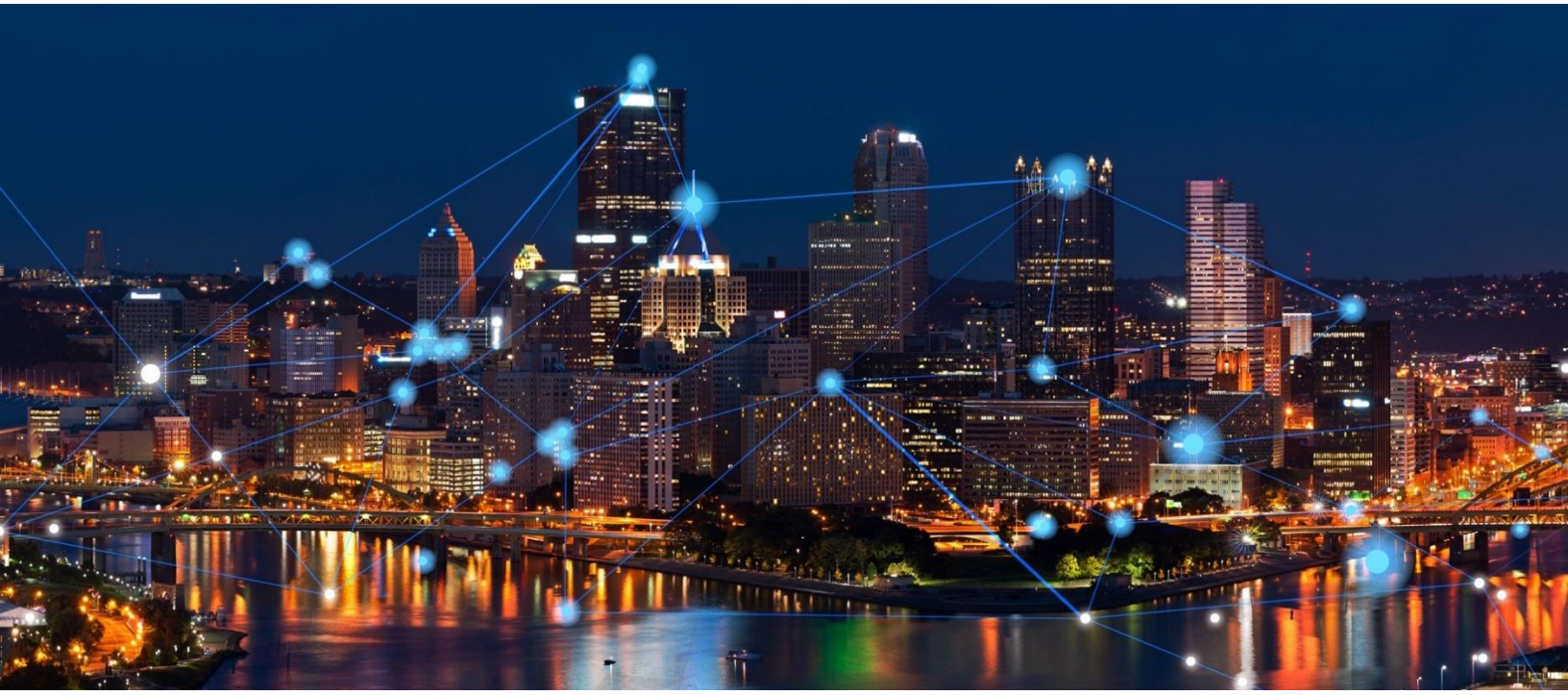


Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators

Publication: August 13, 2025

U.S. Cybersecurity and Infrastructure Security Agency
U.S. Environmental Protection Agency
U.S. National Security Agency
U.S. Federal Bureau of Investigation
Australian Signals Directorate's Australian Cyber Security Centre
Canadian Centre for Cyber Security
Germany's Federal Office for Information Security
Netherlands' National Cyber Security Centre
New Zealand's National Cyber Security Centre

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see Traffic Light Protocol (TLP) Definitions and Usage.

Executive Summary

When building a modern defensible architecture, it is essential for operational technology (OT) owners and operators across all critical infrastructure sectors to create an OT asset inventory supplemented by an OT taxonomy. Using these tools helps owners and operators identify which assets in their environment should be secured and protected, and structure their defenses accordingly to reduce the risk a cybersecurity incident poses to the organization's mission and service continuity.

An asset inventory is an organized, regularly updated list of an organization's systems, hardware, and software. For OT environments, a key part of creating an asset inventory is developing an OT taxonomy: a categorization system that organizes and prioritizes OT assets, aids in risk identification, vulnerability management, and incident response by classifying assets based on function and criticality.

This guidance outlines a process for OT owners and operators to create an asset inventory and OT taxonomy. This process includes defining scope and objectives for the inventory, identifying assets, collecting attributes, creating a taxonomy, managing data, and implementing asset life cycle management. These steps define a thorough and systematic approach to creating and maintaining an OT asset inventory and OT taxonomy, enabling organizations to maintain an accurate and up-to-date record of their OT assets.

Furthermore, this guidance outlines how OT owners and operators can maintain, improve, and use their asset inventory to protect their most vital assets. Steps include OT cybersecurity and risk management, maintenance and reliability, performance monitoring and reporting, training and awareness, and continuous improvement. By addressing these areas, organizations can enhance their overall security posture and ensure the reliability and safety of their OT environments.

To illustrate real world examples of OT taxonomies, CISA developed conceptual taxonomies through working sessions with organizations in the Energy Sector and Water and Wastewater Sector (see **Appendix B: Taxonomy for Oil and Gas Organizations**, **Appendix C: Taxonomy for Electricity Organizations**, and **Appendix D: Water and Wastewater**). These are not authoritative taxonomies for these sectors but are meant to help guide sector-specific organizations develop their own asset classification systems.

Table of Contents

Introduction

Operational technology (OT) includes a broad set of technologies that covers process automation, instrumentation, cyber-physical operations, and industrial control systems (ICS). Many OT systems are increasingly connected to business operations and applications that rely on process data and trends analysis for operations. If not assembled and integrated securely, these connections can introduce paths for cyber actors to move between networks.

OT is vital to critical infrastructure services like energy production and distribution, as well as water and wastewater treatment, making it a prime target for malicious cyber actors seeking to disrupt or destroy systems and services or perform other nefarious activities, such as extortion. OT cyber incidents can have severe consequences for OT owners and operators, such as financial losses, operational disruptions, and compromises of environmental and health and human safety. Cyber actors can cause incidents in multiple ways, including exploiting:

- **Vulnerabilities** in flawed or outdated software/firmware to gain access to OT systems.
- **Weak authentication mechanisms** to gain unauthorized access to OT systems.
- **Insufficient network segmentation** to move laterally from IT to OT environments and between OT systems.
- **Insecure OT protocols** to intercept communications, inject malicious commands, and disrupt or manipulate industrial processes.
- **Insecure remote access points** to gain access to OT systems, allowing for lateral movement or for command and control.

Creating an asset inventory is necessary for building a modern defensible architecture and one of CISA's Cybersecurity Performance Goals (CPGs).[1] A modern defensible architecture mitigates risk through a thoughtful system design and implementation that enables OT cyber defenders to identify, prevent, and respond to cyber threats while ensuring reliability, operational continuity, safety, and compliance with regulatory requirements.[2] An **OT asset inventory**—an organized, regularly updated list of an organization's OT systems, hardware, and software—is foundational to designing a modern defensible architecture because without an inventory, organizations do not know what they have and what should be secured and protected.

Developing an asset inventory is a multi-step process where OT owners and operators identify, classify, and document assets. OT owners and operators that develop an **OT taxonomy** as part of the inventory process can significantly enhance the process. An OT taxonomy is a categorization system used to organize and prioritize OT assets to facilitate risk identification, vulnerability management, and incident response. The

[1] CISA's CPGs provide a minimum set of practices and protections that CISA and the National Institute of Standards and Technology (NIST) recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. Visit CISA's CPGs webpage for more information on the CPGs, including additional recommended baseline protections.

[2] For more information on modern defensible architecture, see ASD ACSC's Modern defensible architecture.

taxonomy aids owners and operators in conducting asset inventories by facilitating classification of assets by function and/or criticality and visualizing asset relationships and dependencies.

This guide, authored by the Cybersecurity and Infrastructure Security Agency (CISA) and the following partners,[3] presents the key elements and best practices for creating an asset inventory as well as industry-accepted approaches for developing an OT taxonomy:

- Environmental Protection Agency (EPA)
- National Security Agency (NSA)
- Federal Bureau of Investigation (FBI)
- Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC)
- Canadian Centre for Cyber Security (Cyber Centre)
- Germany's Federal Office for Information Security (BSI)
- Netherlands' National Cyber Security Centre (NCSC-NL)
- New Zealand's National Cyber Security Centre (NCSC-NZ)

This guide emphasizes the importance of proactive planning, collaboration between IT and OT teams, and where possible and appropriate, the integration of cutting-edge technologies to stay ahead of potential threats. The OT landscape is constantly evolving. This guide is not intended to provide a comprehensive view of all possible OT assets. Instead, this document is intended to supplement an organization's existing OT asset inventory resources.

The guide also contains conceptual taxonomies (see **Appendix B: Taxonomy for Oil and Gas Organizations**, **Appendix C: Taxonomy for Electricity Organizations**, and **Appendix D: Water and Wastewater**) developed through working sessions for oil and gas organizations and electricity organizations in the Energy Sector and for Water and Wastewater Sector organizations. CISA created these taxonomies through eight collaborative working sessions held in early 2025. CISA collected and incorporated feedback from approximately 14 organizations and 33 participants, including representatives from U.S. federal agencies and the private sector. These are not authoritative instructions for these sectors but are meant to help guide sector-specific organizations that lack widely adopted methods of classifying their OT assets.

The authoring organizations encourage owners and operators to:

- Review and implement the recommendations in the **Steps to Develop an OT Asset Inventory and Taxonomy** section to enhance your asset inventory process.
- Socialize this guidance, both within your organization and with your peers.
- Provide feedback on this product and recommendations for future products via CISA's anonymous product survey.

[3] Hereafter referred to as the "authoring agencies."

Acknowledgements

CISA led the development of this guide through the Joint Cyber Defense Collaborative (JCDC)[4] in collaboration the Department of Energy (DOE) and other government and private sector partners, including OT owners and operators.

The following industry stakeholders contributed to the development of this document:

- American Water
- British Petroleum PLC
- Denver Water
- Duke Energy Corporation
- Energy Threat Analysis Center (ETAC)[5]
- Eversource Energy
- James Kimzey Regional Water District
- Lansing Board of Water & Light
- Loudoun Water
- Marathon Petroleum Corporation
- Montgomery Township Municipal Sewer Authority
- Pacific Gas & Electric Company
- Southern California Edison

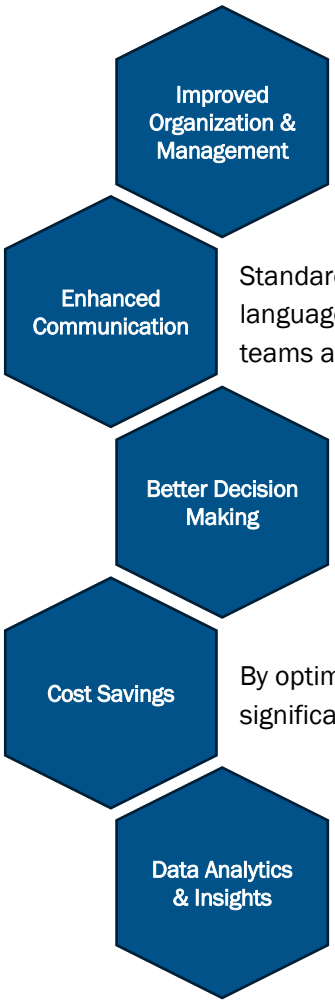
OT Taxonomies

Maintaining an accurate, up-to-date asset inventory is complex. OT environments often contain diverse assets, such as legacy systems, specialized devices, sensors, and instrumentation. These assets use various proprietary protocols for communication. Owners and operators need context on a components' role in monitoring and control of the physical process; this may require owners and operators to physically review and inspect assets and associated process areas.

[4] JCDC is a public-private collaborative within CISA that leverages authorities granted by Congress in the 2021 National Defense Authorization Act (NDAA) to unite the global cyber community in defense of cyberspace.

[5] The U.S. Department of Energy and the private sector established the ETAC for operational collaboration on energy sector threat situational awareness, mitigation, and response. The ETAC brings together industry and government experts, including the Electricity Information Sharing and Analysis Center (E-ISAC) and national labs, to identify and address cyberthreats to the U.S. energy system through work at the unclassified and classified levels.

Owners and operators should incorporate development of an OT taxonomy into their asset inventory process to address this complexity. An OT taxonomy provides a classification methodology for components and systems, streamlining the creation and maintenance of the asset inventory. Key benefits of framing an OT asset inventory through an OT taxonomy are:



A well-structured OT taxonomy enables effective categorization and organization of various assets, processes, and data. This makes it easier to manage and retrieve information, leading to more efficient operations.

Standardizing terminology and classifications helps ensure everyone speaks the same language. This reduces misunderstandings and improves collaboration between different teams and departments.

With a clear understanding of the relationships and dependencies between different assets and processes, organizations can make more informed decisions. This includes optimizing resource allocation, planning maintenance, and implementing upgrades.

By optimizing asset management and reducing inefficiencies, an OT taxonomy can drive significant cost savings, minimize downtime, and improve overall operational efficiency.

A structured OT taxonomy enables better data analytics by providing a clear framework for organizing and analyzing data. This leads to valuable insights that can drive continuous improvement and innovation.

Steps to Develop an OT Asset Inventory and Taxonomy

The authoring agencies recommend owners and operators complete the following steps to develop an OT asset inventory and taxonomy (see **Figure 1**):

Figure 1: Asset Inventory Steps

1. Define Scope and Objectives.

a. **Define governance over asset management.** Identify the authority that requires an OT asset inventory be created. Determine what offices or positions in the organization are responsible for and/or benefit from establishing and maintaining the inventory.

b. **Assign roles.** Assign roles and responsibilities for data collection and validation.

c. **Define the scope.** Set the boundaries of the program (e.g., specific zones, facilities, systems, and development timeline) and identify what constitutes an "asset" for the purposes of the inventory.

2. Identify Assets and Collect Attributes.

a. **Identify assets.** Conduct a physical inspection and logical survey by gathering detailed digital and network-based information about system components. Compile a comprehensive list of OT assets and network infrastructure dependencies. The scope of the asset inventory should consider assets identified in documentation and physical inspection.

b. **Collect asset attributes.** These should be included in the inventory as fields that describe the asset. Prioritize the collection of the following high priority attributes (see **Appendix A: Asset Inventory Fields** for information on the benefit of these attributes and other attributes that the authoring agencies recommend collecting if your organization is resourced to collect them):

i. Active/supported communication protocols
ii. Asset criticality
iii. Asset number
iv. Asset Role/Type
v. Hostname
vi. IP address
vii. Logging
viii. Media Access Control (MAC) address
ix. Manufacturer
x. Model
xi. Operating system (OS)
xii. Physical location/address
xiii. Ports/services
xiv. User accounts

3. Create a Taxonomy to Categorize Assets.

There are five steps to build a taxonomy (see **Figure 2**). **Note:** See **Appendix B: Taxonomy for Oil and Gas Organizations**, **Appendix C: Taxonomy for Electricity Organizations**, and **Appendix D: Water and Wastewater**

for taxonomies CISA developed through working sessions for oil and gas organizations and electricity organizations in the Energy Sector and for Water and Wastewater Sector organizations.

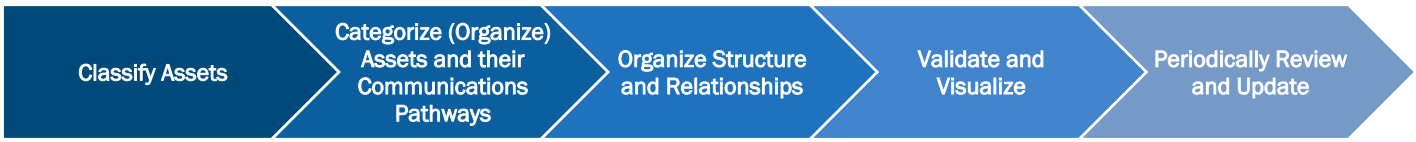


Figure 2: How to Build an OT Taxonomy

a. **Classify assets.** Some common methodologies for classifying OT assets align to criticality or function.
   i. **Criticality-based classification**:
      (1) Assets are classified based on their importance to the organization's operations, safety, and mission.
      (2) Critical assets are those whose failure or compromise would have the most significant impact.
   ii. **Function-based classification**:
      (1) Assets are grouped based on their roles or exposure within the OT environment, such as control systems, communication devices, monitoring tools, engineering, maintenance, or management functions.
      (2) This approach helps in understanding dependencies and interconnections.

b. **Categorize (organize) assets and their communications pathways.**
Note: There are multiple models and standards to organize assets, communications pathways, and others; this is at the discretion of the organization. The International Society of Automation (ISA)/International Electrotechnical Commission (IEC) 62443 series of standards—which CISA used to develop the taxonomies in **Appendix B: Taxonomy for Oil and Gas Organizations**, **Appendix C: Taxonomy for Electricity Organizations**, and **Appendix D: Water and Wastewater**—organizes assets into Zones and Conduits:[6]
   i. A **Zone** is a grouping of logical or physical assets (e.g., control assets, safety assets, assets in a demilitarized zone [DMZ]) that share common security requirements based on factors such as criticality and consequence. For example, all machines that control a production line might be in one Zone because they need the same level of protection. Zones help place focus on securing similar assets, where current security capabilities can be compared against established requirements.
   ii. **Conduits** consist of the grouping of cyber assets dedicated exclusively to communications, and which share the same cybersecurity requirements. They ensure that only authorized data or traffic can pass between Zones. For instance, a Conduit might connect a factory's control system to its monitoring system, but with strict rules to prevent unauthorized access. OT

[6] *Security for Industrial Automation and Control Systems – Part 3-2: Security Risk Assessment for System Design*. International Society of Automation, 2020.

systems can be connected to several conduits simultaneously. To determine Conduits, organizations should map communication pathways between zones incorporating data flow analysis, protocol identification, and Layer2/Layer3 network details.

c. **Organize structure and relationships.**
   i. Identify process dependencies (e.g., operational sequences or control flows).
   ii. Adopt consistent naming conventions for assets to ensure clarity and consistency across the hierarchy.
   iii. Create detailed documentation to include naming convention methodology, structure, and deviations.
   iv. Document roles and responsibilities of interaction with assets—operators, technicians, vendors, integrators, etc. (ownership of functions like operations or maintenance, not access or credential specific).

d. **Validate and visualize.**
   i. Cross-check collected inventory for accuracy and completeness.
   ii. Create diagrams to represent asset categories (e.g., Zones and Conduits). See **Figure 3** for an example diagram of an electricity organization taxonomy aligned to Zones and Conduits.

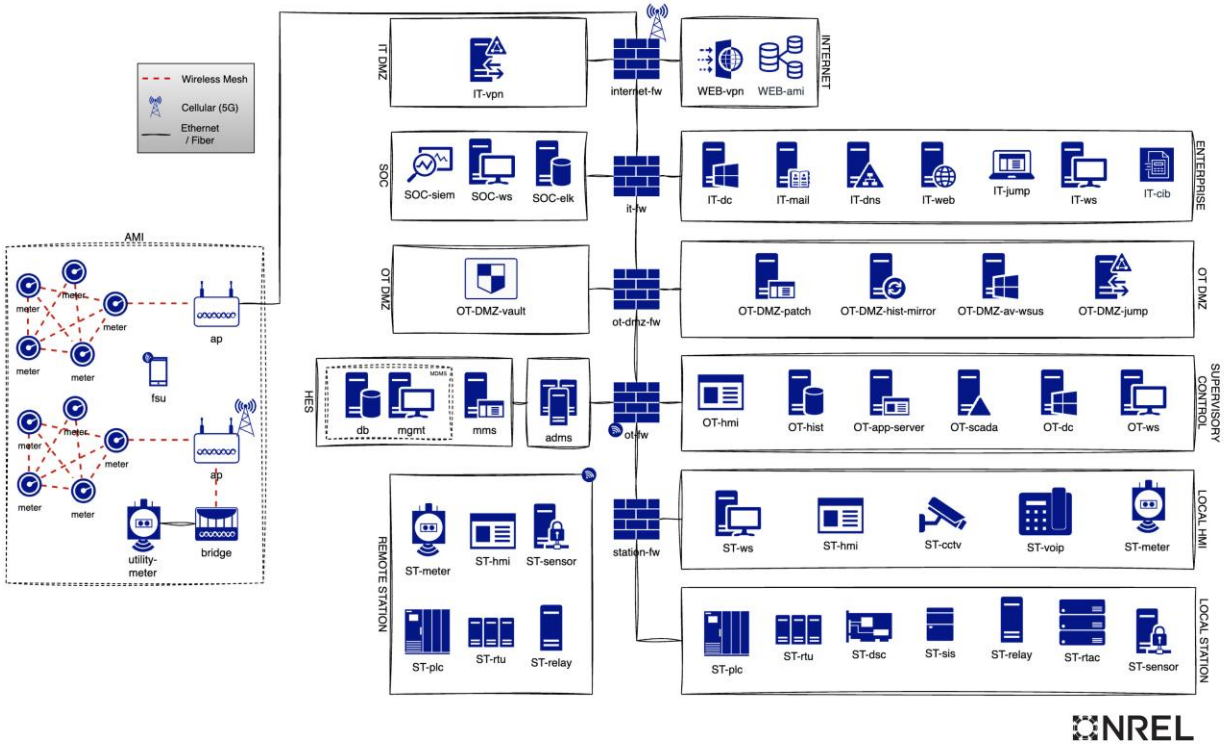


Figure 3: Example Distribution Environment Reference Architecture[7]

[7] Provided by the National Renewable Energy Laboratory (NREL).

iii. Use tables or charts to show asset relationships and dependencies.

e. **Periodically review and update.**
   i. Periodically review and update the taxonomy to reflect changes in technology and operations.
   ii. Gather feedback from stakeholders to ensure the taxonomy meets their needs and accurately represents the OT environment.

4. Manage and Collect Data.

a. **Identify additional asset information sources.** Identify sources of data for each asset (e.g., integrator agreements, vendor manuals and handbooks, maintenance records, recorded operational data, and configuration specifications) that may enhance the inventory and conduct a cost-benefit analysis of including them.

b. **Store data.** Establish a centralized database or asset management system to store and manage additional asset data, implementing security controls to ensure data protection and resilience against cyber threats.

5. Implement Life Cycle Management.

a. **Define life cycle stages.** Define the stages of each asset's life cycle (e.g., acquisition, deployment, commissioning, maintenance, and decommissioning).

b. **Develop life cycle policies.** Develop policies for managing assets throughout their life cycle, including maintenance schedules, replacement plans, and backup strategies. This includes following an organization's change management process and requiring asset inventory updates for introduction or removal of devices into the system in all cases, even under emergency change authority.

Post Inventory and Taxonomy Development Actions

The following sections outline key actions OT owners and operators should take with their inventory.

OT Cybersecurity and Risk Management

- **Identify known vulnerabilities**, available patches, updates, and hardening guidance for vendor systems and applications.
- **Cross-reference inventories** with established vulnerability databases, such as CISA's Known Exploited Vulnerabilities (KEV) Catalog, which highlights actively exploited vulnerabilities, and MITRE's Common Vulnerabilities and Exposures (CVE) database[8], which provides detailed reports on identified security flaws.
  - Continuously explore security controls for known OT vulnerabilities in vendor systems and applications that cannot be patched immediately or are end of life.

[8] "Common Vulnerabilities and Exposures (CVE)." cve.org. Accessed June 24, 2025. https://www.cve.org/.

- Prioritize critical assets and systems and detail redundancy plans and the ability to operate under compromise if vulnerabilities are targeted in critical assets and systems.
- Implement real-time monitoring to detect emerging threats and vulnerabilities.
- Use the KEV catalog as authoritative input to a vulnerability management prioritization framework. Vulnerability management frameworks—such as the Stakeholder-Specific Vulnerability Categorization (SSVC) model—consider a vulnerability's exploitation status. Organizations should also consider using automated vulnerability and patch management tools that automatically incorporate and flag or prioritize KEV vulnerabilities.

- **Prioritize threat factors** by mapping potential attack patterns to known threat intelligence sources like MITRE ATT&CK Matrix for ICS[9] and MITRE's Common Attack Pattern Enumeration and Classification (CAPEC): Industrial Control System Patterns.[10] Prioritize security efforts based on the most critical risks.
- **Strengthen security posture** by designing a security architecture that incorporates effective controls, such as segmentation, access management, and monitoring.

Maintenance and Reliability

- **Review maintenance plans**, considering vulnerability assessment findings and mitigations. Schedule mitigating actions or patching during maintenance windows—unless urgency drives an emergency change.
- **Compare the costs** of potential downtime or degraded services with the cost of replacing these vulnerable systems (if they are legacy) or deploying compensating controls.
- **Implement more secure systems** by using cyber-informed engineering[11] principles and secure by design guidance to embed security in the procurement of new systems and engineering designs (See joint guide Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Product). Leverage taxonomy and risk management processes to inform security decisions.
- **Analyze OT spare parts inventory** to determine whether the stockpile of spare OT components sufficiently covers the critical assets identified in the inventory to ensure operational reliability.

[9] "ICS Matrix." MITRE ATT&CK®. Accessed June 24, 2025. https://attack.mitre.org/matrices/ics/.

[10] "CAPEC VIEW: Industrial Control System (ICS) Patterns." MITRE. Accessed June 27, 2025. https://capec.mitre.org/data/definitions/703.html.

[11] "Cyber-Informed Engineering," Idaho National Laboratory (INL). Accessed June 24, 2025. https://inl.gov/national-security/cie/.

Performance Monitoring and Reporting

- **Continuously monitor asset performance and status**; prioritize process variable monitoring focused on real-time indicators like temperature, pressure, or flow to detect performance issues or maintenance needs, and/or network and system diagnostics monitoring, which leverages continuous monitoring tools to analyze communication health, device connectivity, and process flow integrity.
- **Develop reporting mechanisms** to track asset performance, maintenance activities, and compliance with policies.
- **Identify asset inventory owners** to oversee updates and validate asset classifications to ensure the ongoing accuracy, maintenance, and reporting of the OT asset inventory.

Training and Awareness

- **Train staff** in asset management practices, tools, and procedures.
- **Implement awareness programs** to ensure all stakeholders understand the importance of asset management.

Continuous Improvement

- **Implement a feedback loop** to gather insights from asset management activities and identify areas for improvement.
- **Use change management processes** to accurately track OT asset modifications, additions, and decommissioning.
- **Conduct regular reviews** of the inventory and audits of the asset management program to ensure it remains effective and aligned with organizational goals.

Additional Resources

For more information on asset management and OT cybersecurity, see the following resources:

- NIST's Cybersecurity Framework
- CISA's Principles of Operational Technology Cyber Security
- CISA's Cybersecurity Performance Goals (CPGs)
- EPA's Water Sector Cybersecurity Program Case Study: Small Wastewater System

Questions and Feedback

Stakeholders are encouraged to provide feedback via CISA's anonymous product survey.

Contact Information

U.S. organizations are encouraged to report suspicious or criminal activity related to information in this guide to:

- CISA via CISA's 24/7 Operations Center at SOC@mail.cisa.dhs.gov or 1-844-Say-CISA (1-844-729-2472) or your local FBI field office. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.
- For NSA cybersecurity guidance inquiries, contact CybersecurityReports@nsa.gov.
- Water and Wastewater Systems Sector organizations, contact the EPA Water Infrastructure and Cyber Resilience Division at watercyberta@epa.gov to voluntarily provide situational awareness.

Australian organizations visit cyber.gov.au or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents and access alerts and advisories.

Canadian organizations report incidents by emailing Cyber Centre at contact@cyber.gc.ca.

German organizations visit bsi.bund.de/EN/IT-Sicherheitsvorfall/it-sicherheitsvorfall_node.html to report cyber security incidents.

Netherlands' organizations visit ncsc.nl for advisories, and report incidents by emailing NCSC-NL at cert@ncsc.nl.

New Zealand organizations report cyber security incidents to incidents@ncsc.govt.nz or call 04 498 7654.

Disclaimer

This document does not address OT safety topics, such as risks to human life, health, property, or the environment. This document does not create policies, impose requirements, mandate actions, or override existing legal or regulatory obligations. All actions taken under this document are voluntary.

The information in this report is being provided "as is" for informational purposes only. The authoring agencies do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favor by the authoring agencies.

Version History

August 13, 2025: Initial version.

Appendix A: Asset Inventory Fields

Successful asset management requires understanding what data to capture for each asset in an inventory. Table 1 shows recommended asset inventory fields and potential benefits of including them.

For a more detailed description of the attributes with respect to monitoring using CISA's Malcolm and vulnerability management using the Common Security Advisory Framework (CSAF)[12], see the following repository[13]:

Table 1: Asset Inventory Fields, Attributes, and Recommendation on Priority of Requirement

Asset Inventory Field	Attribute Benefit	Priority
Active/Supported Communication Protocols	Useful for analyzing network traffic. Initially focus on assets that interact with devices outside the IT/OT perimeter or with supervisory control and data acquisition (SCADA) devices over a wide area network, followed by assets that do not.	High
Asset Criticality	Enables assets to be managed based on their operational role, safety impact, and/or exposure to risks.	High
Asset Number	Unique identifier assigned to the asset by the organization.	High
Asset Role/Type	Useful for understanding context and function of the asset in the network. Common examples of asset type are: ▪ Engineering workstation ▪ Programmable logic controller (PLC) ▪ Historian ▪ Network switch/router ▪ Hypervisor host	High
Hostname	Potentially useful for understanding context and function of the asset in the network if included in host naming conventions.	High
IP Address	Useful in analyzing network traffic.	High

[12] "Common Security Advisory Framework (CSAF)," Oasis, accessed August 8, 2025, https://www.csaf.io/.

[13] "DINA-community/String-Sysiphos/Attributes of Data Model," GitHub, last modified August 2, 2025, https://github.com/DINA-community/String-Sysiphos/blob/main/datamodel/datamodel_attributes.md.

Asset Inventory Field	Attribute Benefit	Priority
Logging	Provides details about how logs from the asset are collected to enable detection and investigation of potentially malicious activity.	High
MAC address	Useful for determining manufacturer, if not otherwise specified. (**Note:** Could only refer to network card manufacturer.)	High
Manufacturer	Useful for determining known vulnerabilities.	High
Model	Useful for determining known vulnerabilities.	High
Operating System	Useful for determining known vulnerabilities, if applicable.	High
Physical Location/Address	Provides detail on where to find the asset.	High
Ports/Services	Useful for verifying role and determining attack surface, but extremely time consuming to develop and maintain. Initially focus on assets that interact with devices outside the OT security perimeter or with SCADA devices over a wide area network, followed by assets that do not. **Note:** If there is not an active cyber security control (e.g., a firewall) preventing communication outside the OT perimeter, then focus would apply to all assets for ports/services.	High
User Accounts	Useful in knowing which user account is expected to be most active, or if the asset is expected to be accessed by many different users.	High
Backup Frequency/Type	Provides frequency for how often backups are performed (e.g., daily, weekly, monthly) and method used (e.g., full, incremental, differential).	Medium
Baseline Image	Useful to know if there is a particular known-good image that the OS installation was based on, aiding in post-incident recovery.	Medium
Department/Owner	Useful in understanding who owns or is responsible for the asset.	Medium

Asset Inventory Field	Attribute Benefit	Priority
Distributor	Useful in understanding where an asset originates (may not be manufacturer).	Medium
Firmware/Software Version	Useful for determining known vulnerabilities, if applicable.	Medium
OS Version	Useful for determining known vulnerabilities, if applicable.	Medium
Physical or Virtual	Provides context on whether asset is physical or virtual.	Medium
Virtual Local Area Network (VLAN)	Offers visibility into the asset's network structure.	Medium
Antivirus (AV)/Endpoint Protection	Provides details on the asset's capability to protect itself from malicious activities.	Low
Date of Manufacture	Useful in determining obsolescence.	Low
Hypervisor (if applicable)	Provides context in what type of hypervisor is running the virtual machine (VM).	Low
Local Time Zone	Useful when conducting user behavior analysis where timelines come into play.	Low
Location Within Hypervisor (if applicable)	Provides context on where the VM resides within the hypervisor.	Low
Network Monitoring	Provides information about how well communications to the asset are monitored to detect potentially malicious communications.	Low
Notes/Description	Provides additional context about the asset, how it is used, issues it has had, etc.	Low
Primary Communication Method	Useful to limit attack surfaces and assess whether an incident is local, remote, or network-wide (e.g., wired, wireless, cellular, microwave/radio frequency (RF), satellite), and corollary to communications protocols.	Low
Serial Number	Unique identifier; needed to verify some access to vendor patches/support.	Low

Asset Inventory Field	Attribute Benefit	Priority
Time Source	Provides clarity on how an asset synchronizes its operations (e.g., Network Time Protocol (NTP), GPS, Atomic Clock, Local Clock) as disruption of an external time source and associated drift could result in significant impacts.	Low

Appendix B: Taxonomy for Oil and Gas Organizations

CISA conducted a virtual exercise with working session participants from the Oil and Natural Gas Subsector to identify the necessary steps for organizations to develop their own OT taxonomy. Since this exercise was virtual, CISA did not perform actions that required direct knowledge of physical sites, component details or asset attributes, dependencies, or data flows.

The authoring agencies encourage Oil and Natural Gas Subsector organizations to use this taxonomy as one example for developing their own taxonomies.

Exercise Steps

1. Identify Assets.
   a. Through a rapid data collection exercise, CISA generated a notional list of oil and natural gas assets. Since CISA could not conduct a physical inspection, CISA started with identifying key OT process areas with participants:
      i. Safety systems
      ii. Management/engineering
      iii. Process control and monitoring
      iv. Environmental systems
      v. Communications systems
      vi. Network equipment
      vii. Cyber-physical security
   b. After identifying the key process areas, CISA identified the notional assets listed in Table 2 for each key process area (this list is not exhaustive and may not capture all relevant assets):

Table 2: Notional Oil and Natural Gas Subsector Organization Asset List by OT Process Area

Safety	Management/ Engineering	Process Control and Monitoring	Environmental	Communications	Network Equipment	Cyber-Physical Security
Emergency shut down	Temporary connected devices (i.e., laptops, removable media)	SCADA	Stack monitoring	Wired	Network switches	Identity and access management
Fire and gas systems	Integrated data management systems	Distributed control systems (DCS)	Continuous environmental monitoring	Microwave back haul	Firewalls	Detection and monitoring systems

Safety	Management/ Engineering	Process Control and Monitoring	Environmental	Communications	Network Equipment	Cyber-Physical Security
Controllers/safety instrumented systems	Remote access (jump-server)	PLC	Leak detection	Industrial Internet of Things (IIoT) network	Infrastructure monitoring (uptime performance, fault status)	Antivirus /patching
Sequence of events	Backup and recovery	Advanced process control	Heat tracing	Cellular modems	Wireless access points	Vulnerability scanning
Electrical safety/load shed	Engineering maintenance network	Historian	Building management systems (BMS)	Two-way radio networks	Media converters	Endpoint detection
Dynamic positioning	Virtualization/containers/orchestration	Third-Party packages (e.g., compressor, turbine controls, burner, packaged boiler)	Power management systems	Fiber optic networks	Data diodes	Physical access control systems

2. **Classify Assets.**
   a. CISA created three criticality classifications based on security considerations:
      i. High-criticality assets should have the most stringent security measures, such as network segmentation and role-based access control.
      ii. Medium-criticality assets should have robust monitoring and regular updates to ensure reliability.
      iii. Low-criticality assets should have basic security measures. They are included in the inventory for completeness.
   b. CISA refined the key process areas previously identified (**Table 2**) into functions.

3. Categorize Assets.
   a. CISA grouped the *functions* into like categories (i.e., Zones. CISA grouped the Zones by criticality). This resulted in the asset taxonomy shown in **Table 3** through **Table 5.**

Table 3: High-Criticality Assets

Primary Production Systems	Safety Systems	Control Systems	Power Systems
Drilling rigs	Emergency shutdown systems (ESD)	DCS	Backup generators
Wellheads	Fire and gas detection systems	PLCs for critical processes	Uninterruptible power supplies (UPS)
Subsea equipment	Blowout preventers (BOP)		

Table 4: Medium-Criticality Assets

Processing Equipment	Monitoring Systems	Communications Systems	Networking Equipment
Separators (oil, gas, water)	Condition monitoring sensors (vibration, temperature, pressure)	SCADA systems	Switches and routers for process control networks
Compressors	Data historians	Remote terminal units (RTUs)	
Heat exchangers			

Table 5: Low-Criticality Assets

Auxiliary Systems	Non-Critical Monitoring	Peripheral Devices
Heating, ventilation, and air conditioning (HVAC) systems	Environmental monitoring (e.g., emissions tracking)	Operator workstations
Lighting systems	Non-essential data logging	Non-critical human-machine interfaces (HMI)

4. Next Steps.
   a. CISA did not complete the **Organizing Assets and Their Communications Pathways**, **Organize Structure and Relationships**, and **Validate and Visualize** steps because they require identified assets and knowledge of deployed communications pathways and process dependencies. By

completing these next steps in a real inventory, an Oil and Natural Gas Subsector organization would be able to create a taxonomy that illustrated asset zones, conduits, and categories, as well as asset relationships and dependencies. This would enable them to create a taxonomy that accurately represents their OT environment and aids with completion of the inventory.

Appendix C: Taxonomy for Electricity Organizations

CISA conducted a virtual exercise with working session participants from electricity organizations in the Energy Sector to identify the necessary steps for organizations to develop their own OT taxonomy. Since this exercise was virtual, CISA did not perform actions that required direct knowledge of physical sites, component details or asset attributes, dependencies, or data flows.

The authoring agencies encourage Energy Sector organizations to use this taxonomy as one example for developing their own taxonomies.

Exercise Steps

1. Identify Assets.
   a. Through a rapid data collection exercise, CISA generated a notional list of electricity organization assets. Since CISA could not conduct a physical inspection, CISA started with identifying key OT process areas with participants:
      i. DMZ
      ii. Communications systems
      iii. Power generation
      iv. Power transmission and distribution
      v. Physical access controls, electronic access control, or monitoring systems
      vi. Energy management systems (EMS)
      vii. Distributed energy resource (DER) storage
      viii. Energy
   b. After identifying the key process areas, CISA identified the notional assets listed in Table 6 for each key process area (this list is not exhaustive and may not capture all relevant assets):

Table 6: Notional Electricity Organization Asset List by OT Process Area

DMZ	Communications	Generation	Transmission and Distribution	Physical Access Controls, Electronic Access Control, or Monitoring Systems	Energy Manage-ment Systems (EMS)	Distributed Energy Resources (DER)	Energy Resource Storage
Firewalls	Digital analog converters (DAC)	HMI	Protective controls (relays)	Badge readers/smart keys	Condition monitoring (i.e., digital fault record)	Communi-cations to and from inverters	Power control system (i.e., battery manage-ment system)
Application servers	Microwave	PLCs	HMIs	Cameras	Centralized remedial action scheme (CRAS)	Hybrid inverter	Monitoring
Cyber monitoring tools	Satellite	Engineering work-stations	Engineering workstations	Role Based Access	Fault Location Isolation Service Restoration (FLISR)	Power control systems (distributed energy resources manage-ment system)	Mainte-nance
Remote Access Servers	Fiber	Local area network (dependent on age of facility)	RTUs/PLCs	Motion detectors	Front end processor	Biomass generators	Pump/ hydro
Intrusion detection/ prevention services	Routers/ switchers	Turbine control systems	Smart meters	Intrusion detection systems	Alarm and event notifications	Solar photo-voltaic (PV) systems	Thermal system

DMZ	Communications	Generation	Transmission and Distribution	Physical Access Controls, Electronic Access Control, or Monitoring Systems	Energy Manage-ment Systems (EMS)	Distributed Energy Resources (DER)	Energy Resource Storage
Data historians	Cellular modems	Renewa-bles	Power line carrier com-munication systems	Controlled access points	Phasor measure-ment units	Fuel cells	Com-pressed air

2. **Classify Assets.**
   a. CISA created three criticality classifications based on security considerations:
      i. High-criticality assets should have the most stringent security measures, such as network segmentation and role-based access control.
      ii. Medium-criticality assets require robust monitoring and regular updates to ensure reliability.
      iii. Low-criticality assets can have basic security measures but should still be included in the inventory for completeness.
   b. CISA refined the key process areas and assets previously identified (**Table 6**) into functions.
3. **Categorize Assets.**
   a. CISA grouped the functions into like categories (i.e., Zones. CISA then grouped the Zones by criticality). This resulted in the asset taxonomy shown in **Table 6** through **Table 9**.

Table 7: High-Criticality Assets

Primary Equipment	Protection Systems	Control Systems	Power Supply Systems
Power transformers	Protection relays (over/under current), distance type (impedance, reactance), differential (current, voltage)	DCS	Backup generators
Circuit breakers	Fault detection and isolation mechanisms	PLCs managing critical functions	(UPS for critical equipment
Switchgear	Voltage regulators	SCADA systems	

Primary Equipment	Protection Systems	Control Systems	Power Supply Systems
Busbars			

Table 8: Medium-Criticality Assets

Monitoring and Measurement Devices	Communications Systems	Environmental Control Systems
Current and voltage sensors	RTUs	Cooling systems for transformers or control rooms
Metering devices for energy and power quality	Gateways	Heating, ventilation, and air conditioning (HVAC)
Data historians for operational insights	Networking equipment (switches, routers)	

Table 9: Low-Criticality Assets

Facility Support Systems	Peripheral and Non-Critical Devices	Non-Critical Monitoring
Lighting systems for indoor and outdoor facilities	HMIs for secondary or non-urgent systems	Ambient temperature sensors
Building security systems (non-critical zones)	Operator workstations used for administrative tasks	Alarm systems for minor operational thresholds

4. Next Steps.
    a. CISA did not complete the **Organizing Assets and Their Communications Pathways**, and **Organize Structure and Relationships**, and **Validate and Visualize** steps because they require identified assets and knowledge of deployed communications pathways and process dependencies. By completing these next steps in a real inventory, an electricity organization would be able to create a taxonomy that illustrated asset zones, conduits, and categories, as well as asset relationships and dependencies. This would enable them to create a taxonomy that accurately represents their OT environment and aids with completion of the inventory.

Appendix D: Water and Wastewater

CISA conducted a virtual exercise with working session participants from Water and Wastewater Sector organizations to identify the necessary steps for organizations to develop their own OT taxonomy. Since this exercise was virtual, CISA did not perform actions that required direct knowledge of physical sites, component details or asset attributes, dependencies, or data flows.

The authoring agencies encourage Water and Wastewater Sector organizations to use this taxonomy as one example for developing their own taxonomies.

Exercise Steps

1. Identify Assets.
   a. Through a rapid data collection exercise, CISA generated a notional list of water and wastewater assets. Since CISA could not conduct a physical inspection, CISA started with identifying key OT process areas with participants:
      i. Collection
      ii. Water Treatment
      iii. Water Distribution
      iv. Re-Use Water
      v. Data Management – Expand into Enterprise Integration Support
      vi. Wastewater Treatment
      vii. Communications Infrastructure
   b. After identifying the key process areas, CISA identified the notional assets listed in **Table 10** for each key process area (this list is not exhaustive and may not capture all relevant assets):

Table 10: Water and Wastewater Function-Based OT Taxonomy

Collection	Water Treatment	Distribution	Re-Use Water	Data Management - Expand into Enterprise Integration Support	Wastewater Treatment	Communications Infrastructure
Sewer metering vaults	Quality (pH, monitoring systems)	Pressure monitoring sensors	Pump stations	Visualize and reporting tools	Pump stations	Fiber optic
Sewage pump station	Process control (PLCs/RTUs)	Remote valve systems	Pressure reducing vaults	Business intelligence analytics	Biological treatment	Industrial Ethernet

Collection	Water Treatment	Distribution	Re-Use Water	Data Management - Expand into Enterprise Integration Support	Wastewater Treatment	Communications Infrastructure
Measurement (flow meters)	Chemical dosing	Backup power management	Quality	Compliance	Solids handling	Industrial wireless
Tank level sensor	Environmental	Meters/telemetry	Metering	Databases/data lakes	Advanced treatment	Cellular
Quality sensor	Temperature transducer	IOT sensors	Aeration tanks	Cybersecurity measures for data protection in motion	Primary settling tanks	Licensed and unlicensed radio networks
Pressure transducer	Nutrient removal system	Pressure reducing valves	Treated water storage tank levels	Data communication/polling software (OPC UA, MQTT, Modbus)	Sludge dewatering systems	Microwave backhaul

2. **Classify Assets.**
   a. CISA created three criticality classifications based on security considerations:
      i. High-criticality assets should have the most stringent security measures, such as network segmentation and role-based access control.
      ii. Medium-criticality assets require robust monitoring and regular updates to ensure reliability.
      iii. Low-criticality assets can have basic security measures but should still be included in the inventory for completeness.

b. CISA refined the key process areas and assets previously identified (Table 6) into functions.

3. Categorize Assets.
   a. CISA grouped the functions into like categories (i.e., Zones. CISA then grouped the Zones by criticality). This resulted in the asset taxonomy shown in Table 11 through Table 13.

Table 11: High-Criticality Assets

Primary Treatment Systems	Secondary Treatment Systems	Safety and Environmental Systems	Control Systems	Power Systems
Pumps (e.g., intake, discharge, high-pressure)	Aeration systems	Emergency shutdown systems	SCADA systems	Backup generators
Screens, clarifiers, and grit removal systems	Biological treatment reactors	Chemical dosing systems for pH control or disinfection	DCS for core processes	UPS
		Spill containment systems	OT communications infrastructure	

Table 12: Medium-Criticality Assets

Water Quality Monitoring	Communications Systems	Networking Equipment	Auxiliary Systems
Online analyzers for turbidity, chlorine, or dissolved oxygen	RTUs	Network switches	Sludge management equipment (e.g., pumps, centrifuges)
Sampling stations	PLCs	Firewalls for process control systems	Non-essential pumping systems (e.g., irrigation or utility water)

Table 13: Low-Criticality Assets

Facility Support Systems	Peripheral Devices	Non-Critical Monitoring
HVAC	HMIs for non-critical processes	Sensors for ambient temperature, facility water usage, or general alarms
Lighting systems for buildings	Operator workstations	

4. Next Steps.
   a. CISA did not complete the **Organizing Assets and Their Communications Pathways**, **Organize Structure and Relationships**, and **Validate and Visualize** steps because they require identified assets and knowledge of deployed communications pathways and process dependencies. (See **Figure 3** for an example diagram). By completing these next steps in a real inventory, a Water and Wastewater Sector organization would be able to create a taxonomy that illustrated asset zones, conduits, and categories, as well as asset relationships and dependencies. This would enable them to create a taxonomy that accurately represents their OT environment and aids with completion of the inventory.

References

CVE.org. "Common Vulnerabilities and Exposures (CVE)." Accessed June 24, 2025. https://www.cve.org/.

GitHub. "DINA-community/String-Sysiphos/Attributes of Data Model." Last modified August 2, 2025. https://github.com/DINA-community/String-Sysiphos/blob/main/datamodel/datamodel_attributes.md.

Idaho National Laboratory. "Cyber-Informed Engineering." Accessed June 24, 2025. https://inl.gov/national-security/cie/.

International Society of Automation. *Security for Industrial Automation and Control Systems – Part 3-2: Security Risk Assessment for System Design*, 2020.

MITRE. "CAPEC VIEW: Industrial Control System (ICS) Patterns." Accessed June 27, 2025. https://capec.mitre.org/data/definitions/703.html.

MITRE ATT&CK. "ICS Matrix." Accessed June 24, 2025. https://attack.mitre.org/matrices/ics/.

Oasis. "Common Security Advisory Framework (CSAF)." Accessed August 8, 2025. https://www.csaf.io/.