WATER ISAC

Cybersecurity Fundamentals for Water and Wastewater Utilities

Small Systems Guidance Compendium

August 2025

waterisac.org/fundamentals

Table of Contents

Preface

The *12 Cybersecurity Fundamentals for Water and Wastewater Utilities* was completed in December 2024 and published under a single cover in May 2025. This special edition compendium specifically incorporates the Small Systems Guidance from the *12 Cybersecurity Fundamentals for Water and Wastewater Utilities*.

Intended audience. Small/rural/less cyber mature water and wastewater utilities.

Why the separate compendium? A desire to make the guidance a little more manageable but still touch on key cybersecurity fundamentals that smaller water and wastewater utilities should consider addressing.

How many fundamentals for small systems? Small Systems Guidance was incorporated into eight of the twelve fundamentals and represented in the following:

1 | Plan for Incidents, Emergencies, and Disasters

2 | Minimize Control System Exposure

3 | Create a Cyber Secure Culture and Protect from Insider Risks

4 | Implement System Monitoring for Threat Detection and Alerting

5 | Account for Critical Assets

6 | Enforce Access Controls

7 | Embrace Risk-Based Vulnerability Management

8 | Secure the Supply Chain

What's consistent across the *12 Cybersecurity Fundamentals and Small Systems Compendium*? There are many references to CISA's Cross-Sector Cybersecurity Performance Goals (CPGs)[1] and the *Five ICS Cybersecurity Critical Controls*[2] within the eight sections.

Special Notes.

- ***Sharing cybersecurity guidance with service providers.*** We recognize that many small/rural utilities outsource technology and systems integration services. As such, it is practical to consult with those providers on cybersecurity practices to help protect your OT and IT networks. It may be helpful to share this compendium and the larger *12 Cybersecurity Fundamentals for Water and Wastewater Utilities*[3] guide with them.
- ***Receive a call about an incident at your utility?*** There may be an instance when you receive a call from someone with information about a cyber incident at your utility. Unless you know this person, it is important not to divulge any information to them – regardless of who they say they're with – CISA, FBI, EPA, even WaterISAC. However, do not ignore them. Rather, record all the information they will provide to you and then immediately contact someone you **trust** to help you get to the bottom of the issue. That someone you trust could be your NRWA Circuit Rider, local law enforcement, or one of your neighboring utilities.
- ***National Rural Water Association (NRWA).***[4] If you belong to NRWA or any of its state associations,[5] your utility may qualify for free WaterISAC membership as part of your NRWA benefits. *Contact us to find out or sign up!*[6]

Thank you for accessing ***WaterISAC's Cybersecurity Fundamentals for Water and Wastewater Utilities | Small Systems Guidance Compendium***. We hope you appreciate the thoughtful compendium. Please let us know what you think!

The WaterISAC Team

1 **https://www.cisa.gov/cross-sector-cybersecurity-performance-goals**
2 **https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls**
3 **https://www.waterisac.org/system/files/articles/WaterISAC_12%20Fundamentals_FULL%2012%20High%20Res.pdf**
4 **https://nrwa.org/**
5 **https://nrwa.org/about/state-associations/**
6 **https://www.waterisac.org/user/register?destination=nrwa-signup&destination=nrwa-signup**

1 Plan for Incidents, Emergencies, and Disasters

WHY THIS IS IMPORTANT FOR SMALL SYSTEMS: Regardless of utility size, the inability to promptly and efficiently contain, mitigate, and communicate about cybersecurity incidents, emergencies, or disasters could result in significant operational disruption.

Developing plans for how a utility will respond to incidents, emergencies, and disasters is critical for recovering from such events quickly. IT and OT teams should be concerned primarily with cyber incident response plans and disaster recovery plans. These are just two elements of, or adjuncts to, overall business continuity or continuity-of-operations plans.

Five ICS Cybersecurity Critical Controls[1] | Control No. 1: ICS-specific Incident Response Plan

- Organizations must have an ICS-specific incident response plan to account for the complexities and operational necessities of responding in operational environments. **A common mistake for organizations is thinking about incident response as a final element in its security program.**

Smaller systems and less cyber mature utilities may find benefit in CPG practice ***2.S Incident Response Plans*** that requires **little to no monetary investment.** Likewise, this goal has a **high impact toward risk reduction** and is considered **low complexity to implement.**

CPG | 2.S Incident Response (IR) Plans

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.

Participating in or executing tabletop exercises (TTXs) may seem daunting, but for smaller or less resourced utilities the process will be extremely valuable and probably enlightening. According to VERVE, *even a rudimentary low-cost cyber-focused TTX, or paper-based training can be devised to illustrate gaps in your utility's processes, resources, training, and technology. Tabletop exercises don't need to be "hacker" orientated and don't require elaborate props or expensive third-party trainers and platforms to be effective.*[2]

RECOMMENDED RESOURCE

Dragos OT-CERT[3] members have access to the following CIRP and TTX resources:

- Cyber Incident Response Plan Getting Started Guide
- OT Cyber Incident Response Plan Worksheet
- Exercise Scenario Briefing: OT-CERT Self Service Tabletop: Ransomware Disrupts Operations
- OT-CERT-Self Service TTX Ransomware Facilitator Kit

OT-CERT OPERATIONAL TECHNOLOGY CYBER EMERGENCY READINESS TEAM

1 https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/
2 https://verveindustrial.com/resources/blog/getting-prepared-tabletops-and-scripts-to-act-through-a-ransomware-event/
3 https://www.dragos.com/community/ot-cert/

RECOMMENDED RESOURCES

Incident Response Guide for Water and Wastewater Sector | CISA | EPA | FBI

CISA Tabletop Exercise Packages (CTEP) | CISA

Planning Considerations for Cyber Incidents: Guidance for Emergency Managers | FEMA | CISA

Business Continuity in a Box | CISA & Australian Cyber Security Centre (ACSC)

Develop and Conduct a Water Resilience Tabletop Exercise with Water Utilities | EPA

Homeland Security Exercise and Evaluation Program (HSEEP) | FEMA

Incident Command System for Industrial Control Systems (ICS4ICS) | ISA Global Cybersecurity Alliance

How Incident Response (IR) Tabletop Exercises Strengthen OT Security Posture | Dragos

Power Outage and Black Sky Resilience Resources | WaterISAC

Emergency Planning for Water & Wastewater Utilities - M19 | AWWA

2 Minimize Control System Exposure

WHY THIS IS IMPORTANT FOR SMALL SYSTEMS: Unidentified connections into the OT network present unnecessary risk to availability, control, and safety of industrial automation and control systems.

All communication pathways that exist between the ICS/OT network and hostile networks – internal (IT, business) and external (internet) – must be identified. Isolating (air-gapping) a control system from the rest of the world would be ideal. However, complete isolation is likely not practical and may not even be possible.

Connections are difficult to avoid given the demands for remote system access by staff and third parties due to system monitoring/ maintenance or to export control system data for regulatory and business purposes. Even if these connections could be avoided, there are always control system upgrades and patches that make some kind of communication with the outside world unavoidable. Implementing a defensible architecture is the key to minimizing control system exposure and requires a combination of physical and logical network segmentation, hardware and software that restrict traffic, protection of control system design and configuration documents, encrypted communications, restrictive procedures, and physical security.

Five ICS Cybersecurity Critical Controls[1] | Control No. 2: Defensible Architecture

Minimizing control system exposure contributes to having a defensible architecture. As highlighted in the Five ICS Cybersecurity Critical Controls, Control No. 2., common attributes of defensible architectures related to minimizing control system exposure include:

- Segmented environments where possible to reduce ingress and egress into as few pathways as possible, ultimately creating "choke points" for enhanced security and monitoring.
- Determining when bi-directional access is needed, both now and in the future vs. truly read-only applications.

Smaller systems and less cyber mature utilities may find benefit in this CPG practice, ***2.W No Exploitable Services on the Internet*** that requires **little to no monetary investment.** Likewise, this goal has a **high impact toward risk reduction** and is considered **low complexity to implement.** Generally speaking, this could prove useful for water and wastewater utilities to identify devices that are accessible from the internet that they may not have been aware.

CPG | 2.W No Exploitable Services on the Internet

- 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.

Removing exploitable services (CPG | 2.W) that do not need to be accessible from the internet is considered *low cost to implement*. This activity can often be a "quick win" for smaller systems in reducing cyber risk. However, for critical services that may be deemed a necessity, such as remote access, it is imperative that access be securely implemented, which will likely require a financial investment. *See Secure Remote Access discussed earlier in this Fundamental for guidance.*

Discovering internet facing assets is trivial for threat actors. Small systems are encouraged to learn which assets are accessible from the internet before adversaries exploit/compromise them. CISA's Stuff Off Search (S.O.S.) guide[2] provides information on how to use some well-known publicly available full spectrum search engines including Shodan, Censys, and Thingful to help protect your assets and get your "Stuff Off Search" (S.O.S.)

1 https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/
2 https://www.cisa.gov/sites/default/files/publications/Assets_Showing_Primer_508c.pdf

RECOMMENDED RESOURCES

Cyber Resource Hub | CISA

Know What Your Adversaries Know! | CISA

Get Your S.O.S* How-to Guide (Stuff Off Search*) | CISA

Recommendations to Implement Secure Remote Access (SRA) Today | Dragos

Data Diodes Protect Critical Water Infrastructure | Fend

Top 20 Secure PLC Coding Practices | PLC Security

3 Create a Cyber Secure Culture and Protect from Insider Risks

WHY THIS IS IMPORTANT FOR SMALL SYSTEMS: Cybersecurity is a shared responsibility among all staff. Every employee, executive, and board member is accountable for the overall cybersecurity posture of an organization. Creating a cyber secure culture relies on leadership support and staff engagement that can result in a significant risk reduction against insider threats and risks.

When employees are not involved in cybersecurity, not only can vulnerabilities and threats proliferate or go unnoticed, but employees can become insider threats or conduits through which incidents occur – intentionally or unintentionally. Utilities should instill good cyber hygiene practices in every facet of employees' daily tasks. All staff should know what to do when faced with a potential security incident, whether it is a physical or cyber attack. Developing a strong culture will also minimize insider threats.

Executive and Board Engagement – Leadership is Crucial for Culture Change

Effective cybersecurity starts at the top. Unfortunately, leadership at small organizations often lacks sufficient awareness of cybersecurity threats and needs.

Cybersecurity and culture support from the top-down involves identifying someone to be responsible and accountable for cybersecurity. Without a formal cybersecurity leader there is a lack of sufficient cybersecurity accountability, investment, and effectiveness.

CPG | 1.B Organizational Cybersecurity Leadership

- 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 | 1.C OT Cybersecurity Leadership

- 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.

Cybersecurity Awareness and Readiness Training

To create and maintain a culture of cybersecurity, all personnel should receive regular, ongoing cybersecurity awareness training. In addition, role-specific training should be provided for commonly targeted staff like executives, executive assistants, human resource, finance personnel, IT administrators, engineers, SCADA staff, and operators.

While cybersecurity is an expansive subject, there are certain principal topics that should be regularly emphasized for general awareness and to promote positive cyber hygiene. One common theme that warrants frequent inclusion in training materials is social engineering-based tactics, such as phishing. Training should regularly incorporate the importance of safe internet browsing and best practices for secure email handling.

For creating a cybersecurity culture, the following CPG practices may be beneficial for smaller systems and less cyber mature utilities. These practices *generally* require **little to no monetary investment,** are considered **low complexity to implement,** and when implemented yield a **high impact toward risk reduction.**

CPG | 2.I Basic Cybersecurity Training

- 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.

For small systems, where employees are not exposed to cybersecurity incident data, there can be a misconception that the organization is too small or "why would someone want to attack us?" It is important to help staff understand that organizations often become victims of circumstance or targets of opportunity. For instance, a utility may use a particular device or application that has a known and exploited vulnerability. Attackers frequently scan the internet for such vulnerable devices and exploit them with no knowledge of the target. It is helpful to show public examples of incidents and impacts that are relevant to each organization to help employees understand the importance of being vigilant. Consider periodically bringing staff together for lunch-and-learn opportunities to talk about relevant public incidents. These opportunities will help foster a culture of cybersecurity. If you're not sure how to facilitate a discussion on a cyber attack or threat, WaterISAC is here to help!

CPG | 2.J OT Cybersecurity Training

- 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.

RESOURCE | Resiliency for Water Utilities Program

The Cyber Readiness Institute,[1] in partnership with the Center on Cyber and Technology Innovation and Microsoft, is actively recruiting participants to participate in a free cybersecurity training program for small and medium-sized water and wastewater utilities. Complementing other technical assistance programs, the CRI program provides coach-supported training and resources focused on improving cybersecurity risk management and ability to respond and recover from a cybersecurity incident.

The program only requires about an hour per week for six weeks and very minimal technical expertise. Participants proceed at their own pace, with the help of a coach to work through implementing organization-wide trainings and policies for strong passwords, multi-factor authentication, patch management, anti-phishing, business continuity, and other core cyber readiness topics. The program will help utilities establish an asset inventory and improve employee awareness of cybersecurity issues.

If you are interested in participating in this program or learning more, please visit the Cyber Readiness Program - Resiliency for Water Utilities Program[2] on the Cyber Readiness Institute's website.

CYBER READINESS INSTITUTE

RECOMMENDED RESOURCES

OUCH! Newsletters | SANS Institute

STOP. THINK. CONNECT.™ | National Cybersecurity Alliance (NCA)

Cyber Readiness Program - Resiliency for Water Utilities Program | Cyber Readiness Institute (CRI)

National Insider Threat Awareness Month | USA Learning

1 https://cyberreadinessinstitute.org/
2 https://cyberreadinessinstitute.org/water-utilities-cyber-ready-training-interest/

4 Implement System Monitoring for Threat Detection and Alerting

WHY THIS IS IMPORTANT FOR SMALL SYSTEMS: While many of the cybersecurity fundamentals in this publication are developed with prevention in mind, in this "assume breach" world, we must be able to detect suspicious and nefarious activity. Without the ability to detect threats within your environments, adversaries will go unnoticed.

Continuous monitoring and threat detection is necessary for the visibility into both IT and ICS/OT networks. The ability to detect threats enables faster threat identification, satisfies regulatory or compliance requirements, and typically reduces adversary dwell time within the network(s). Effective monitoring and threat detection can prevent or minimize financial losses by identifying and mitigating threats before they cause substantial harm.

CPG | 3.A Detecting Relevant Threats and TTPs

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.

OT threat detection and monitoring is important for small utilities and shouldn't be overlooked. However, there are many small utilities that still lack threat detection and monitoring on the IT network. IT threat detection and monitoring is equally important and small systems may find it a more straightforward endeavor to gain visibility before embarking on OT monitoring. Nonetheless, both IT and OT monitoring are important, and it would be practical to consider implementing them at the same time.

While log collection discussed in CPG | 2.T is more costly and complex to implement than the other CPGs referenced in this compendium, CISA has a free resource to assist. *Logging Made Easy* (LME)[1] is a viable solution for small utilities with limited IT security tools and resources seeking a no-cost logging service. LME is a reliable, centralized log management alternative. **LME serves as a SIEM tool, tailored to organizations currently lacking this pivotal capability.** LME equips even the most vulnerable entities with the means to swiftly detect and respond to suspicious activity. At the time of this writing, LME only covers Windows-based devices and is limited to on-premises networks with an Active Directory.

Likewise, another resource to assist with logging is the *Host-Based Logging Guidance: Instructions for Managing Windows Event Logs* from Dragos OT-CERT.[3] Members of OT-CERT have access to a two-part series that provides more understanding

The Five ICS Cybersecurity Critical Controls | Control No. 3: ICS Network Visibility and Monitoring[2]

ICS network visibility and monitoring is not just a technology problem. Among the five ICS Critical Controls, ICS Critical Control No. 3 is most often approached by organizations with the question, "what product do we buy to solve our problems?" There is no silver bullet technology that addresses this security control. An organization needs to consider the following factors to inform a technology selection:

- What data acquisition capabilities exist or are planned in connection with ICS Critical Control No. 2? *(Note: ICS Critical Control No. 2 Defensible Architecture was discussed in Fundamental 2 | Minimize Control System Exposure)*
- What vendors and protocols are in use across systems of interest?
- What workforce staffing and capabilities exist or are anticipated to support the program?
- What processes exist or are anticipated in connection with ICS Critical Control No. 1 that will drive incident response actions?

1 https://www.cisa.gov/cybersecurity-performance-goals-cpgs
2 https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/
3 https://www.dragos.com/community/ot-cert/

and recommended practices for host-based logging. The resource includes guides (documents) and jump-start videos that provide detailed technical "how-to" information for implementing a reasonable level of centralized logging in Windows domain environments. Part 1 covers a recommended set of specific Windows event logs to monitor and the process to create a custom filter view to review the logs. Part 2 includes a technical how-to for configuring each Windows device in the domain to forward its logs to a centralized log collection server.

Recommended Practice

In addition to host-based logging, small systems are encouraged to log events from secure email gateways (SEGs). Logging email events is vital for detecting unauthorized access, data breaches, and compliance, as well as for troubleshooting, forensic analysis, and incident response.

Maintaining Awareness of the Threat Environment

Following threat and analysis reports provided by WaterISAC, CISA, FBI, and others is an effective way to maintain awareness of critical infrastructure threat trends. These reports often include threat actors' tactics, techniques, and procedures (TTPs), behaviors, and other indicators of compromise (IoCs) to help detect known intrusion activity within your environment. Smaller utilities may find it useful to follow WaterISAC for the most relevant threats to water and wastewater utilities and are strongly encouraged to pass along the information to systems integrators and other third-party support to assist with detection and protection.

RECOMMENDED RESOURCES

The Five ICS Cybersecurity Critical Controls | SANS Institute

ICS Cybersecurity Field Manual Series | SANS Institute

Dragos Community Defense Program (CDP) | Dragos

Logging Made Easy | CISA

Practical Goal

When bolstering ICS/OT monitoring and threat detection, smaller systems should consider planning for future capacity. According to the U.S. Department of Energy, the bare minimum devices that should be monitored in an ICS/OT environment are:[9]

Programmable Logic Controllers (PLCs) and other field devices that directly control physical processes. These devices are critical as they can be targeted by attackers to cause physical damage or disruption.

Human-Machine Interfaces (HMIs) and operator stations that allow personnel to monitor and control the ICS/OT systems. Monitoring these devices can detect unauthorized access attempts.

Supervisory Control and Data Acquisition (SCADA) servers and Distributed Control System (DCS) controllers that manage and coordinate the overall control system. Monitoring these central components is essential for detecting anomalous activity.

Network switches, routers, and firewalls that interconnect the various ICS/OT components. Monitoring network traffic can reveal unauthorized access, malware communication, and other suspicious activity.

Engineering workstations used to program and configure the ICS/OT devices. Monitoring these workstations can detect unauthorized changes to the control system configurations.

Domain controllers and authentication servers that manage user accounts and permissions in the ICS/OT environment. Monitoring these servers can detect credential misuse and unauthorized access attempts.

The monitoring should focus on detecting unauthorized access, malware, and anomalous behavior that could indicate a cyber attack. The monitoring solution should be tailored to the specific ICS/OT environment and integrate with ICS protocols and communications.

4 https://www.energy.gov/ceser/considerations-icsot-cybersecurity-monitoring-technologies

5 Account for Critical Assets

WHY THIS IS IMPORTANT FOR SMALL SYSTEMS: By identifying, inventorying, classifying, and documenting the *most critical ICS/OT assets*, utilities can prioritize and allocate security resources effectively to protect those assets from potential threats, attacks, or failures that could disrupt operations or cause safety incidents.

Identifying assets is one of the foundations of a cybersecurity risk management strategy. Most frameworks and seminal guidance resources prominently list asset inventory. Even the 2019 version of this publication included "Perform Asset Inventories" as the #1 fundamental leading with the cliché, *'you can't protect what you don't know you have.'*

CPG | 1.A Asset Inventory

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.

As previously stated, most authoritative cybersecurity guidance leads with some sort of asset management strategy. CISA's *Cross-Sector Cybersecurity Performance Goals* (CPGs)[1] include *Asset Inventory* as the first goal, 1.A. While this CPG assesses asset inventory as a high impact outcome, when using automated tools, it's not low cost or low complexity to implement. Despite the high impact outcome toward risk reduction, the medium complexity and cost to implement is above the threshold of this guide's suggestions for small systems, hence emphasis is placed on a more practical approach of **managing the most critical assets** with the intent to scale in the future. That said, as the majority of water and wastewater systems in the U.S. have a relatively small number of assets, **managing asset inventories can be done effectively via manual processes such as using a spreadsheet and network drawings that are updated on a periodic basis and/or when new systems are added or upgraded.**

Practical Application

In many cases, third parties can be an important part of understanding and documenting OT assets. For example, systems integrators, design engineers, and OT asset programmers can possess deep knowledge of how an OT system is constructed and the composition of assets. A possible way to capture that knowledge is to include a line item in a scope of work requiring a detailed asset inventory as part of the deliverables. It is often the case that multiple third parties will have varying scope on a given project and so a contribution from each is required to build a complete asset inventory that should include all relevant hardware, software, and data.

Additionally, for quick jump-start on the asset inventory, Dragos OT-CERT[2] members have access to the *OT Asset Inventory Template* and *OT Asset Inventory Guide*. The template is a spreadsheet that plant engineers can begin using immediately to develop or refresh an asset inventory. The *OT Asset Inventory Guide* explains how to use the complementary *OT Asset Inventory template*.

Considerations for Critical Assets

Critical assets could include, but are not limited to, sensors, actuators, variable frequency drives (VFDs), circuit breakers, automatic transfer switches (ATSs), critical skid systems, programmable logic controllers (PLCs), human machine interfaces (HMIs), distributed control systems (DCSs), SCADA systems, remote terminal units (RTUs), data radios, industrial control software, industrial firewalls and other security appliances, domain controllers, and critical databases.

Internet of things (IoT) and industrial internet of things (IIoT) within in the control system environment must also be considered.

1 https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
2 https://www.dragos.com/community/ot-cert/

Hot, Warm, or Cold Standby Components

In many cases, cyber resilience can be bolstered with the use of standby devices. For example, a critical controller or HMI can be duplicated in both hardware and configuration, then disconnected from the network, and maintained in either a powered or unpowered state. This "offline" cold or warm standby asset will provide resilience for multiple failure modes including cyber incidents.

Practical Application

In the event of a cyber incident, once the threat is contained or mitigated, it is feasible that normal operations can be restored by replacing affected assets with the presumably non-compromised backup device. **An important aspect of this approach is to include updates to backup devices as part of the change management process.** In the case of the HMI, the cold backup can simply be a cloned copy of the hard drive that can be swapped out as part of the incident response procedure. There are considerations here regarding software licensing, malware that could infect other non-volatile memory in an asset, etc.; however, those are details that can typically be considered on a case-by-case basis.

For Consideration

The *SANS ICS Cybersecurity Field Manual Vol. 2*[8] outlines a practical example to establishing an ICS asset inventory.

1. Start by reviewing any already-created network diagrams and engineering documentation such as "as-built documents."
2. Use an encrypted laptop with at least a basic spreadsheet application to start cataloging and storing ICS asset information during a physical site walk through, as seen below in Table 1: Sample Asset Inventory Attributes.
3. Augment physical inspection with passive network packet captures on critical network segments that host critical ICS assets by using either a SPAN or mirrored port configuration off a fully managed switch or hardware TAP.
4. Ensure field device configurations are backed up during an incident and securely stored for later comparison to detect whether an unauthorized change occurred and reload trusted configurations and project files (controller logic), if needed.
5. At a minimum, record attributes from the commonly targeted critical assets such as data historians, HMIs, PLCs, RTUs, engineering workstations, core network devices, and active safety instrumented systems.

Table 1: Sample Asset Inventory Attributes

Sample Asset Inventory Attributes
Site location
Facility type
Asset type and ID tag
Asset location room, cabinet, rack
Description of asset function for operations
Impact to operations if assets are unavailable
IP and MAC address
Network protocols used
Model, manufacturer, serial number
Firmware version for controllers and related modules, chassis information
Applications installed on critical assets with versions
Assets deemed critical – data historians, HMIs, primary controllers, control system network switches
Project files and configuration (last change date, secure storage location, etc.)
Dependencies – systems, networks, other assets, etc.
Primary and secondary contact for asset

RECOMMENDED RESOURCES

Part 3: Creating An OT Asset Inventory | Dale Peterson

OT Asset Management in 2024: A product category in its own right | Ralph Langner

Industrial Internet of Things Safety and Security Protocol | WEF

6 Enforce Access Controls

WHY THIS IS IMPORTANT FOR SMALL SYSTEMS: Maintaining strict access controls play a crucial role in protecting resources, data, and systems from unauthorized access, ensuring confidentiality, integrity, availability, and safety. Access controls should be enforced for users and devices.

Access control involves providing control system access only to those individuals who are authorized to have it. Restricting access to select individuals limits the number of people who can interact with key systems. When logging and auditing is enabled (Fundamental 4), this restriction also makes it much easier to detect suspicious and unauthorized access. Some important components of access controls include role-based controls, principle of least privilege, and strong authentication.

Role-Based Access Control

Role-based access control (RBAC) grants or denies access to systems or network resources based on job functions or responsibilities. This control limits the ability of individual users – or attackers – to reach files or parts of the system they should not access. For example, SCADA system operators likely do not need access to the billing department or certain administrative files. Therefore, define permissions based on the level of access each job function needs to perform its duties.

For Consideration

Executives, directors, IT administrators, cybersecurity, software developers, finance, human resources, and SCADA operators are examples of roles that typically involve higher levels of account and resource access that need to be further scrutinized. No matter how "senior" a role, or how much tenure someone has, anyone can intentionally or unintentionally use privileged access in a manner that negatively impacts your utility.

Principle of Least Privilege

Similar to RBAC is the principle of least privilege. By applying the principle of least privilege to a user account, only the absolute minimum permissions necessary to perform a required task are assigned. In other words, administrative or other privileged accounts are reserved for special use and are not to be logged in perpetually. Most malware operates with permissions of the logged in user. By granting access and permissions based on roles and least privilege, malware has limited access to the resources it can compromise.

CPG | 2.E Separating User and Privileged Accounts

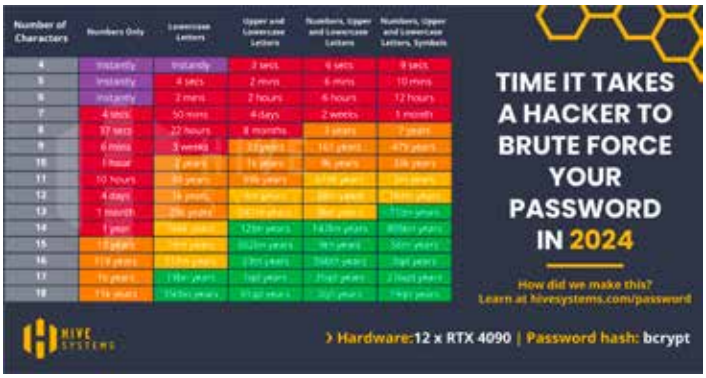
No user accounts always have administrator or super-user privileges. Administrators maintain separate user accounts for all actions and activities not associated with the administrator role (e.g., for business email, web browsing). Privileges are reevaluated on a recurring basis to validate continued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

The concept of least privileged applies to configuring user accounts that allow the given user with least amount of privilege to meet their job requirements. This helps ensure that if their account is compromised, the attacker is limited in the actions they can take without executing additional steps to increase privileges. In some cases, personnel have multiple roles. In those cases, it is recommended that they have multiple accounts for each role that can be utilized accordingly.

Two of the CPGs discussed in this section (**2.B Minimum Password Strength** and **2.E Separating User and Privileged Accounts**) are considered **low cost and low complexity to implement** and result in a **high impact toward risk reduction.** Smaller systems are strongly recommended to implement these CPGs.

Strong Authentication

Implementing minimum password strength policies in small ICS/OT environments can significantly enhance security without incurring high costs. Utilities should set password strength and complexity requirements and communicate the standard to all staff and contractors. While the recommended minimum password length varies, it is typically accepted to be greater than eight characters, incorporating a mix of upper- and lower-case letters, numbers, and special characters to increase complexity. The following image from Hive Systems[1] denotes the time it takes to brute force a password in 2024.



A critical consideration in adopting standards and requirements for password policies is to understand the capabilities of the devices and software in the specific OT environment and set technically feasible requirements.

CPG | 2.B Minimum Password Strength

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.

1 https://www.hivesystems.com/password

Practical Application

Use cases for consideration around account privilege for water and wastewater utilities:

HMI Accounts

- *Default Account* – The HMI should boot into and, after inactivity or logoff, return to a default Guest user account with limited privileges to see screens but no capability to change setpoints, acknowledge alarms, etc.
- *Operator Privilege account* – System operators who are users of the HMI but have some limitations for control and alarm changes should have individual accounts with their privilege restrict to operations capabilities within their role only.
- *Senior Operator/Manager privilege account* – Operators and managers with the authorization to change critical operational setpoints and other similar actions, should have individual accounts with capabilities associated with their role.
- *Engineer account* – Engineers who have authorization to make administrative and configuration changes on the HMI should have individual accounts with the capabilities within their role.

OT/IT Department Access

- *User Account:* An IT technician, who uses a regular user account (*name.user*) for daily tasks such as email, documentation, and accessing non-administrative applications.
- *Privileged Account:* For system maintenance, server configuration, or installing software, the technician switches to the privileged account (*name.admin*), which has administrative rights on the network and critical systems.

Database Management

- *User Account:* A database analyst has a lower privileged user account (*name.user*) to run queries, generate reports, and analyze data from the database.
- *Privileged Account:* When the analyst needs to perform database maintenance tasks, such as creating or deleting tables and managing user permissions, the privileged account (*name.dba*) is used.

RECOMMENDED RESOURCES

Multi-Factor Authentication (MFA) | CISA

What is FIDO? |FIDO Alliance

CISA Releases Guidance on Phishing-Resistant and Numbers Matching Multifactor Authentication | CISA

Role Based Access Control | NIST

Implementing Least-Privilege Administrative Models | Microsoft

Exploitation of Unitronics PLCs used in Water and Wastewater Systems | CISA

7 Embrace Risk-Based Vulnerability Management

WHY THIS IS IMPORTANT FOR SMALL SYSTEMS: Vulnerability management across OT and IT is essential for water and wastewater utilities in maintaining operational continuity, protecting critical infrastructure, and mitigating the risks associated with cyber threats in increasingly interconnected industrial systems.

Vulnerability management is a foundation of every cybersecurity program. Like asset inventory (Fundamental 5 | Account for Critical Assets) and risk assessments, it is a continuous process and completely dependent on and intertwined with those activities. **Vulnerabilities are present everywhere – hardware, software, firmware, configurations, supply chains, and staff practices.** Therefore, vulnerability management is an absolute necessity in every organization. While tasks like patching and antivirus are important in addressing some vulnerabilities, effectively managing vulnerabilities requires a holistic program that applies a risk-based approach across OT and IT environments.

The Five ICS Cybersecurity Critical Controls[1] | Control No. 5: Risk-based Vulnerability Management Program

A risk-based vulnerability management program focuses on those vulnerabilities that actually drive risk to the organization, especially those that map to the scenarios identified in ICS Critical Control No. 1. Often, the vulnerabilities that drive risk in ICS are those that help an adversary gain access to the ICS or introduce new functionality that can be leveraged to cause operational issues such as the loss of view, control, or safety. **The focus of the vulnerability management program is not simply to patch vulnerabilities but also, in many cases, to mitigate their impact or monitor for their exploitation.**

Address Vulnerabilities Before the Bad Guys Exploit Them

With the sheer number of IT devices and internet-accessible ICS/OT devices, vulnerabilities present a significant opportunity for cyber attacks. Public resources like Shodan,[2] Censys,[3] and even Google enable the discovery of vulnerable devices by anyone with an internet connection. Combining data garnered from these discovery tools with vulnerability exploitation kit frameworks like Metasploit and Cobalt Strike, even novice threat actors are able to launch attacks with very little knowledge or understanding about the systems (IT or OT) they are targeting. Performing authorized scans and assessments, including penetration tests, will help identify exploitable vulnerabilities within your environment before the bad guys do.

Throughout this guide, the CISA CPG's that have been referenced for smaller systems and less cyber mature utilities have been denoted as requiring *little to no monetary investment with high impact toward risk reduction and low complexity to implement*. However, **CPG 1.E Mitigating Known Vulnerabilities** is an exception. Despite the *medium complexity* of mitigating known vulnerabiities, it is strongly recommended for small systems to at least address this for critical assets. Mitigating known vulnerabilities has a high impact on risk reduction that cannot be overstated and significantly decreases the attack surface.

1 https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/
2 https://www.shodan.io/dashboard
3 https://censys.com/

CPG | 1.E Mitigating Known Vulnerabilities

All known exploited vulnerabilities (listed in CISA's *Known Exploited Vulnerabilities Catalog*[10] in internet-facing systems are patched or otherwise mitigated within a risk-informed span of time, prioritizing more critical assets first.

Operational Technology (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 | 4.C Deploy Security.txt Files

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

Reference **security.txt**[11] to define the process for security researchers to securely disclose security vulnerabilities to your utility.

Don't Assume Cybersecurity

The maintenance of traditional computers and SCADA equipment for business and operations at water and wastewater utilities can be overwhelming. As such, it's common for small or less technically mature utilities to contract service providers or integrators for both IT and OT support. **In many cases, that support does not provide adequate, if any, cybersecurity protections.** Technology or managed service providers (TSPs or MSPs) may perform patching of and provide antivirus on Windows devices for IT and OT systems (if the OEM or maintenance agreement allows it), but that is typically the extent of protection unless the service contract or scope of work outlines further requirements.

Vulnerability Management Resources

As a starting point in identifying critical vulnerabilities on external facing systems, less resourced systems are highly encouraged to avail themselves to *CISA's Free Vulnerability Scanning (VS) for Water Utilities*[12] service. CISA's vulnerability scanning can help utilities identify and address cybersecurity weaknesses that an attacker could use to impact a system.

CISA's *Known Exploited Vulnerabilities (KEV) Catalog*[13] is a highly recommended resource to help all organizations prioritize patching. **CISA's KEV catalog includes vulnerabilities known to be exploited** – either attempted or successful – by cyber threat actors. The KEV catalog offers network defenders a starting point for prioritizing remediation efforts on the subset of vulnerabilities that are causing immediate harm based on adversary activity. Utilities and their service providers are encouraged to check the KEV catalog and the regular updates for potentially impacted components in your environment and address accordingly.

In addition to referencing CISA's KEV catalog for prioritizing known exploited vulnerabilities, it is necessary for utilities and their integrators to be aware of and apply a risk-based approach to addressing industrial control systems vulnerabilities for OT and SCADA components used within your OT environment. While it's best to track published updates and notifications directly from vendors or manufacturers, CISA also tracks and provides regular *ICS Advisories*.[14] The ICS Advisories found at CISA provide concise summaries covering industrial control system (ICS) cybersecurity topics primarily focused on mitigations that ICS vendors have published for vulnerabilities in their products.

RECOMMENDED RESOURCES

Industrial Control Systems Advisories | CISA

Known Exploited Vulnerabilities Catalog | CISA

The OT Vulnerability Management Handbook | Langner, Inc.

10 **https://www.cisa.gov/known-exploited-vulnerabilities-catalog**
11 **https://securitytxt.org/**
12 **https://www.cisa.gov/resources-tools/resources/cisas-free-cyber-vulnerability-scanning-water-utilities**
13 **https://www.cisa.gov/known-exploited-vulnerabilities-catalog**
14 **https://www.cisa.gov/news-events/cybersecurity-advisories?f%5B0%5D=advisory_type%3A95**

8 Secure the Supply Chain (service providers, integrators, and other "trusted" third parties)

WHY THIS IS IMPORTANT FOR SMALL SYSTEMS: Engaging with third-party vendors expands a utility's attack surface whereby cyber threats can infiltrate a utility through its supply chain. Likewise, as third parties often have access to sensitive data/information, this necessitates regular assessments of third-party security postures.

A supply chain or third-party risk management strategy helps identify and mitigate potential threats and contributes to maintaining operational integrity by reducing the risk of disruption to critical (operational or business) processes due to third parties.

However, understanding supply chain risks can be particularly challenging for small utilities due to limited resources and lack of experience. It's not uncommon for small organizations to struggle with things like:

- Conducting due diligence and getting third parties to share sensitive information about their security practices. (CISA's *Secure by Design* guidance contains questions that utilities can use as a starting point to assess a third party's security practices).
- Effectively identifying and documenting all third-party relationships.
- Creating and enforcing robust vendor risk management policies.
- Developing and maintaining an effective incident response plan for third-party-related security incidents.

Abusing Trusted Relationships

As outlined in *Fundamental 3 | Create a Cyber Secure Culture and Protect from Insider Risks*, integrators, contractors, consultants, vendors, and other third parties represent potential (insider) threats to an organization. Additionally, these trusted third parties also constitute vital parts of the supply chain and must be managed effectively to reduce risk to your utility. In many cases, third parties represent a risk due to the expanded attack surface of just doing business with them. However, in recent years, threat actors have been actively and increasingly leveraging these trusted relationships as a cyber attack vector due to the effectiveness and potential for large-scale compromises. Furthermore, attackers are keenly aware that smaller businesses are not always as cyber secure as the larger companies with whom they contract, thus it's not uncommon for attackers to compromise smaller organizations to gain a foothold into larger entities.

Attackers typically gain initial access by compromising the credentials or systems of a trusted partner, such as an IT service provider, managed security provider, or systems integrator. As this attack vector continues to evolve, it's practical for organizations to prioritize technology controls that can detect and respond to these sophisticated tactics in real-time, while also fostering a culture of security awareness among employees and partners that it's okay to trust these third-party relationships, but they still must be verified.

RESOURCE | Secure by Demand Guide: How Software Customers Can Drive a Secure Technology Ecosystem[1]

Below are questions that utilities can use as a starting point for assessing a manufacturer's approach to product security or when in procurement discussions with third party integrators, resellers, or service providers.

To overcome these challenges, small utilities may wish to consider reaching out to larger utilities, prioritizing critical vendors, and focusing on essential risk management practices within their resource constraints.

- Has the manufacturer taken CISA's Secure by Design Pledge? What progress reports has the manufacturer published in line with its commitments to the pledge?
- How does the manufacturer make it simple for customers to install security patches? Does it offer support for security patches on a widespread basis and enable functionality for automatic updates?
- Does the manufacturer support integrating standards-based single sign-on (SSO) for customers at no additional cost? If the software manufacturer manages authentication, does it enable multi-factor authentication (MFA) or other phishing-resistant forms of authentication like passkeys by default, and at no cost?
- Has the software manufacturer eliminated default passwords in its products? If not, is it working to reduce the use of default passwords across its product lines?
- What classes of vulnerability has the software manufacturer systematically addressed in their products? For those that they haven't yet addressed, do they have a roadmap showing how they plan to eliminate those classes of vulnerability?
- Does the manufacturer generate a software bill of materials (SBOM) in a standard, machine-readable format and make this available to customers? Does the SBOM enumerate all third-party dependencies, including open source software components?
- How does the software manufacturer vet the security of open source software components it incorporates and facilitate contributions back to help sustain those open source projects? Does the software manufacturer have an established process to do so, such as through an open source program office (OSPO)?
- Does the software manufacturer include accurate Common Weakness Enumeration (CWE) and Common Platform Enumeration (CPE) fields in every CVE record for the software manufacturer's products?
- Has the software manufacturer published a vulnerability disclosure policy that authorizes testing by members of the public on products offered by the software manufacturer?

1 **https://www.cisa.gov/sites/default/files/2024-08/SecureByDemandGuide_080624_508c.pdf**

RECOMMENDED RESOURCES

NIST Cybersecurity Framework 2.0: Quick-Start Guide for Cybersecurity Supply Chain Risk Management (C-SCRM) | NIST

10 Questions to Ask Suppliers as Part of Third-Party Security Reviews | Dragos

Software in the Supply Chain: The Newest Insider Threat to ICS Networks | Dragos

Water Sector Cyber Resilience Briefing – You can Demand Secure by Design and Default (October 2024) | WaterISAC (members only access)

Software Bill of Materials (SBOM) | CISA

1620 I Street, NW, Suite 500
Washington, DC 20006
1-866-H2O-ISAC (1-866-426-4722)

waterisac

waterisac

waterisac.org/fundamentals