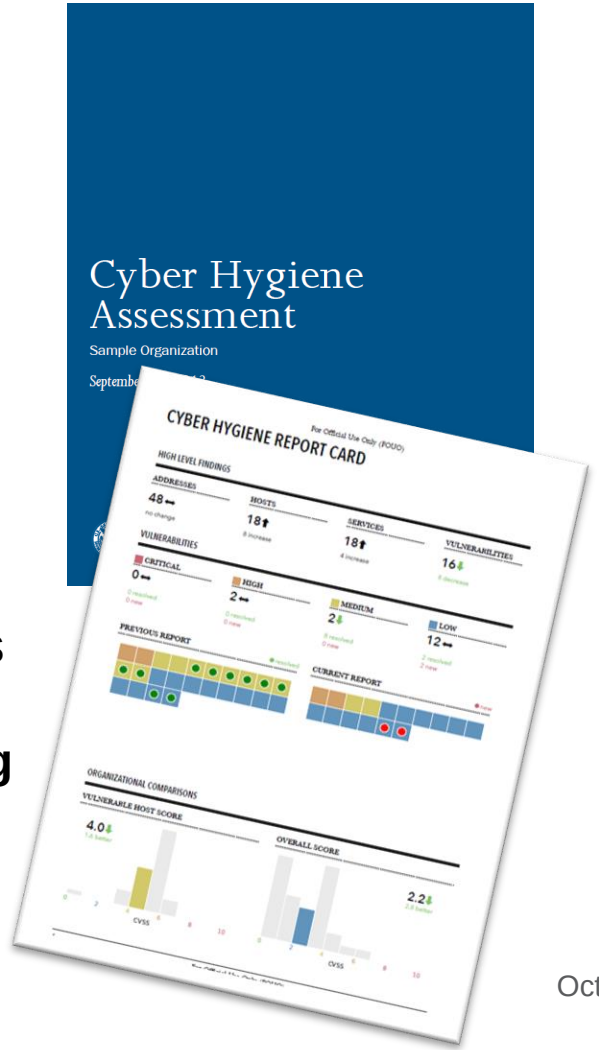
Purpose: Assess Internet-accessible systems for known vulnerabilities and configuration errors.

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



Cyber Exercises and Planning

CISA's National Cyber Exercise and Planning Program develops, conducts, and evaluates cyber exercises and planning activities for state, local, tribal and territorial governments and public and private sector critical infrastructure organizations.

- Cyber Storm Exercise – DHS's flagship national-level biennial exercise
- Exercise Planning and Conduct
- Cyber Exercise Consulting and Subject Expertise Support
- Cyber Planning Support
- Off-the-Shelf Resources
- Exercise-In-A-Box

https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

CISA Tabletop Exercise Packages

CISA Tabletop Exercise Packages (CTEPs) are a comprehensive set of resources designed to assist stakeholders in conducting their own exercises.

Each package is customizable and includes template exercise objectives, scenarios, and discussion questions as well as a collection of references and resources.

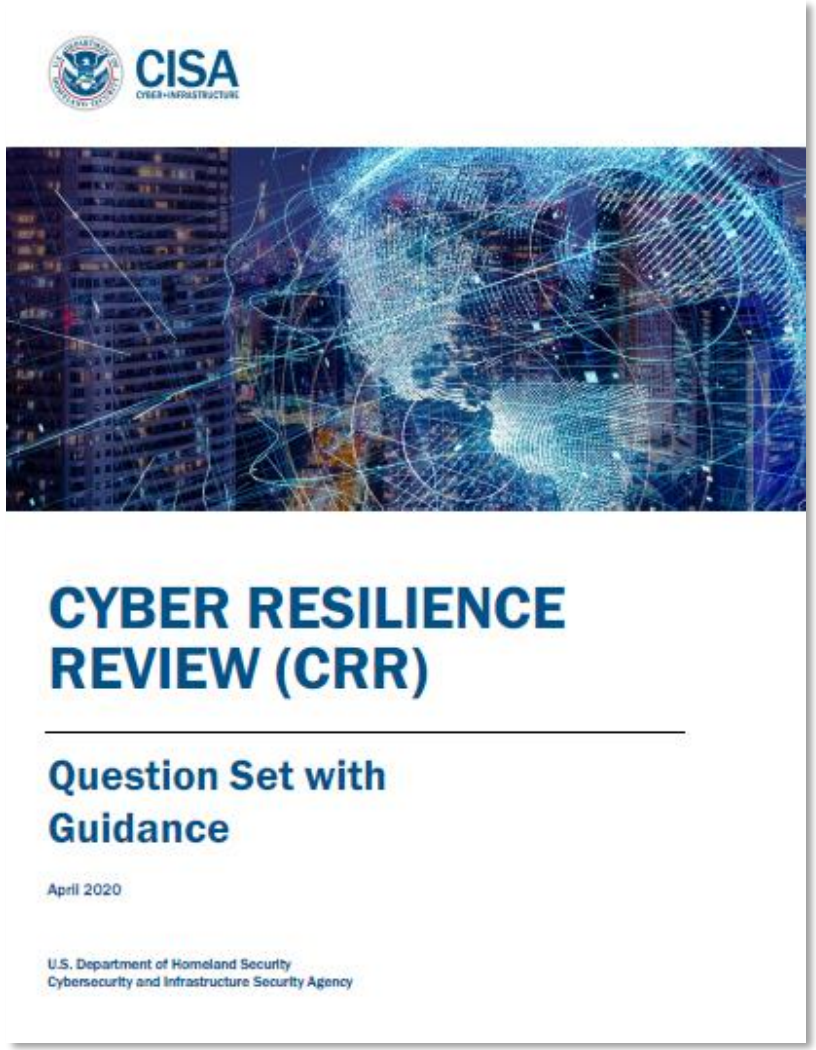
Resource Name
Chemical Sector CTEP Situation Manual - November 2023
Commercial Facilities CTEP Situation Manual - November 2023
Communications CTEP Situation Manual - February 2024
Critical Manufacturing CTEP Situation Manual - November 2023
Cyber Insider Threat CTEP Situation Manual - September 2023
Dams Sector CTEP Situation Manual - March 2024
Defense Industrial Base CTEP Situation Manual - July 2024
Early Voting CTEP Situation Manual - January 2024
Elections Vote by Mail CTEP Situation Manual - January 2024
Elections Voting Machine Compromise CTEP Situation Manual - January 2024
Electricity Subsector CTEP Situation Manual - July 2024

Cyber Resilience Review

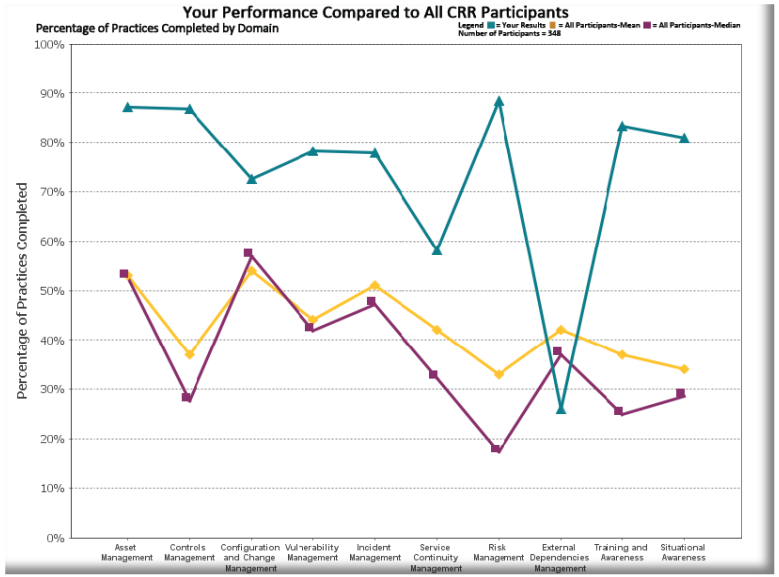
- **Purpose:** Evaluates that maturity of an organization's capacities and capabilities in performing, planning, managing, measuring, and defining cybersecurity capabilities across the following 10 domains:

Asset Management	Service Continuity Management
Controls Management	Risk Management
Configuration and Change Management	External Dependency Management
Vulnerability Management	Training and Awareness
Incident Management	Situational Awareness

- Benefits include: Helps public and private sector partners understand and measure cybersecurity capabilities as they relate to operational resilience and cyber risk



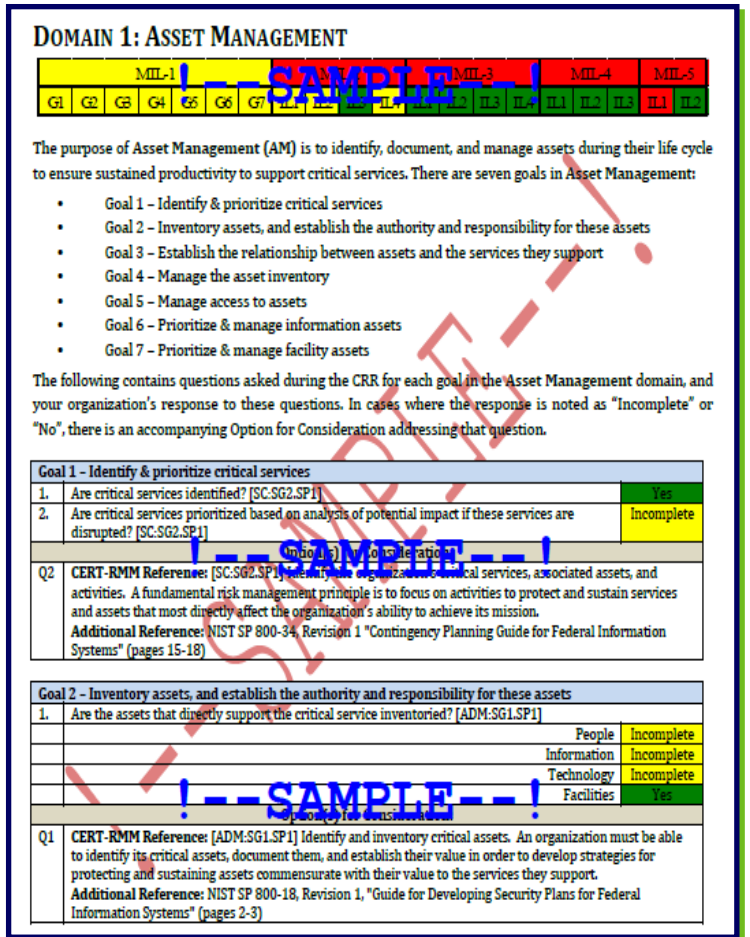
CRR Sample Report



Comparison data with other CRR participants
**facilitated only*

A summary "snapshot" graphic, related to the **NIST Cyber Security Framework**.

Domain performance of existing cybersecurity capability and options for consideration for all responses



DOMAIN 1: ASSET MANAGEMENT

MIL-1							MIL-3				MIL-4			MIL-5	
G1	G2	G3	G4	G5	G6	G7									

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)	

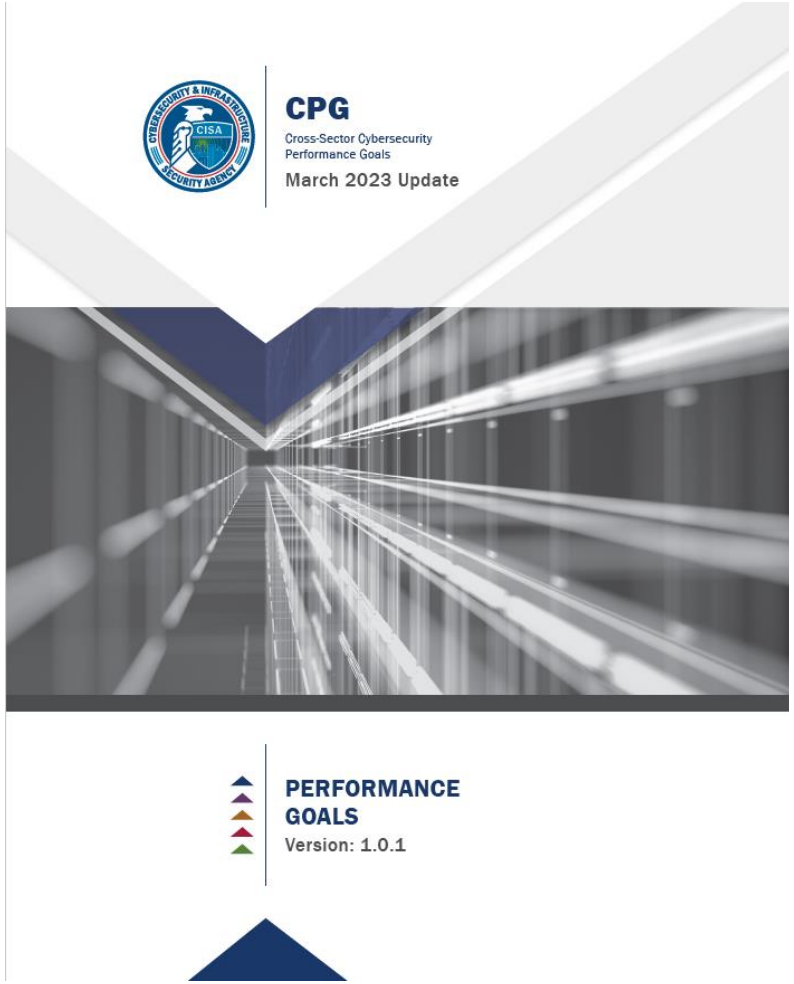
Ransomware Readiness Assessment

- **Ransomware Readiness Assessment:** 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.
- **Facilitated:** Self-Administered, undertaken independently
- **Benefits**:
- 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.

[CISA's CSET Tool Sets Sights on Ransomware Threat | CISA]

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.

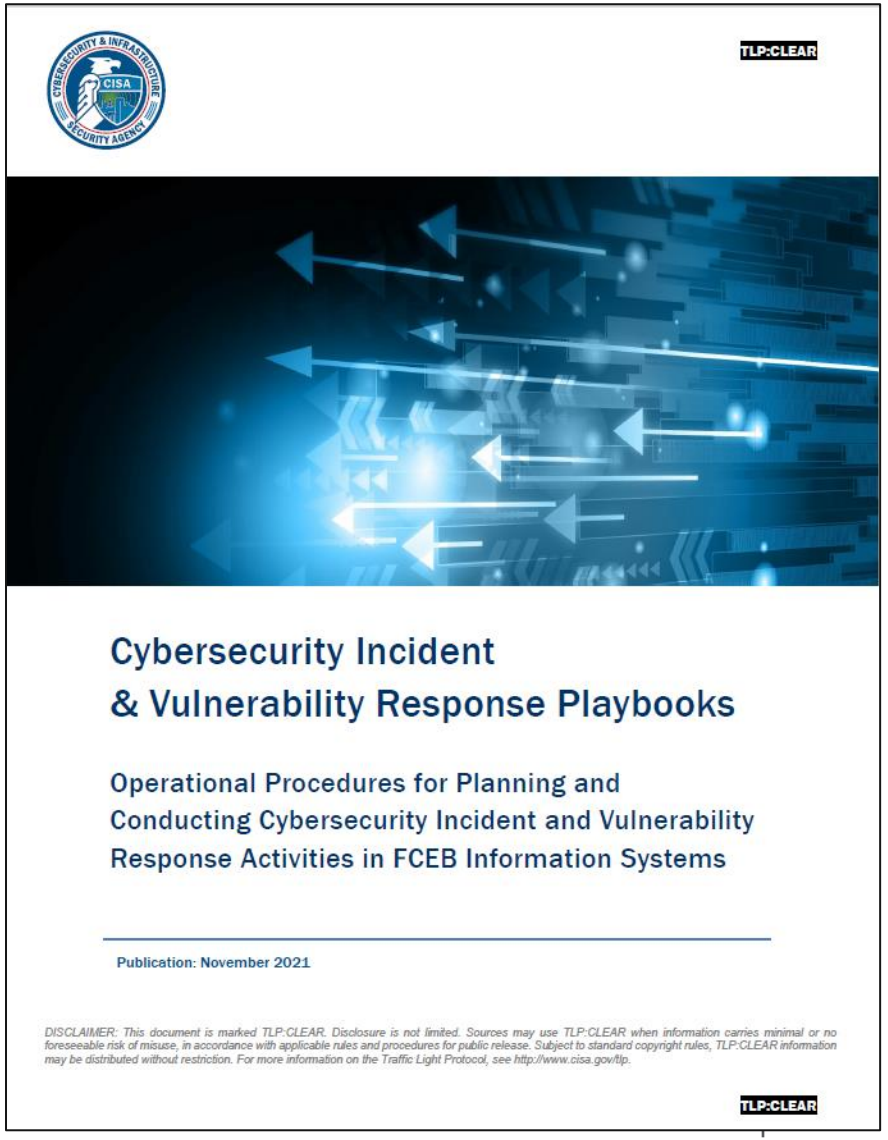


Incident / Vulnerability Response Playbooks

Incident Response playbook: provides a standardized response process for cybersecurity incidents and describes the process and completion through the incident response phases as defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61 Rev. 2,5

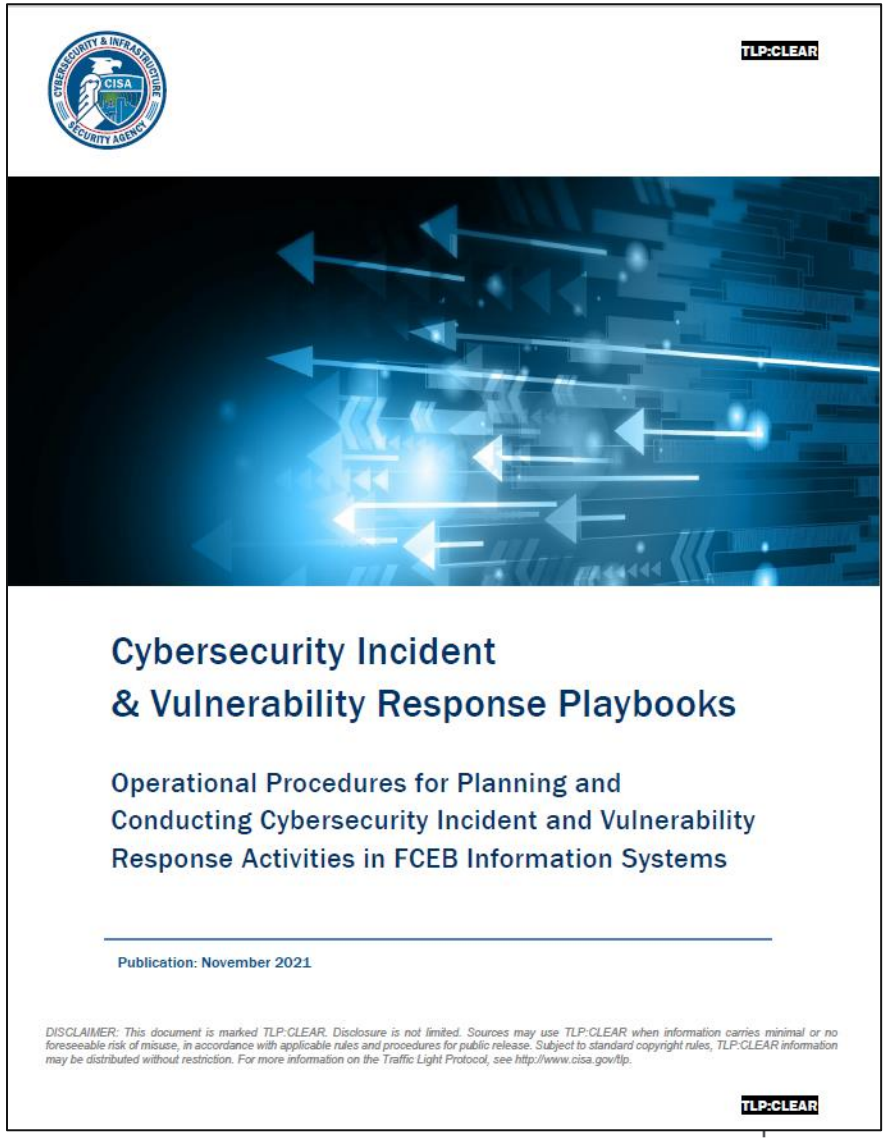
Vulnerability Response playbook: standardizes the high-level process that that is observed to be used by agencies should follow when responding to these urgent and adversaries to gain unauthorized high priority vulnerabilities

https://www.cisa.gov/resources-tools/resources/federal-government-cybersecurity-incident-and-vulnerability-response-playbooks



Incident / Vulnerability Response Playbooks

Step	Incident Response Procedure	Action Taken	Date Completed
	Detection & Analysis		
1. Declare Incident			
1a.	Perform initial categorization of incident.[34]		
1b.	Designate agency incident coordination lead.		
1c.	Notify CISA and, if applicable, law enforcement.		
1d.	Designate CISA reporting POCs and provide information for both primary and secondary POCs, to include names, phone numbers, and email addresses, to CISA for appropriate coordination.		
2. Determine Investigation Scope			
2a.	Identify the type and extent of the incident.		
2b.	Assess operational or informational impact on organization's mission.		
3. Collect and Preserve Data			
3a.	Collect and preserve the data necessary for incident verification, categorization, prioritization, mitigation, reporting, attribution, and as potential evidence in accordance with NIST 800-61r2.		



CISA SCuBA Secure Configuration Baselines

Detailed, **product-specific guidance** on configuring agency cloud environments to meet the minimum-security recommendations. Cloud Security Provider suites are open to vulnerabilities if misconfigured. Current baselines efforts are centered around M365 and GWS products.

Microsoft 365 Applications

- ✓ Azure Active Directory
- ✓ Defender for Office 365
- ✓ Exchange Online
- ✓ Power BI
- ✓ Power Platform
- ✓ SharePoint Online + OneDrive for Business
- ✓ Teams

Google Workspace Applications

- ✓ Gmail
- ✓ Common Controls
- ✓ Drive/Docs
- ✓ Meet
- ✓ Chat and Classic Hangouts
- ✓ Calendar
- ✓ Groups for Business
- ✓ Sites
- ✓ Classroom

ScubaGear & ScubaGoggles Overview

- The Microsoft 365 (M365) SCBs were published on October 20, 2022. Pilot engagements and RFC comments informed key improvements made to the security configuration guidance and ScubaGear tool. The SCBs and ScubaGear tool can be found on GitHub - ScubaGear.
- On December 6, 2023, the SCuBA team published the initial draft of the Google Workspace (GWS) Secure Configuration Baselines (SCBs) and GWS assessment tool, ScubaGoggles, for public comment on GitHub – ScubaGoggles.
- Both tools:
  - **Compare tenant configurations** to CISA's security recommendations.*
  - **Lower the amount of effort** required for entities to assess themselves, providing a detailed report.
  - Have code updates that will be **released on a regular basis** to address Google's and Microsoft's configuration updates.
  - Ability for CISA to have **real-time visibility into tenant configuration via ScubaConnect** .

As of 10/15/2024

By the Numbers

M365

- 7 Secure Configuration Baselines
- Over 1,600 GitHub Stars
- 24,316 downloads of v1.3.0
- 30K+ total downloads across all releases

GWS

- 9 Secure Configuration Baselines
- 151 Policy Control Statements
- 2 releases
- Over 150 GitHub Stars
- 400+ total downloads across all releases

*GWS SCB guidance does not cover Google services outside of GWS (e.g., Maps, Photos), or any GWS Marketplace Apps created by 3rd Party developers

Introducing 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

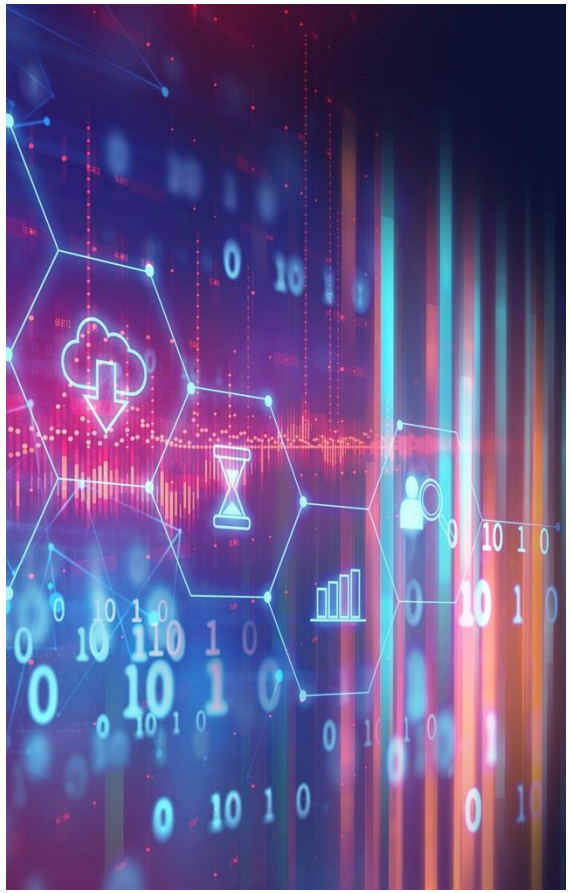
- User-friendly instructions for downloading and installing LME are available at LME's GitHub Repo
- LME's instructions provide detailed steps organized by chapters and explain how the tool uses endpoint agents for thorough event data collection and analysis.

Jon Easton

Contact LME: CSSO Email | LME's GitHub Repo

Cyber Security Evaluation Tool (CSET)

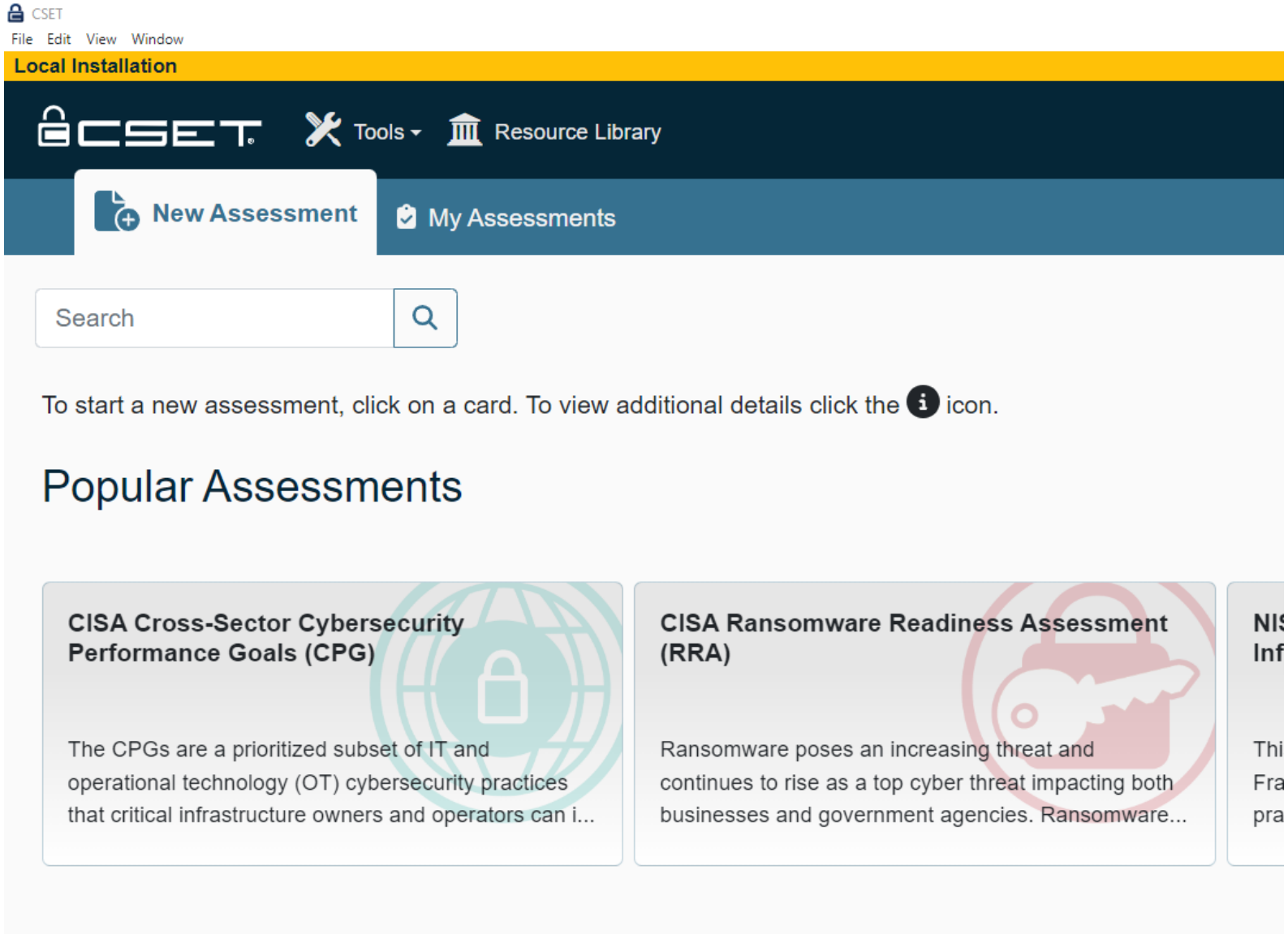
- **Purpose:** Assesses control system and information technology network security practices against industry standards.
- **Facilitated:** Self-Administered, undertaken independently
- **Benefits:**
  - Immediately available for download upon request
  - Understanding of operational technology and information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



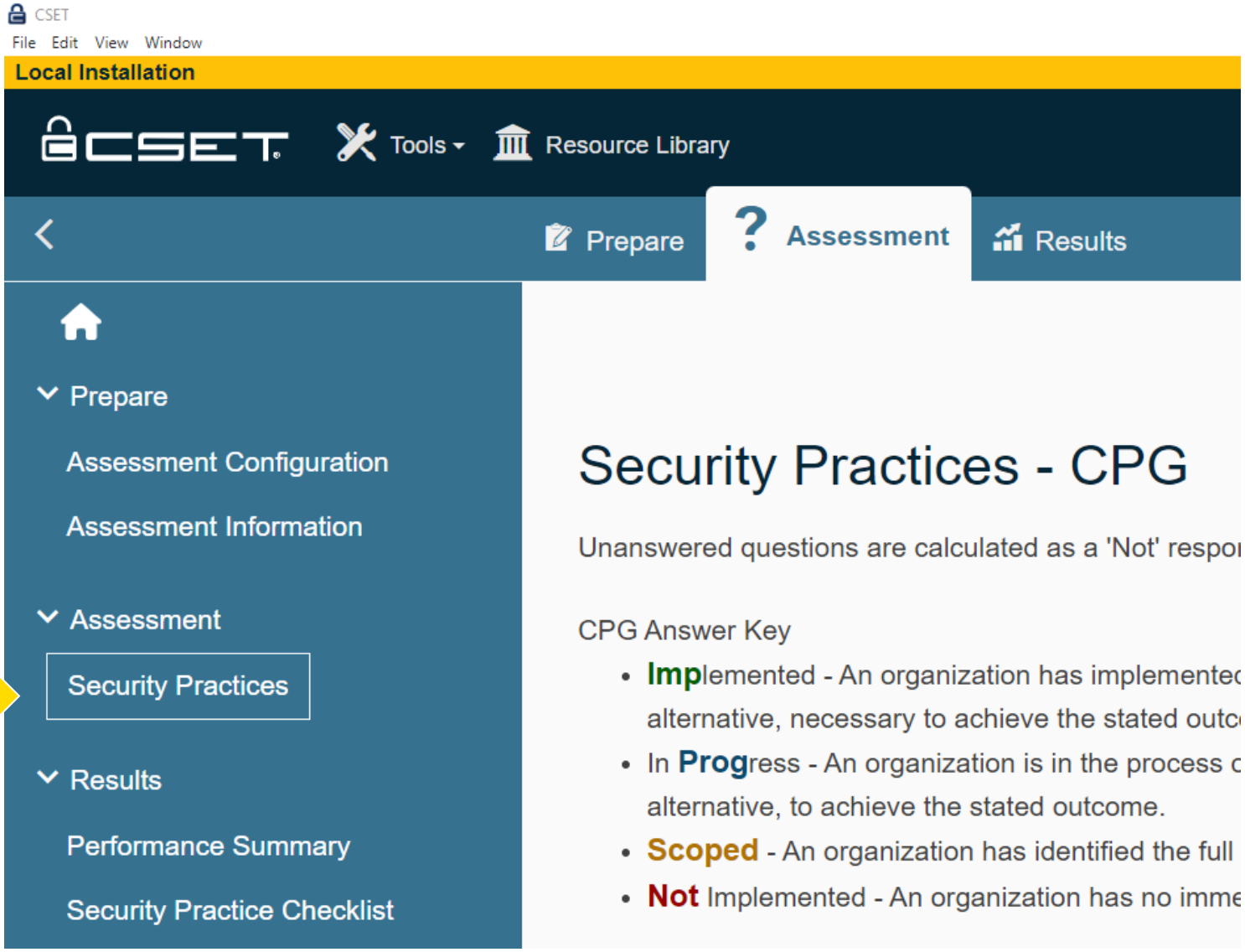
https://github.com/cisagov/cset/releases

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

CSET CPG


CSET
File Edit View Window
Local Installation
CSET
Tools
Resource Library
New Assessment
My Assessments
Search
To start a new assessment, click on a card. To view additional details click the 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 i...
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...

Assessment Items (Goals)



Format in CSET

1.C **Security Practice**

OT Cybersecurity Leadership

Imp | Prog | Scoped | Not

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 Cybsersecurity 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

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/

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.C OT Cybersecurity Leadership — ID.GV-1, ID.GV-2

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

TTP OR RISK ADDRESSED:

Lack of accountability, investment, or effectivness 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.

CPG - Identity

1.D Improving IT and OT Cybersecurity Relationships **ID.GV-2, PR.AT-5**

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

TTP OR RISK ADDRESSED:

Poor working relationships and a lack of mutual understanding between IT and OT cybersecurity can often result in increased risk for OT cybersecurity.

RECOMMENDED ACTION: Organizations sponsor at least one "pizza party" or equivalent social gathering per year that is focused on strengthening working relationships between IT and OT security personnel, and is not a working event (such as providing meals during an incident response).

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 - Identity

1.I Vendor/Supplier Cybersecurity Requirements ID.SC-3

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

TTP OR RISK ADDRESSED:

Supply Chain Compromise (T1195, ICS T0862)

RECOMMENDED ACTION: Organizations' procurement documents include cybersecurity requirements and questions, which are evaluated in vendor selection such that, given two offerings of roughly similar cost and function, the more secure offering and/or supplier is preferred.

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.C Unique Credentials — PR.AC-1

COST: $$$$ **IMPACT:** MEDIUM **COMPLEXITY:** MEDIUM

TTP OR RISK ADDRESSED:

Valid Accounts (T1078, ICS T0859)

Brute Force - Password Guessing (T1110.001)

RECOMMENDED ACTION: Organizations provision unique and separate credentials for similar services and asset access on IT and OT networks. Users do not (or cannot) reuse passwords for accounts, applications, services, etc. Service accounts/machine accounts have unique passwords from all member user accounts.

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.F Network Segmentation — PR.AC-5, PR.PT-4

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

TTP OR RISK ADDRESSED:

Network Service Discovery (T1046)

Trusted Relationship (T1199)

Network Connection Enumeration (ICS T0840)

Network Sniffing (T1040, ICS T0842)

RECOMMENDED ACTION: All connections to the OT network are denied by default unless explicitly allowed (e.g., by IP address and port) for specific system functionality. Necessary communications paths between the IT and OT networks must pass through an intermediary, such as a properly configured firewall, bastion host, "jump box," or a demilitarized zone, which is closely monitored, captures network logs, and only allows connections from approved assets.

CPG - Protect

2.G Detection of Unsuccessful (Automated) Login Attempts — PR.AC-7

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 in a 10-minute period.

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.I 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.J OT Cybersecurity Training — PR.AT-2, PR.AT-3, PR.AT-5

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

TTP OR RISK ADDRESSED:

User Training (M1017, ICS M0917)

RECOMMENDED ACTION: In addition to basic cybersecurity training, personnel who maintain or secure OT as part of their regular duties receive OT-specific cybersecurity training on at least an annual basis.

CPG - Protect

2.K Strong and Agile Encryption — PR.DS-2

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

TTP OR RISK ADDRESSED:

Threat actor-in-the-Middle (T1557)

Automated Collection (T1119)

Network Sniffing (T1040, ICS T0842)

Wireless Compromise (ICS T0860)

Wireness Sniffing (ICS T0887)

RECOMMENDED ACTION: Properly configured and up-to-date transport layer security (TLS) is utilized to protect data in transit, when technically feasible. Organizations should also plan to identify any use of outdated or weak encryption, update these to sufficiently strong algorithms, and consider managing implications of post-quantum cryptography.

OT: To minimize the impact to latency and availability; encryption is used where feasible, usually for OT communications connecting with remote/external assets.

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.M Email Security — PR.DS-5, PR.AC-7

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

TTP OR RISK ADDRESSED:

Phishing (T1566)

Business Email Compromise

RECOMMENDED ACTION: On all corporate email infrastructure (1) STARTTLS is enabled, (2) SPF and DKIM are enabled, and (3) DMARC is enabled and set to "reject." For further examples and information, see CISA's past guidance for federal agencies.

CPG - Protect

2.N Disable Macros by Default — PR.IP-1, PR.IP-3

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

TTP OR RISK ADDRESSED:

Phishing - Spearphishing Attachment (T1566.001)

User Execution - Malicious FIle (T1204.002)

RECOMMENDED ACTION: A system-enforced policy that disables Microsoft Office macros, or similar embedded code, by default on all devices. If macros must be enabled in specific circumstances, there is a policy for authorized users to request that macros are enabled on specific assets.

CPG - Protect

2.0 Document Device Configurations PR.IP-1

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

TTP OR RISK ADDRESSED:

Delayed, insufficient, or incomplete ability to maintain or restore functionality of critical devices and service operations.

RECOMMENDED ACTION: Organizations maintain accurate documentation describing the baseline and current configuration details of all critical IT and OT assets to facilitate more effective vulnerability management and response and recovery activities. Periodic reviews and updates are performed and tracked on a recurring basis.

CPG - Protect

2.P Document Network Topology — PR.IP-1, ID.AM-3

COST: $$$$ **IMPACT:** MEDIUM **COMPLEXITY:** MEDIUM

TTP OR RISK ADDRESSED:

Incomplete or inaccurate understanding of network topology inhibits effective incident response and recovery.

RECOMMENDED ACTION: Organizations maintain accurate documentation describing updated network topology and relevant information across all IT and OT networks. Periodic reviews and updates should be performed and tracked on a recurring basis.

CPG - Protect

2.Q Hardware and Software Approval Process PR.IP-3

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

TTP OR RISK ADDRESSED:

Supply Chain Compromise (T1195, ICS T0862)

Hardware Additions (T1200)

Browser Extensions (T1176)

Transient Cyber Asset (ICS T0864)

RECOMMENDED ACTION: Implement an administrative policy or automated process that requires approval before new hardware, firmware, or software/ software version is installed or deployed. Organizations maintain a risk-informed allowlist of approved hardware, firmware, and software that includes specification of approved versions, when technically feasible. For OT assets specifically, these actions should also be aligned with defined change control and testing activities.

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.T Log Collection — PR.PT-1

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

TTP OR RISK ADDRESSED:

Delayed, insufficient, or incomplete ability to detect and respond to potential cyber incidents.

Impair Defenses (T1562)

RECOMMENDED ACTION: Access- and security-focused (e.g., IDS/IDPS, firewall, DLP, VPN) logs are collected and stored for use in both detection and incident response activities (e.g., forensics). Security teams are notified when a critical log source is disabled, such as Windows Event Logging.

OT: For OT assets where logs are non-standard or not available, network traffic and communications to and from logless assets is collected.

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 - Protect

2.V Prohibit Connection of Unauthorized Devices PR.PT-2

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

TTP OR RISK ADDRESSED:

Hardware Additions (T1200)

Replication Through Removable Media (T1091, ICS T0847)

RECOMMENDED ACTION: Organizations maintain policies and processes to ensure that unauthorized media and hardware are not connected to IT and OT assets, such as by limiting use of USB devices and removable media or disabling AutoRun.

OT: When feasible, establish procedures to remove, disable, or otherwise secure physical ports to prevent the connection of unauthorized devices, or establish procedures for granting access through approved exceptions.

CPG - Protect

2.W No Exploitable Services on the Internet — PR.AC-3

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

TTP OR RISK ADDRESSED:

Active Scanning - Vulnerability Scanning (T1595.002)

Exploit Public-Facing Application (T1190, ICS T0819)

Exploitation of Remote Service (T1210, ICS T0866)

External Remote Services (T1133, ICS T0822)

Remote Services - Remote Desktop Protocol (T1021.001)

RECOMMENDED ACTION: Assets on the public internet expose no exploitable services, such as RDP. Where these services must be exposed, appropriate compensating controls are implemented to prevent common forms of abuse and exploitation. All unnecessary OS applications and network protocols are disabled on internet-facing assets.

CPG - Protect

2.X Limit OT Connections to Public Internet PR.PT-4

COST: $$$$ **IMPACT:** MEDIUM **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)

External Remote Services (T1133, ICS T0822)

RECOMMENDED ACTION: No OT assets are on the public internet, unless explicitly required for operation. Exceptions must be justified and documented, and excepted assets must have additional protections in place to prevent and detect exploitation attempts (e.g., logging, MFA, mandatory access via proxy or other intermediary).

CPG - Detect

3.A Detecting Relevant Threats and TTPs	ID.RA-2, ID.RA-3, DE.CM-1

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

TTP OR RISK ADDRESSED:

Without the knowledge of relevant threats and ability to detect them, organizations risk that threat actors may exist in their networks undetected for long periods.

RECOMMENDED ACTION: Organizations have documented a list of threats and cyber threat actor TTPs relevant to their organization (for example, based on industry, sectors, etc.), and have the ability (such as via rules, alerting, or commercial prevention and detection systems) to detect instances of those key threats.

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 Infrastrcuture Act of 2022 (CIRCIA).

CPG - Respond

4.B Vulnerability Disclosure/Reporting RS.AN-5

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

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)

RECOMMENDED ACTION: Consistent with NIST SP 800-53 Revision 5, organizations maintain a public, easily discoverable method for security researchers to notify (e.g., via email address or web form) organizations' security teams of vulnerable, misconfigured, or otherwise exploitable assets. Valid submissions are acknowledged and responded to in a timely manner, taking into account the completeness and complexity of the vulnerability. Validated and exploitable weaknesses are mitigated consistent with their severity.

Security researchers sharing vulnerabilities discovered in good faith are protected under Safe Harbor rules.

In instances where vulnerabilities are validated and disclosed, public acknowledgement is given to the researcher who originally submitted the notification.

CPG - Respond

4.C Deploy Security.txt Files — RS.AN-5

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

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)

RECOMMENDED ACTION: All public-facing web domains have a security.txt file that conforms to the recommendations in RFC 9116.

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.

Reports and Summary

Jon Easton
Cybersecurity Advisor
Region II (NY, NJ, PR, USVI)
Jonathan.Easton@cisa.dhs.gov
(771) 217-0640


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY