



12 Cybersecurity Fundamentals for Water and Wastewater Utilities

Recommended Practices to Reduce Exploitable Weaknesses
and Consequences of Attacks



Released: December 2024

waterisac.org/fundamentals



TABLE OF CONTENTS

Preface1

Fundamental 1
Plan for Incidents, Emergencies, and Disasters3

Fundamental 2
Minimize Control System Exposure12

Fundamental 3
Create a Cyber Secure Culture and Protect from Insider Risks21

Fundamental 4
Implement System Monitoring for Threat Detection and Alerting28

Fundamental 5
Account for Critical Assets 34

Fundamental 6
Enforce Access Controls39

Fundamental 7
Safeguard from Unauthorized Physical Access..... 48

Fundamental 8
Install Independent Cyber-Physical Safety Systems55

Fundamental 9
Embrace Risk-Based Vulnerability Management59

Fundamental 10
Develop and Enforce Cybersecurity Policies and Procedures (Governance)63

Fundamental 11
Secure the Supply Chain (service providers, integrators, and other
“trusted” third parties)65

Fundamental 12
Participate in Information Sharing and Collaboration Communities71

PREFACE

The last iteration of the *fundamentals* was published just under five years ago in 2019 and WaterISAC is excited to bring this refresh to our members and the larger water and wastewater systems sector.

- At that time, we went from 10 to 15.
- This time, we've condensed down to 12.

Why the change? A desire to make it a little more manageable, but still touch on key fundamentals that water and wastewater utilities should consider addressing.

What changed to get us from 15 to 12? A few things were combined, most notably:

- *Tackle Insider Threats* section was appropriately merged with building a cyber secure culture (this quarter's release).
- *Address All Smart Devices (IIoT, IoT, Mobile, etc.)* was consolidated with the fundamental on asset management (which will be released next quarter in June 2024).
- Among other things, given AWIA requirements it was decided that Assess Risks (risk assessments) is an "assumption" and as such there will be a discussion in the introduction.

What other changes? In an attempt to keep the fundamentals practical, especially for smaller systems to address, the refreshed fundamentals will be released in small manageable chunks - three per quarter (in March, June, September, and December).

- **Note:** the current 2019 version of WaterISAC's *15 Cybersecurity Fundamentals for Water and Wastewater Utilities* will remain on the website until the end of the year, so there will be a full set available until all 12 refreshed ones have been released.

What's new? While reviewing the 15 Fundamentals, we quickly realized that much of the information was still relevant and applicable and didn't see any reason to reinvent the wheel. However, there's been a lot of newly published guidance lately and updated information and resources over the past 5 years and we wanted to incorporate some of that into this document – kind of "mappings" to the relevant resources as appropriate.

- **One of the most significant updates to this version is extensive incorporation throughout each section of CISA's Cross-Sector Cybersecurity Performance Goals (CPGs)¹ and references to The Five ICS Cybersecurity Critical Controls.²**
- A "Why this is important" message.
- Also, in most of the *fundamentals* we've incorporated Small Systems Guidance.
- We've added a lot of visual elements. Everyone loves eye candy! Instead of just a bunch of words, we've added visual elements to emphasize the more practical/notable applications, information, resources, etc. Specifically, we've either added new or pulled out existing info that could be best described as:
 1. Practical Application
 2. For Consideration
 3. Risk Scenario
 4. Bonus Material
 5. *Additional Resources, Examples, How to get started, and more...*

Thank you for accessing WaterISAC's **12 Cybersecurity Fundamentals for Water and Wastewater Utilities** and we hope you appreciate the thoughtful updates. 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/>



Plan for Incidents, Emergencies, and Disasters

WHY THIS IS IMPORTANT: The inability to promptly and efficiently contain, mitigate, and communicate about cybersecurity incidents, emergencies, or disasters could result in significant operational disruption. Effective response plans will limit damage, reduce recovery time and costs, and increase confidence of partners and customers.

It might be surprising to find response planning at the beginning of a recommended practices guide. *The Five ICS Cybersecurity Critical Controls*¹ makes a solid case for prioritizing incident response planning, especially an **ICS-specific Incident Response Plan** over other fundamentals, practices, or controls. As response plans are developed, utilities may find the planning activity extremely useful for identifying significant cybersecurity and continuity of operations gaps, and informing subsequent best practices for implementation.



Practical Application

Effectively responding to a cyber incident or attack requires things like logging to be in-place and properly configured. The lack of sufficient log data hinders incident response efforts by reducing visibility and delaying incident identification. Cyber Incident Response Plan (CIRP) development would help identify if logs are available and effectively configured.

Five ICS Cybersecurity Critical Controls | 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.**

RESOURCE | Dragos OT-CERT Host-Based Logging Guidance

Members of Dragos OT-CERT have access to *Host-Based Logging Guidance: Instructions for Managing Windows Event Logs*. In addition, OT-CERT has jump start videos which provide demonstrations of everything covered in the guide.



BONUS MATERIAL | Mandiant DFIR Framework for Embedded Systems

Collecting and analyzing forensic data is a core component of the incident response process. This process is central to determining the existence, and subsequent scope of a compromise, the tools used by adversaries, and their capabilities. However, obtaining digital forensics and incident response (DFIR) data is not always a simple task, especially when operational technology (OT) systems are involved. Mandiant's DFIR Framework for Embedded Systems is comprised of three steps focused on preparation and gathering information from embedded devices during the early stages of the incident response process.

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.

¹ <https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/>

These plans should not be developed by a single department, but rather in collaboration with teams across all departments. Including external stakeholders such as emergency response and law enforcement authorities in the development of the plans can also be valuable. This holistic inclusion will ensure a cooperative and unified response that leverages all organizational resources for more accurate plans.

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.

CPG | 5.A Incident Planning and Preparedness

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

In January 2024, CISA, EPA, and FBI, as well as the federal government and WWS Sector partners created an Incident Response Guide (IRG) for Water and Wastewater Sector.² The unique value of this IRG is that it provides water and wastewater sector owners and operators information about the federal roles, resources, and responsibilities for each stage of the cyber incident response lifecycle. Sector owners and operators can use this information to augment their respective IR plans and procedures.

RESOURCE | Incident Response RACI Matrix

Red Canary has developed a fully customizable Incident Response RACI matrix³ to help visualize and manage the delegation of responsibilities as they relate to significant incidents. This matrix is also a useful tool for understanding incident response in the context of business, while pinpointing areas for improvement.

Cyber Incident Response Plan

Despite established safeguards, many organizations still experience cybersecurity compromises. Indeed, experts note experiencing a compromise is not a matter of if, but when. However, organizations that fare best will be those that are able to quickly detect the intrusion (Fundamental 4)⁴ and have a defined plan in place to respond. An effective CIRP will limit damage, increase confidence of partners and customers, and reduce recovery time and costs. Furthermore, the incident response plan needs to be in place before an incident occurs and should be incorporated into organizational business continuity plans.

For Consideration

The value of CIRPs is priceless. However, Talos Intelligence outlines seven common mistakes⁵ that organizations make when creating or updating an incident response plan. Avoiding some of these pitfalls ensures your utility's plan will be updated faster and is more thorough, so you are ready to act when, not if, an incident happens.

Pitfalls to avoid when creating an Incident Response Plan

TALOS




Failing to define a document hierarchy



Being too general



Being too specific




Writing in isolation



Not testing the IR plan



Letting it go stale



Being too IT focused

² https://www.cisa.gov/sites/default/files/2024-01/WWS-Sector_Incident-Response-Guide.pdf
³ <https://redcanary.com/blog/incident-response-and-readiness-guide/>
⁴ Fundamental 4 | Implement Threat Detection and Monitoring will be released in June 2024
⁵ <https://blog.talosintelligence.com/seven-common-mistakes-companies-make-when-creating-an-incident-response-plan-and-how-to-avoid-them/>

Two recommendations to include in the CIRP are:

- emergency operating procedures for industrial process operation – at least as appendices or in references. It's important to plan in advance for how water operations staff will maintain system operations during an incident, with potentially degraded capability.
- pre-planned steps for common or high impact incident scenarios, such as a ransomware infection, compromise of remote access, or a loss of a critical function. (In other words, according to the *Five ICS Cybersecurity Critical Controls*, these intelligence-driven, common, or high-impact scenarios should be prioritized because the likelihood of them being repeatable is high. Additionally, they are real-world scenarios that have already happened, and because there are a small enough number, they can serve as especially useful focus areas.)

Proactively considering the details of maintaining operations during these incidents in advance will also result in improved response effectiveness, and likely reduce impacts and time to recover.

Cyber Incident Response Team

For enhanced response capability in the event of a cybersecurity incident, organizations should consider forming a cyber incident response team to develop and manage the incident response process. The security operations center is responsible for day-to-day investigations, but a separate team should be established to respond to critical cybersecurity incidents. The cyber incident response team should develop the incident response governance model (Fundamental 10),⁶ including defining the types and severity of incidents that will require a comprehensive response.

The cyber incident response team should be comprised of organizational stakeholders, including other departments and external entities. In addition to IT and OT security staff and operators, team composition should include other staff such as executives, communications and public relations teams, human resources, legal, product, and engineering personnel.

System Backups

System backups play a critical role in timely recovery and reducing the risk of data destruction or inhibiting system recovery after a cyber incident. Backups need to be protected from the risk of being corrupted or destroyed (such as during a ransomware attack), validated, and tested to ensure effective recovery when needed.

Restoration from backups need to be tested periodically. Assuming backups can be used for restoration without verifying efficacy through test restorations can often prove costly. It is also recommended to take the time to create human readable backups in addition to automated/native backup functions. In the event replacement devices cannot use the automated backup file, the human readable version will increase the efficiency of restoration.



Practical Application

Use resource planning tools, such as automatically generated work orders to have staff verify data back up integrity, rotate backup media, locate backup files, and perform test restorations from backups.

CPG | 2.R System Backups

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

Cyber Insurance

Recovering from a cyber incident can be expensive. Average estimates for the cost of cyber attacks run from tens of thousands of dollars for small organizations to millions of dollars for large organizations. Expenses can include emergency support of vendors that specialize in incident forensics and recovery, replacement of corrupted software, computers and other hardware, complimentary credit monitoring for customers whose data was stolen, customer notification, lost productivity of employees who cannot work until the system has been restored, legal fees and liabilities, and even public relations outreach.

⁶ Fundamental 10 | Develop and Enforce Cybersecurity Policies and Procedures is scheduled to be released in December 2024

Cyber insurance is a tool in the resilience toolkit. Not only can insurers reimburse or pay for some or all expenses listed above, many policies provide expert emergency support in the form of knowledge and vendors and contractors specializing in forensics and recovery. While cyber insurance has matured, there is still a lack of standardization across policies, so researching insurers, comparing policies, and “right-sizing” a policy is important.

For instance, some policies may not pay claims for pre-existing breaches, acts of war, or if the cause of the breach was an employee who fell victim to a phishing email or other social engineering tactic. Most insurers insist on minimum required security controls, risk assessment, or cyber risk profile before granting a policy.

Disaster Response Plans

Under America’s Water Infrastructure Act, drinking water systems must develop emergency response plans (ERPs) and update them every five years. The plans must address both cyber systems and physical systems. The plans required under the act go beyond emergency response. The law’s provisions also require utilities to document how they will mitigate threats and how they will enhance mitigation and resilience.

While ERPs are not required for wastewater utilities under the law, these utilities may find it useful to prepare them. Regardless of the law, these plans can provide guidance during times of heightened confusion or stress. For this reason, plans help reduce the severity of impacts and facilitate a faster recovery for the system and the affected organization’s overall operations.

IT and OT professionals may be more familiar with the concept of the disaster response plan (DRP), which can be folded into a utility’s ERP. Both documents are traditionally part of an organization’s business continuity plan or continuity of operations plan, which is described in the Water Research Foundation’s *Business Continuity Planning for Water Utilities*.

During the preparation of the emergency response plan, input should be obtained from various stakeholders, which can include personnel from IT, OT, physical security departments of the organization, and external partners. All stakeholders should regularly train on and exercise the plan.

DRPs can include:

- A list of major goals of the disaster plan.
- Names and contact information of IT and OT personnel, vendors, and contract support.
- Roles and responsibilities.
- Profiles of software and hardware used by the utility, including a discussion of which utility functions rely on each software and hardware item.
- Service level agreements for outsourced services during a disaster.
- Recovery time objectives.
- Maximum tolerable downtime.
- Backup procedures.
- Plans for mobilizing to temporary work locations.
- Plans for backing up to a temporary site.
- Plans for restoring the home site.
- Plans for testing and exercising the DRP.

Backup Out-of-Band Communications

Does your utility have a backup communications plan? It is important to consider such critical response dependencies before an incident occurs. Out-of-band communications play a vital role during incident response by providing alternative methods or technologies that enable teams to maintain secure communications during an incident. For example, the email server may be down due to a compromise or ransomware attack, the internet may be out due a DDoS attack – or worse, the incident could coincide with larger regional incidents which could likely result in cellular carrier capacity becoming saturated. Therefore, it is important to consider how response would be impacted if communication mechanisms were not available.

For Consideration

When choosing out-of-band communications, utilities may wish to consider the following:

- What common dependencies does it share with your primary communications mechanism?
- Are the cyber incident response and operations teams onboarded to that mechanism?
- Is the backup communications mechanism encrypted?
- Does your utility have two-way radios?
- Is your utility signed up for telecommunications priority services⁷ such as Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS)?

Power Resilience

Utilities require power to operate their IT and ICS equipment, and they can protect their systems against the impacts of power outages by having on-site generation available in emergencies. Generators can be either utility-owned or supplied during an incident through preexisting contracts. NIST encourages utilities to have an uninterruptible on-site power supply that can span the time between when power is lost, and emergency power generation is activated. Utilities should also have plans in place to ensure that generators will have adequate fuel throughout an emergency. Water utilities can also coordinate with their local power utility to ensure that critical facilities are a high priority during power restoration efforts. Additional information about power outage resilience is available on WaterISAC's "Power Outage and Black Sky Resilience resources" web page.

For Consideration

It is important to consider protecting automatic transfer switches (ATS) and intelligent circuit breakers once you start to think about the cyber in power dependency. If your ATS is on the network, it can become a single point of failure for both utility and emergency power. The same considerations should be addressed with network connected uninterruptible power supplies (UPS).

Practice Makes Proficient

As is true for all response and recovery plans, CIRPs and DRPs are not complete once they have been developed. The plans need to be operationalized, regularly reviewed, practiced, and updated accordingly. Organizations should practice their plans through regular operational and tabletop exercises (TTXs). To further test readiness, consider incorporating a red team and/or blue team approach to the exercises. Additionally, purple teaming⁸ exercises will promote enhanced collaboration between red and blue teams.

Tabletop Exercises (TTXs)

As stated, utilities are highly encouraged to practice CIRPs through workshops and tabletop exercises (TTXs). There are multiple options available for exercising, from a basic workshop discussion to full-scale and coordinated functional exercise. CISA offers several TTX options, from self-service to end-to-end exercise planning and conduct support, to assist utilities in examining their cybersecurity plans and capabilities.

*CISA Tabletop Exercise Packages (CTEPs)*⁹ are a comprehensive set of resources designed to assist stakeholders in conducting their own exercises. Each package is customizable and includes template exercise objectives, scenarios, and discussion questions as well as a collection of references and resources. CTEPs cybersecurity scenarios cover various cyber threat vector topics such as ransomware, insider threats, phishing, and **industrial controls**. CTEPs also include physical scenarios and cyber-physical convergence scenarios. **The cybersecurity¹⁰ and cyber-physical convergence¹¹ scenarios include exercises specifically designed for Water and Wastewater Systems.**

Utilities may wish to engage external entities to help plan, develop, and execute exercises. Through its Stakeholder Exercises,¹² CISA offers fully supported end-to-end exercise planning and conduct support. NCEP support includes planning meetings, document and scenario development, facilitation, and after-action report development. Utilities can participate in CISA-led discussion-based exercises in the form of seminars or workshops. Stakeholder exercises also support operations-based exercises that leverage functional and full-scale drills to test security plans and capabilities more comprehensively.

⁷ <https://www.cisa.gov/topics/emergency-communications/priority-services>

⁸ <https://scythe.io/roles/purple-teaming>

⁹ <https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages>

¹⁰ <https://www.cisa.gov/resources-tools/resources/cybersecurity-scenarios>

¹¹ <https://www.cisa.gov/resources-tools/resources/cyber-physical-convergence-scenarios>

¹² <https://www.cisa.gov/resources-tools/services/stakeholder-exercises>

There are also private options such as WaterISAC Champion organizations, Gate 15 and Dragos, that support various exercise activities. Gate 15¹³ specializes in activities such as TTXs, drills, continuous improvement workshops, and more. Dragos TTX Service¹⁴ can help test and strengthen your ICS cybersecurity strategy in a collaborative workshop. When engaging private third parties, to ensure a cohesive experience, WaterISAC recommends working with firms that use the FEMA *Homeland Security Exercise and Evaluation Program (HSEEP)*¹⁵ principles. HSEEP provides a set of guiding principles for exercise and evaluation programs, as well as a common approach to exercise program management, design and development, conduct, evaluation, and improvement planning.

There are additional opportunities to participate in exercises on a regional or national level that incorporate multiple stakeholders across multiple critical infrastructure sectors to practice responding

to and recovering from coordinated cyber and physical security threats and incidents.

*Cyber Storm*¹⁶ is a CISA-sponsored cybersecurity exercise focused on policy, procedure, information sharing, coordination, and decision-making. The exercise provides a venue to simulate discovery of and response to a large-scale, coordinated cyber-attack impacting critical infrastructure, and an opportunity for the Federal Government, SLTT organizations, and the private sector to address cyber incident response as a community.

*GridEx*¹⁷ is the largest grid security exercise in North America. It is hosted every two years by NERC's Electricity ISAC (E-ISAC).

*Black Sky Exercise*¹⁸ allows organizations to perform a reality check in a no-fault environment without a bad day happening. It allows discretionary time to prepare for that rare but very possible Black Sky Event.¹⁹

BONUS MATERIAL | Critical infrastructure cybersecurity prioritization: A cross-sector methodology for ranking operational technology cyber scenarios and critical entities²⁰

Today, critical infrastructure cyber protection correlates sixteen different sectors, with no way to compare a standardized risk metric from a municipal water facility in Wyoming with a large commercial energy provider in Florida or a rural hospital in Texas with a train operator in New York. This section proposes a scoring methodology for cross-sector entity prioritization using qualitative scenario planning and quantitative indicators for severity scoring, assessing the potential for scenarios to cause public panic and to stress/overcome local, state, and federal response capacity.

This methodology has two primary use cases:

1. The scoring matrix provides a way to rank and prioritize relevant cyber scenarios for a single entity, organization, facility, or site in scope.
 - a. The ranking, based on weighted scores, will allow any entity, organization, facility, or site to choose scenarios to exercise based on a choice of two real-world impacts (impact A, impact B) or to assess both impacts when choosing a tabletop scenario.

- b. This ranking has the potential to prioritize scenarios that will cause public panic and/or overwhelm response resources over scenarios that simply have a higher cyber severity rating (see Table 1).

2. The standardized priority score provides an overall priority score for the entity, organization, facility, or site.

- a. This score can be used to compare and rank different entities, locations, facilities, or sites within a given jurisdiction—city or local, state, federal, sector-specific, etc.

This methodology can be incorporated into assessments, training, and tabletop exercises in the planning phase of cyber risk mitigation and incident response. It can also be used by leaders to prioritize multiple critical infrastructure sectors or locations in their jurisdiction from a cybersecurity perspective.

¹³ <https://gate15.global/services/>

¹⁴ <https://www.dragos.com/tabletop-exercise/>

¹⁵ <https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep>

¹⁶ <https://www.cisa.gov/resources-tools/services/cyber-storm>

¹⁷ <https://www.nerc.com/pa/CI/ESISAC/Pages/GridEx.aspx>

¹⁸ <https://eiscouncil.org/what-is-a-black-sky-exercise/>

¹⁹ <https://eiscouncil.org/black-sky/>

²⁰ <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/critical-infrastructure-cybersecurity-prioritization/#introduction>



For Consideration

A fun and engaging exercise option is Backdoors & Breaches, an Incident Response Card Game,²¹ from Black Hills Information Security and Active Countermeasures. Backdoors & Breaches contains 52 unique cards to help you conduct incident response tabletop exercises and learn attack tactics, tools, and methods. To enhance play even more, there are several expansion decks available, including ICS/OT, cloud security, and more.

Manual Operations

Manual control of water and wastewater systems should also be practiced as part of IR procedures to help understand limitations and inform design enhancements that can make future manual control more efficient.

IR plans should include measures for reacting to destructive malware in an ICS environment. In such situations, organizations should be prepared to

restore from off-line backups and to “island” their ICS environments by disconnecting from non-ICS networks. They should also be prepared to revert to manual operations if network conditions impact visibility from the SCADA system, or if malware potentially renders control devices inoperable or untrustworthy.

Practice ensures that all stakeholders understand the procedures that would be implemented in the event of a significant cyber disruption or breach, enabling a more effective and efficient response.



Practical Application

Use organizational resource planning tools, such as automatically generated work orders, to have operations operate in manual mode. This will create the muscle memory for operating that mode during an incident under more stressful conditions.

²¹ <https://www.blackhillsinfosec.com/projects/backdoorsandbreaches/>

SMALL SYSTEMS GUIDANCE

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.*²²

For Consideration

Executing low-cost ransomware or cyber-event tabletop (TTX) or paper-based training has several benefits:

- It raises awareness within the organization about the current state of maturity and incident/event preparedness.
- It satisfies a compliance or framework checkbox.
- Such training offers a low-cost, high-reward way to illuminate gaps that could threaten the organization's overall event response.
- The exercises can be devised internally by individuals who understand how the facilities actually run.
- It brings all parties to the table and settles disputes over who owns what.
- Communication/collaboration driven by the tabletops often facilitate organizational change and foster improved inter-domain trust.



RECOMMENDED RESOURCE

Dragos OT-CERT²³ 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



²² <https://verveindustrial.com/resources/blog/getting-prepared-tabletops-and-scripts-to-act-through-a-ransomware-event/>
²³ <https://ot-cert.dragos.com/>

RECOMMENDED RESOURCES

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

CISA Tabletop Exercise Packages (CTEP) | CISA

Stakeholder Exercises | CISA

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

Cybersecurity Incident & Vulnerability Response Playbooks | CISA

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

Cyber Storm | CISA

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

GridEx | Electricity ISAC (E-ISAC)

Homeland Security Exercise and Evaluation Program (HSEEP) | FEMA

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

Backdoors & Breaches, an Incident Response Card Game | Black Hills Information Security & Active Countermeasures

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

From reaction to resilience: Our reimagined Incident Response & Readiness Guide | Red Canary

Is your IR plan DOA? | Red Canary

7 common mistakes companies make when creating an incident response plan and how to avoid them | Talos Intelligence

Getting Prepared: Tabletops and Scripts to Act Through a Ransomware Event | VERVE – A Rockwell Automation Company

Power Outage and Black Sky Resilience Resources | WaterISAC

Emergency Planning for Water & Wastewater Utilities - M19 | AWWA

Business Continuity Planning for Water Utilities | WRF

Introducing Mandiant's Digital Forensics and Incident Response Framework for Embedded OT Systems | Mandiant

How to Manage the Rising Cost of OT Cyber Insurance | VERVE – A Rockwell Automation Company

2

Minimize Control System Exposure

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

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 Controls¹ | 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.

CPC | 2.X Limit OT Connections to Public Internet

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

According to **NIST Special Publication NIST SP 800-82r3 Guide to Operational Technology (OT) Security** (September 2023),² minimizing control system exposure encompasses (but is not limited to) the following:

- Implementing a network topology for the OT system that has multiple layers, with the most critical communications occurring in the most secure and reliable layer.
- Providing logical separation between the corporate and OT networks (e.g., stateful inspection firewalls between the networks, unidirectional gateways).
- Considering where physical separation may be required as opposed to logical separation.
- Employing a DMZ network architecture (e.g., prevent direct traffic between the corporate and OT networks).
- Using multi-factor authentication for remote access to the OT system.
- Restricting physical access to the OT network and devices. *This will be discussed further in Fundamental 7.*
- Applying security techniques, such as encryption and/or cryptographic hashes, to OT data storage and communications where appropriate.

¹ <https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/>

² <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf>

External (Untrusted) Pathways

The control systems of some utilities may not directly face the internet. However, a connection likely exists if those systems are connected to another part of the network, such as the enterprise IT network that has a communication pathway to or from the internet. These connections can be identified through a comprehensive asset inventory (Fundamental 5)³ and evaluated with a thorough risk assessment.

It is not uncommon for compromises to ICS networks to emanate from the IT/business network. Therefore, it is vital to eliminate any unnecessary communication channels discovered between devices on the control system network and equipment on other networks. Any connections that remain need to be carefully evaluated and managed to reduce network vulnerabilities.

Segmentation

Access to network segments can be restricted by physically isolating them entirely from one another, which is optimal for industrial control systems, or by implementing technologies such as firewalls, demilitarized zones (DMZs), virtual local area networks (VLANs), and unidirectional gateways/data diodes.

- **Firewalls** are a hardware device or software program that filter inbound and outbound traffic between different parts of a network, or between a network and the internet.
- **ICS-DMZs** are a network segment that sit between the control system network and any untrusted or other internal network to protect unwanted traffic from communicating directly with critical devices within the control system zones.
- **VLANs** are logical connections that partition different segments of a network, often by function.
- **Unidirectional gateways** and **data diodes** allow for one-way traffic from the control system network and prevent traffic from flowing back into the control system network.



RISK SCENARIO

A utility may have equipment or components that use Bluetooth or other short-range communications protocol for configuration. Despite the limited communication range of such devices, these connections represent another entry point for an adversary. Organizations may be unaware of these short-range connections, but cyber threat actors can find such pathways to access and exploit industrial control systems.

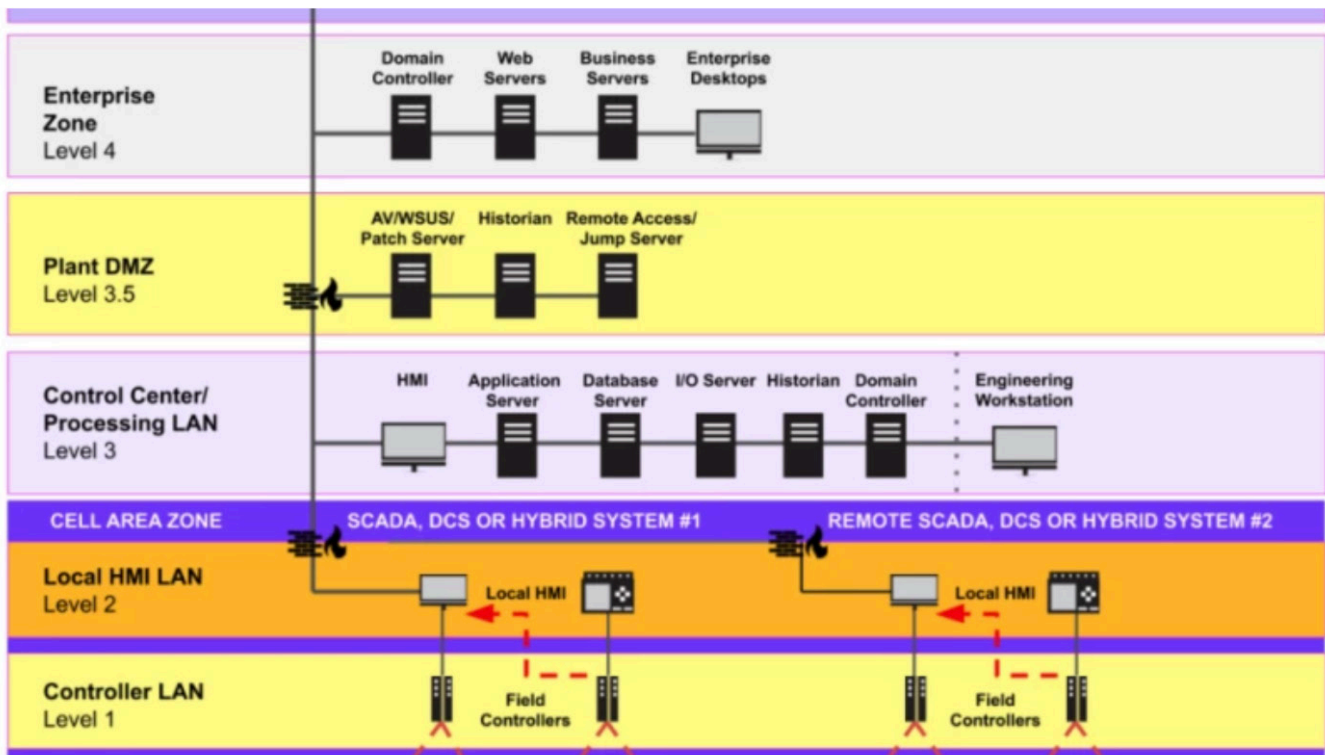
CPG | 2.F Network Segmentation

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

³ Fundamental 5 – Accounting of Assets will be released June 2024

Zone Restrictions

Network segmentation also entails classifying and categorizing IT and ICS/OT assets, data, and personnel into specific groups or zones, and restricting access based on these groupings. By placing resources into different segments of a network, and restricting access to specific zones, a compromise of one device or system is less likely to translate into the exploitation of the entire system. The Purdue model in the image below is used to best illustrate industrial network zones.



This diagram shows the standard architecture of an industrial network configured according to the Purdue Model. Industrial devices are located at levels 0 through 3.⁴

When computer systems are interconnected, cyber threat actors may be able to exploit any vulnerability within an organization's network to gain entry and move laterally throughout the environment to access sensitive equipment and data.

Restrict Traffic

When installed and configured properly, firewalls, ICS-DMZs, VLANs, and unidirectional gateways/data diodes provide crucial functions in filtering or blocking unwanted traffic that could adversely impact availability, reliability, and safety of the control system network. By reducing the number of pathways into and between networks and by properly implementing security protocols on the pathways that do exist, it is much more difficult for a threat actor to compromise the network and gain access to other systems.

Creating network boundaries and segments and classifying assets and data empowers an organization to enforce both detection and

protection controls within its infrastructure. The capability to monitor, restrict, and govern communication flows enables defenders to baseline network traffic, especially traffic traversing a network boundary, and identify anomalous or suspicious communication flows. To ensure unwanted traffic is not traversing the network, firewall and segmentation rules should be reviewed regularly and validated with packet inspection of network traffic to assess the status of unnecessary ports or services.

Ensure assets don't have unknown internet connectivity. As adversaries and red teams gain access to a new asset, it is common practice to test for external connectivity. It is not uncommon to find a particular asset that has unknown or forgotten connectivity to external or untrusted networks. When an artifact like that is discovered, it is often used as a mechanism to establish command and control traffic and persistence within the environment.

⁴ <https://claroty.com/blog/ics-security-the-purdue-model>

Encrypted Communications

Another way to limit control system exposure is to encrypt all communications. Encryption can protect control system maintenance traffic on an internal network, external remote access traffic destined to the control system, or device-to-device traffic over the public telecommunications network or private radio network.

Protocols like IPSec can be used to encrypt traffic over a public telecommunications network. Built-in encryption options or add-on serial traffic encryption devices can be used to protect data radio communications. Encryption makes it very difficult for malicious actors to fake or intercept control system traffic.

For Consideration

While it's desirable to encrypt all traffic on the local area network, it may not be practical and could be cost prohibitive for some organizations to perform packet inspection of the encrypted traffic. Two alternatives for consideration are follows:

- Allow local LAN traffic to remain unencrypted to enable network monitoring and apply encryption as traffic leaves the electronic security perimeter.
- Apply IPSec encryption for the authentication process only. This approach provides data integrity to prevent malicious manipulation but still allows asset owners to perform traffic inspection without the cost of decrypting and re-encrypting the traffic.

Restrictive Procedures

Only dedicated and properly secured devices should be permitted within the control system environment. This restriction applies to laptops, USB memory flash drives, backup hard drives, and any other device that could be infected with malware, including mobile, and "internet of things" (IoT) devices. Each device that has been vetted should be clearly marked. This procedure is required for everyone – staff, contractors, consultants, and vendors.

CPG | 2.V Prohibit Connection of Unauthorized Devices

- Organizations maintain policies and processes to ensure that unauthorized media and hardware are not connected to IT and OT assets, such as by limiting use of USB devices and removable media or disabling AutoRun.
- OT: When feasible, establish procedures to remove, disable, or otherwise secure physical ports to prevent the connection of unauthorized devices, or establish procedures for granting access through approved exceptions.

Practical Application

During periods of large-scale control system enhancements or upgrades, additional restrictive measures may be needed, such as requiring the integrator to use utility owned laptops and software, or possibly developing and testing the new system on a parallel network not connected to the active control system.

While external connections to the control network should always be disabled, that may not be practical. There are instances where a connection is necessary and exceptions must be made for updates, remote administration, vendor access, or other reasons. In these instances, employing an ICS-DMZ is necessary to secure the communication pathways between the networks for those occasions when secure access is temporarily enabled.

Once access is no longer needed, connections must be disabled immediately. Never leave a connection to the control network enabled for an undetermined timeframe. Likewise, in lieu of enabling temporary network access, consider requiring the use of a dedicated and hardened, non-ICS connected PC for things like patch downloads. Downloads should be scanned for malicious content, and cryptographic hashes or digital signatures validated before applying to control system devices.



Practical Application

Hunting for unknown or undocumented connectivity in your ICS/OT environment is not complicated. There are simple, native, non-intrusive commands to test the assets in your environment for external connectivity.

Two very useful command-line/terminal commands are **ping** and **netstat**. The quickest way to check an asset for external connectivity is to check for reachability to an external destination. Google's public DNS IP address (8.8.8.8) is a good test. Likewise, assets should be checked for additional network connections. The following images demonstrate how the **ping** and **netstat** commands are easily executed for each function.

Ping 8.8.8.8

```
Command Prompt
Microsoft Windows [Version 10.0.22621.963]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ExampleUser>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=22ms TTL=55
Reply from 8.8.8.8: bytes=32 time=25ms TTL=55
Reply from 8.8.8.8: bytes=32 time=27ms TTL=55
Reply from 8.8.8.8: bytes=32 time=24ms TTL=55

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 22ms, Maximum = 27ms, Average = 24ms

C:\Users\ExampleUser>
```

Netstat -nao > Netstat_info.txt

```
Command Prompt - netstat
TCP        127.0.0.1:9089          0.0.0.0:0             LISTENING   14280
TCP        127.0.0.1:28385        0.0.0.0:0             LISTENING   4
TCP        127.0.0.1:28390        0.0.0.0:0             LISTENING   4
TCP        127.0.0.1:63227       127.0.0.1:63228       ESTABLISHED 4472
TCP        127.0.0.1:63228       127.0.0.1:63227       ESTABLISHED 4472
TCP        172.16.0.36:139       0.0.0.0:0             LISTENING   4
TCP        172.16.0.36:49408      52.159.127.243:443     ESTABLISHED 4076
TCP        172.16.0.36:49742      40.74.108.123:443      ESTABLISHED 10180
TCP        172.16.0.36:50395     72.21.91.29:80         CLOSE_WAIT  7536
TCP        172.16.0.36:50399   13.107.246.36:443      CLOSE_WAIT  7536
TCP        172.16.0.36:63223   170.114.52.2:443       CLOSE_WAIT  9892
TCP        172.16.0.36:63224   170.114.52.2:443       CLOSE_WAIT  9892
TCP        172.16.0.36:63225   13.249.181.243:443     CLOSE_WAIT  9892
TCP        172.16.0.36:63230   13.249.181.243:443     CLOSE_WAIT  9892
TCP        172.16.0.36:63235   206.247.77.208:443     ESTABLISHED 4472
TCP        172.16.0.36:63336   204.79.197.200:443     TIME_WAIT   0
TCP        172.16.0.36:63337   204.79.197.200:443     TIME_WAIT   0
TCP        172.16.0.36:63338   13.59.123.141:443      ESTABLISHED 4472
TCP        172.16.0.36:63339   204.79.197.200:443     ESTABLISHED 11900
TCP        172.16.0.36:63340   20.140.147.200:443     ESTABLISHED 11900
TCP        172.16.0.36:63341   72.21.91.29:80         ESTABLISHED 11900
TCP        172.16.0.36:63342   13.107.3.254:443       ESTABLISHED 11900
TCP        172.16.0.36:63343   72.21.81.200:443       ESTABLISHED 11900
TCP        172.16.0.36:63344   172.64.142.36:80       ESTABLISHED 8884
TCP        172.16.0.36:63345   172.64.142.36:443      ESTABLISHED 8884
TCP        172.16.0.36:63346   204.79.197.222:443     ESTABLISHED 11900
TCP        172.16.0.36:63347   20.189.173.1:443       ESTABLISHED 12380
TCP        172.16.0.36:63348   52.113.196.254:443     ESTABLISHED 11900
TCP        172.16.0.36:63349   13.107.237.36:443      ESTABLISHED 11900
TCP        172.16.0.36:63350   13.107.18.254:443      ESTABLISHED 11900
```

In this example, the netstat output is sent to a text file so the results can be reviewed for legitimate connections and any undesirable connections (internal or external) can be addressed accordingly.

Secure Remote Access

Remote access has become part of normal operations in industrial environments. The ability to remotely connect to a network adds a great deal of convenience for end users, engineers, systems administrators, integrators, and support vendors. However, it also provides an opportunity for threat actors to infiltrate the network. Methods of remotely connecting securely should be implemented to minimize risk. Implementing a secure remote access architecture for the ICS environment is so important and necessary that it is one of the *Five ICS Cybersecurity Critical Controls* (Control No. 4) which states, establishing secure remote access is a must in modern-day industrial operations.

Firewalls, demilitarized zones, jump servers, virtual private networks (VPNs), secure shell (SSH), multifactor authentication (MFA), and many commercial solutions are viable options that provide increased security when remote access is required. Additionally, remote access can further be restricted with access control lists that only allow access from specific IP addresses and/or ranges and geographic locations (Fundamental 6).

When implementing a secure remote access solution, Dragos recommends:⁵

- Leveraging existing infrastructure and expertise.
- Implementing a DMZ with a secure jump host.
- Multi-factor authentication (MFA).
- Third-party remote access requirements.
- Monitoring and auditing of remote access sessions.

Jump Servers

Jump servers are intermediate servers that reside in the demilitarized zone (DMZ). When remote access is required, jump servers are used for authentication and to provide connectivity to less secure remote servers in the control network. Jump servers provide the ability for remote users to connect to an intermediary device without having to connect directly to other control network servers, workstations, or other less secure devices.

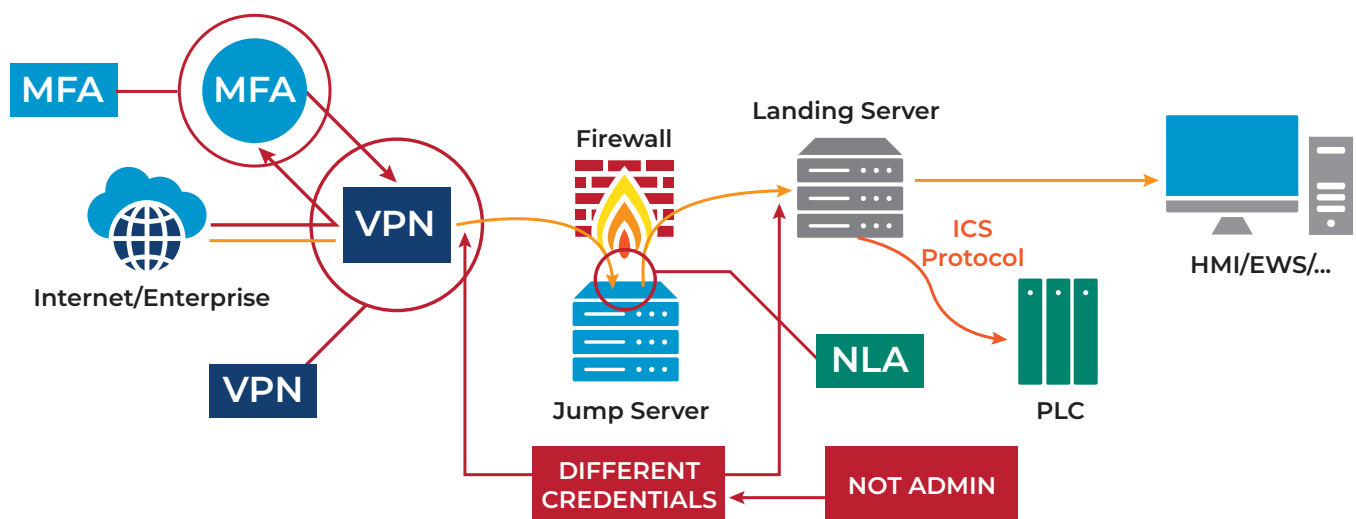
VPN

A VPN is an encrypted data channel to securely send and receive data via public IT infrastructure (such as the internet,) or to securely connect to the control network from other segments of the enterprise network. Through a VPN, users can remotely access internal resources like files, printers, databases, websites, and management interfaces as if directly connected to the network. However, a VPN is only as secure as the devices connected to it; an authorized device infected with malware can still propagate that malware onto the network, leading to additional infections and negating the security of the VPN.

SSH

SSH provides secure authentication and authorization to hosts when remote administration is required. SSH is used to safely and remotely connect to devices to perform management or file transfer activities. It should be disabled by default and access granted only to explicitly defined hosts and networks.

Minimum Baseline Architecture for ICS/OT Secure Remote Access



⁵ <https://www.dragos.com/blog/recommendations-to-implement-secure-remote-access-today/>

Securing Programmable Logic Controllers

Another facet of minimizing control system exposure and implementing a defensible architecture involves hardening control system engineering devices including supervisory control and data acquisition (SCADA), distributed control systems (DCS), programmable logic controllers (PLCs), etc. This section specifically discusses securing PLCs. *In a way, PLCs are the quintessential OT. PLCs are the devices that are deterministic, have real-time capabilities, operate in rough environments, and often run decades without being substituted* (Fluchs, 2022).⁶ PLCs are often (and aptly) described as insecure-by-design, but they don't have to stay that way anymore.

Until 2021, there was no standard PLC security guidance. The industry lacked a common reference to leverage PLCs' built-in security capabilities or to address threats and vulnerabilities – let alone an effective way to implement secure coding. In 2021, the first of its kind guidance resource to help secure the inherently insecure-by-design PLCs was published. *The Top 20 Secure PLC Coding Practices (Version 1.0, published 15 June 2021)* were written by engineers for engineers and technicians that program and maintain PLCs.⁷ The following are examples from the *Top 20 Secure PLC Coding Practices*.

EXAMPLES | 20 Secure PLC Coding Practices

2. Track operating modes

Keep the PLC in RUN mode. If PLCs are not in RUN mode, there should be an alarm to the operators.

Security Objective	Target Group
Integrity of PLC logic	Integration / Maintenance Service Provider Asset Owner

3. Leave operational logic in the PLC wherever feasible

Leave as much operational logic e.g., totalizing or integrating, as possible directly in the PLC. The HMI does not get enough updates to do this well.

Security Objective	Target Group
Integrity of PLC logic	Product Supplier Integration / Maintenance Service Provider Asset Owner

19. Monitor PLC memory usage and trend it on the HMI

Measure and provide a baseline for memory usage for every controller deployed in the production environment and trend it on the HMI.

Security Objective	Target Group
Monitoring	Integration / Maintenance Service Provider Asset Owner

⁶ <https://fluchsfriktion.medium.com/one-year-of-top-20-secure-plc-coding-practices-c2f0042ad4a2>

⁷ Background: The idea of secure coding practices for PLCs was the brainchild of water sector veteran Jake Brodsky and was presented during an S4x20 Conference session.

The coding practices are intended to be used by automation engineers and technicians that program and maintain PLCs. Moreover, these practices are designed to be implemented with native PLC functionality to securely program PLCs with little to no additional software tools or hardware to increase PLC integrity, monitoring, hardening, and resilience. Additional benefits of these coding practices are that they are not an all or nothing approach and can be applied to existing architecture. There is no need to wait until an infrastructure upgrade or greenfield project to start securing PLCs.

EXAMPLE | Template for RFP Language for PLC Security

If your utility outsources SCADA support, be intentional about asking if secure coding practices such as these are being implemented on your project. Likewise, include this as a requirement in your next RFP. PLC Security has provided a sample template for public use.

This Specification sample document is focused on outlining requirements inspired by the Top 20 list for vendor control equipment (e.g., a new process unit is being added to the facility and a vendor skid package with a vendor template design and program). These requirements or the policy can be developed and provided to the vendor to improve the security and integration while beginning to adopt the practices. See **Cybersecurity PLC Vendor Policy Example** in the Resources section.

Zero Trust in OT Networks

According to CISA's Zero Trust Maturity Model,⁸ zero trust provides a collection of concepts and ideas designed to **minimize uncertainty** in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. **The goal is to prevent unauthorized access to data and services and make access control enforcement as granular as possible.**

Given the criticality, OT networks should epitomize the concept of zero trust. Unfortunately, that isn't always easy. However, many zero trust components enforce the concepts discussed in this fundamental and those that will be discussed in Fundamental 6, Enforce Access Controls. Consider the following inset box which has been excerpted from the Software Engineering Institute on how to get started extending zero trust principles into ICS.⁹

How to Get Started | Zero Trust

Creative thinking can help organizations extend zero trust principles even into sensitive industrial environments.

- Depending on the current architecture of the ICS network, it may be necessary to accept that the industrial network is one large implicit trust zone. Where feasible, network segmentation can reduce this trust zone into more manageable pieces.
- Take a hard look at the industrial network and ensure that all interconnections are identified and managed. For example, did a vendor install a cellular modem for maintenance that is providing an unknown back door?
- Restrict interconnections to a limited number of assets that can initiate a remote session from the enterprise network and are mediated by a jump host that itself has robust monitoring.
- Implement logical access restrictions to enforce least privilege by limiting the users that can establish remote connections to only those necessary to meet operational requirements. For example, the organization may grant remote access privileges to engineers who perform maintenance tasks using a remote desktop client.
- Implement stronger authentication, such as multifactor authentication or a privileged access-management system, to provide additional assurance for the assets that are permitted to establish remote access sessions.
- Implement unidirectional gateways for information leaving the industrial network, such as process data being replicated to a database.
- Consider physical access controls that may provide a satisfactory, risk-informed, compensating level of control and monitoring for those who have physical access to OT devices.

⁸ <https://www.cisa.gov/zero-trust-maturity-model>

⁹ Benestelli, B., and Kambic, D., 2022: IT, OT, and ZT: Implementing Zero Trust in Industrial Control Systems. Carnegie Mellon University, Software Engineering Institute's Insights (blog), Accessed February 16, 2024, <https://insights.sei.cmu.edu/blog/it-ot-and-zt-implementing-zero-trust-in-industrial-control-systems/>.

SMALL SYSTEMS GUIDANCE

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.) guide¹⁰ 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.)

ADDITIONAL SERVICE | The Shadowserver Foundation

Utilities may wish to request free, detailed, relevant, daily remediation reports about the state of your networks or constituency. Shadowserver reports will provide a free daily potential attack surface report as well as potential malware or other malicious activity seen originating from your network/constituency.¹¹

¹⁰ https://www.cisa.gov/sites/default/files/publications/Assets_Showing_Primer_508c.pdf

¹¹ <https://www.shadowserver.org/what-we-do/network-reporting/get-reports/>

RECOMMENDED RESOURCES

Cyber Resource Hub | CISA

“Stuff Off Search” Guide | 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

Purdue Model as a Reference for Segmentation | SynSaber

Data Diodes Protect Critical Water Infrastructure | Fend

Learn About Data Diodes | OWL Cyber Defense

Top 20 Secure PLC Coding Practices | PLC Security

Cybersecurity PLC Vendor Policy Example | PLC Security

Zero Trust Maturity Model | CISA

IT, OT, and ZT: Implementing Zero Trust in Industrial Control Systems | Software Engineering Institute

5 Considerations to Implementing Zero-Trust in OT Environments | Claroty

Zero Trust Security to Protect All OT Environments | Palo Alto Networks

3

Create a Cyber Secure Culture and Protect from Insider Risks

WHY THIS IS IMPORTANT: 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.

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. Many organizations remain unprepared to manage cyber risk due to a lack of recognition, understanding, commitment, participation, or empowerment from leadership and/or boards. Leaders don't have to be cybersecurity or technology experts, but they must take responsibility for cultivating a positive cybersecurity culture.

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. The cybersecurity leader could be from or assigned by the executive team or board. Typically, this role is the Chief Information Security Officer (CISO). Furthermore, for effective support, the CISO or equivalent role, should be included on the executive team and meet with the board on a regular basis.

Cybersecurity Awareness and Readiness Training

The National Cybersecurity Alliance (NCA) promotes creating a culture of cybersecurity from the break room to the boardroom. Creating a cybersecurity culture through awareness training is a key organizational risk strategy component to manage human cyber risk by affecting positive behavior change. 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. According to the SANS ICS/OT Cybersecurity Survey: 2023's Challenges and Tomorrow's Defenses,¹ *short-format ICS-specific awareness modules with knowledge checks will strengthen the culture and reduce risk across many roles. ICS practitioners will further enhance defense, response, and recovery capabilities, and administrative and non-technical employees will gain the knowledge to better understand their crucial role and contribution to critical infrastructure protection.*

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.

¹ <https://www.sans.org/white-papers/ics-ot-cybersecurity-survey-2023s-challenges-tomorrows-defenses/>

Advanced Training for Technical Staff

In addition to role-specific training, utility OT, IT, and even legal staff should all be introduced and encouraged to delve into advanced cyber security training. Many free training opportunities are available online and in person.

If the utility is a state or local government organization, there are a variety of classes available from the Federal Virtual Training Environment (FedVTE). There are several free classes available through DHS at Idaho National Laboratory (INL) and classes hosted virtually. Hands-on red team/blue team exercises are available as part of the Industrial Control Systems Cybersecurity (301) training course. Access other training opportunities through the National Initiative for Cybersecurity Careers and

Studies (NICCS) Education and Training Catalog. WaterISAC and other organizations such as the SANS Institute, the Electricity ISAC (E-ISAC), and the Multi-State ISAC (MS-ISAC) hold regular, insightful webinars.

Participation in national and regional cyber drills is another valuable training experience. Since defense is informed by offense, to help defenders think like adversaries, attending grey- or black-hat conferences is another valuable approach. Finally, holding monthly internal cross-departmental meetings with staff involved in all aspects of cybersecurity is a valuable practice to reinforce the importance of remaining vigilant. These departmental meetings should include discussions on threats and vulnerabilities in the news, as well as organizational concerns, successes, and priorities.

SMALL SYSTEMS GUIDANCE

The AWWA Risk Management Guide for Small Systems baseline cybersecurity controls includes Training Staff to be Cybersecurity Aware which involves training staff to reduce the risk associated with a cyberattack. Training should be based on staff members' roles and responsibility within the organization. In addition, training may be informed by the current situational awareness provided by intelligence and law enforcement agencies.²

Likewise, 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 | 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.

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

² <https://www.awwa.org/Portals/0/AWWA/ETS/Resources/Technical Reports/WaterSectorCybersecurityRiskMgmt.pdf?ver=2022-03-17-102456-127>

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. Even if you don't know how to explain the incident yourself, there are usually good videos available on YouTube to help. **Just make sure to use reputable education sources so that the information is accurate and useful.**

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,³ 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 Program⁴ on the Cyber Readiness Institute's website.

**CYBER READINESS
INSTITUTE**

³ <https://cyberreadinessinstitute.org/>

⁴ <https://cyberreadinessinstitute.org/water-utilities-cyber-ready-training-interest/>

INSIDER THREATS & RISKS

All organizations face threats from trusted insiders, but utilities operating within critical infrastructure can experience dire consequences to the environment or humans should industrial control systems be compromised, even unintentionally. The more awareness employees have regarding cyber threats, the less likely they are to cause harm to critical assets or systems.

Strong protective cybersecurity controls and system architecture can quickly be defeated by an adversary with physical or privileged access. It is common to believe our greatest threat is external and remote. However, an insider, whether an employee, visitor, vendor, contractor, integrator, or other trusted consultant can cause as much or more damage than an external threat actor.

RESOURCE | National Insider Threat Awareness Month

Every September is *National Insider Threat Awareness Month (NITAM)*.⁵ Utilities may wish to consider leveraging available NITAM resources to help prevent the exploitation of authorized access from causing harm to your organization.

What Makes an Insider a Threat?

An insider threat is a people problem, not a technology problem; without people, there would be no problem. The bottom line is that every person represents a potential insider threat. However, not all insider threats are malicious.

DEFINITION

Insider Threat: The potential for an individual who has or had authorized access to an organization's critical assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.⁶

Many insider threat incidents occur due to simple negligence – the incidents were accidental, lacking malicious intent or motive to cause harm. For instance, a tired, distracted, or hurried employee can make an honest, careless mistake, or an employee who is inattentive may not perceive how their actions could precipitate a threat. According to the Ponemon Institute's *2023 Cost of Insider Risks Global Report*, the most prevalent insider security incident is caused by careless or negligent employees.⁷

Incidents caused by unintentional actions commonly involve accidental disclosure of sensitive information. For example, unintentional actions are often a result of phishing. Individuals lacking malicious intent are generally referred to as “unintentional” or “accidental” insiders.

On the other hand, individuals with motive and intent to cause damage are considered “malicious” or “intentional” insiders. Malicious insiders typically experience some sort of psychological trigger that motivates them to act with malice. The trigger could be the result of personal stressors, coercion, or a combination of both. Malicious insiders typically commit criminal acts like fraud, theft, espionage, or sabotage.

Top Five Stressors

	Incidents
1. Termination	375
2. Resignation	245
3. Internal Position Change	55
4. Organization M&A Activity	43
5. Emerging Financial Problems	33

Image credit: *Common Sense Guide to Mitigating Insider Threats, Seventh Edition*

⁵ <https://securityawareness.usalearning.gov/cdse/nitam/index.html>

⁶ <https://insights.sei.cmu.edu/library/common-sense-guide-to-mitigating-insider-threats-seventh-edition/>

⁷ <https://ponemonsullivanreport.com/2023/10/cost-of-insider-risks-global-report-2023/>

It takes specialized knowledge to compromise or “hack” into a control system undetected, but it does not take specialized knowledge to misconfigure a control system. Likewise, while some water and wastewater utilities strive to maintain an “air gap” around OT/ICS networks, air does not stop someone from walking up to obtain direct physical access. Furthermore, former employees with specialized knowledge, authorized access, and malicious intent can cause significant harm, including damage to facilities, the environment, and human lives if effective procedures are not followed to disable privileged (physical and cyber) access to the facility and control systems.

An insider threat incident can be accomplished by trusted individuals within your organization – employees, contractors, systems integrators, support vendors, former employees, etc. Trusted insiders do not always purpose to cause harm or destruction, but sometimes damage is the goal or occurs by accident. Alternatively, former disgruntled employees with ongoing access to systems and intent often will do harm if comprehensive termination/off-boarding procedures are not followed to disable access. *Off-boarding will be discussed further in Fundamental 6 – Enforce Access Controls.*⁸

Real-World Incident⁹

TOPEKA, KAN. – A Kansas man pleaded guilty to tampering with the computer system at a drinking water treatment facility in Ellsworth County. Wyatt Travnichuk, 23, of Lorraine pleaded guilty to one count of tampering with a public water system and one count of reckless damage to a protected computer system during unauthorized access.

According to court documents, the Post Rock Rural Water District hired Travnichuk in January 2018, and his duties included monitoring the plant after hours using a remote login system. Travnichuk resigned his position in January 2019. On March 27, 2019, the remote log in system was used to shut down the plant and turn off one of its filters. Investigators established Travnichuk’s cell phone was used to perpetrate the intrusion, and that the phone was in his possession at the time of the shutdown. He told investigators he was intoxicated and didn’t remember anything about the night of March 27, 2019.

Start Somewhere

The *Common Sense Guide to Mitigating Insider Threats, Seventh Edition* recommends that organizations consider implementing policies, procedures, and practices to mitigate insider threats and manage insider risk. Not every organization has the resources to develop a formal insider risk management program (IRMP). However, it is still important to consider some basic steps.

Creating a culture of cybersecurity among all levels of your organization will help deter or prevent many insider threats. However, that is not enough. Every organization needs to implement some controls beyond security awareness efforts to prevent, detect, and respond to all types of insider threats.



Practical Application

Consider establishing a committee of relevant stakeholders to begin evaluating viable methods to prevent, detect, and respond to insider threats. The committee should have representation from key departments across the organization such as human resources, legal, information technology, cybersecurity, physical security, and communications.

Deter. Culture plays a significant role in deterring insider risk. It is important to set expectations through a positive culture. These expectations should be communicated beginning with the recruitment phase, continuing through the employee lifecycle, and even beyond separation. For deterring insider threats, consider:

- Establishing, **communicating**, and enforcing policies/procedures.
- Maintaining separation of duties and least privilege account access.
- Implementing physical security and cybersecurity controls.
- Training **all** new employees (and trusted partners) in security awareness (culture), including insider risks, before granting access to buildings or systems – *and regularly thereafter*.



Additional Consideration

This should include janitorial and maintenance staff for security situations they may encounter, such as social engineering, active shooter, and sensitive documents left out in the open.

⁸ Fundamental 6 – Enforce Access Controls is scheduled to be released June 2024

⁹ <https://www.justice.gov/usao-ks/pr/kansas-man-pleads-guilty-water-facility-tampering>

- Evaluating Cyber-informed Engineering (CIE) principles¹⁰ (Fundamental 8)¹¹ to safeguard from internal accidents or intentional actions.

SIDE NOTE: “Cyber-physical” safety systems can be effective at safeguarding from events or incidents from insider threats as well as external incidents or other failure scenarios.

Detect (*observe and monitor*). Despite best efforts to deter insider threats through cultural awareness, we are all human. While it’s important to trust employees and partners, it is equally important to establish controls to detect insider threat activity. Detecting insider risk is a holistic approach that involves technical solutions and behavioral observation. To detect insider risk, it is important to:

- Involve multiple disciplines/departments within the utility (*remember, it’s a “people problem”*).
- Recognize and report **behavioral** indicators/stressors.
- Apply technical solutions such as auditing/logging/monitoring employee accounts.

Mitigate (*controls and consequences*). It is important to effectively establish controls and consistently enforce consequences for all employees. The CERT National Insider Threat Center’s “Common Sense Guide to Mitigating Insider Threats, Seventh Edition” offers quick wins and high-impact solutions to help you get started mitigating insider threats. The following figure highlights suggestions for beginning with the hiring process.¹²

- ☒ Ensure that potential workforce members undergo a thorough background check, which, at a minimum, should include a criminal background check and credit check.
- ☒ Encourage workforce members to report suspicious behavior to appropriate personnel for further investigation.
- ☒ Provide a confidential method for reporting suspicious behavior without repercussions.
- ☒ Investigate and document all suspicious or disruptive behavior.
- ☒ Enforce policies and procedures consistently for all workforce members.
- ☒ Consider offering an EAP. These programs can help workforce members deal with many personal issues confidentially.

¹⁰ <https://inl.gov/cie/>

¹¹ Fundamental 8 – Implementing Cyber-Physical Safety Systems is scheduled for release September 2024

¹² Software Engineering Institute. Common Sense Guide to Mitigating Insider Threats, Seventh Edition. Software Engineering Institute. 2022.

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)

Federal Virtual Training Environment (FedVTE) Course Catalog | CISA

ICS Virtual Learning Portal | CISA

NICCS Education and Training Catalog | NICCS

How to Talk to the C-Suite and Board About OT Security | Dragos

SANS ICS/OT Cybersecurity Survey: 2023's Challenges and Tomorrow's Defenses | SANS

Common Sense Guide to Mitigating Insider Threats, Seventh Edition | Software Engineering Institute, Carnegie Mellon University

The 13 Key Elements of an Insider Threat Program | Software Engineering Institute, Carnegie Mellon University

2023 Cost of Insider Risks Global Report | Ponemon Institute, DTEX

National Insider Threat Awareness Month | USA Learning

Reducing data exfiltration by malicious insiders | UK National Cyber Security Centre

4

Implement System Monitoring for Threat Detection and Alerting

WHY THIS IS IMPORTANT: 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.

Monitoring critical infrastructure is so crucial to the security of the U.S. that in 2021, President Biden launched the *Industrial Control Systems (ICS) Cybersecurity Initiative*.¹ The initiative began with a pilot for the electricity subsector and in 2022 it was expanded to include the water and wastewater systems sector.² The *ICS Cybersecurity Initiative* was established as a voluntary, collaborative effort between the federal government and the critical infrastructure community to facilitate the deployment of vendor neutral, interoperable technologies that provide asset visibility, **threat detection**, and actionable intelligence for ICS/OT environments. The highest priority for the *ICS Cybersecurity Initiative* is to defend U.S. critical infrastructure by **urging owners and operators to implement monitoring technologies that enhance detection, mitigation, and forensic capabilities**.

The Five ICS Cybersecurity Critical Controls | Control No. 3: ICS Network Visibility and Monitoring³

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?

As part of the *ICS Cybersecurity Initiative*, a document was drafted regarding *Considerations for ICS/OT Monitoring Technologies with an Emphasis on Detection and Information Sharing*⁴ that outline appropriate detection and response capabilities to help guide critical infrastructure owners and operators. The considerations include things such as:

¹ <https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/>
² <https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/27/fact-sheet-biden-harris-administration-expands-public-private-cybersecurity-partnership-to-water-sector/>
³ <https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/>
⁴ https://www.cisa.gov/sites/default/files/publications/ICS-Monitoring-Technology-Considerations-Final-v2_508c.pdf

- Develop ICS network traffic baselines for expected operations, compare monitored traffic to the developed baseline, and generate alerts for deviations from that baseline.
- Detect and alert on:
 - Indicators of known malicious activity.
 - Unauthorized or suspicious connections between OT networks and any external network, including enterprise IT networks or the public internet.
 - Unauthorized or suspicious connections between network segments within the OT network, including non-Internet Protocol (IP) connections.
 - Configuration changes to OT assets
 - **Other tactics, techniques, and procedures (TTPs) in the MITRE ATT&CK® Framework.**
 - The installation or operation of new or unauthorized applications on ICS/OT assets.
 - The exposure and/or usage of ports, protocols, and services that are not necessary for the operation of ICS/OT assets.

SPECIAL RESOURCE | Protecting Critical Water Systems with the Five ICS Cybersecurity Critical Controls⁵

SANS Whitepaper By Dean Parsons

ICS CYBERSECURITY CRITICAL CONTROL NO. 3: ICS Network Visibility and Monitoring

To maximize benefits across ICS security, safety, asset identification, vulnerability detection, operational reliability, and engineering troubleshooting, this control requires active involvement of trained ICS-specific cybersecurity analysts. Essential for real returns on investment and water system safety, those using the control must understand the overall water facility operations, including the common ICS protocols found in water and wastewater environments (DNP3, ModbusTCP, OPC, Profibus, EtherNet/IP and CIP, etc.).

ICS-specific network visibility tools possess advanced capabilities to analyze engineering commands and network interactions between systems, effectively detecting irregularities in water system traffic and alerting to unauthorized access and cyber attacks.



Logging, auditing and monitoring systems, and employing independent process monitoring are valuable network traffic and communications detection methods. Furthermore, by establishing a security operations center (SOC) and integrating an ICS/OT focus into the SOC, utilities are better able to leverage monitoring tools and detection methods to proactively defend ICS/OT networks.

One significant advantage with monitoring a control system is the relatively stable hardware design and network traffic patterns. This stability results in a baseline of network behavior that monitoring systems can evaluate for changes or anomalies in equipment configurations or activity.

Logging and Auditing

Detailed logs are essential for monitoring system, application, and network activity. Without sufficient logs, the ability to detect and respond to cyber incidents is exceedingly hindered. Properly configured logs enable utilities to conduct thorough root-cause analyses to find the source of issues or suspicious activity. Once enabled, logs are often collected and aggregated into a security information and event management (SIEM) system for real-time analysis and correlation. SIEMs ingest event logs from systems like firewalls, VPNs, intrusion detection systems and intrusion prevention systems, antivirus software, proxy servers, end-user devices, servers, and applications.

While utilities may enable logging on capable devices, many fail to aggregate relevant logs to a centralized log management system or SIEM for correlation and analysis. Likewise, even though logging may be enabled, many neglect to **regularly review (audit) the logs** for unusual and suspicious activity for remediation or mitigation. Continuous auditing of logs allows utilities to discover unauthorized activity before it's too late.

CPG | 2.T Log Collection

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

Operational Technology (OT): For OT assets where logs are non-standard or not available (e.g., legacy devices), network traffic and communications to and from logless assets is collected.

⁵ <https://www.sans.org/white-papers/protecting-critical-water-systems-five-ics-cybersecurity-critical-controls/>

CPG | 2.U Secure Log Storage

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

Monitoring

Many commercial ICS-specific cybersecurity monitoring tools and platforms are available. These tools can provide control system inventories, detect unauthorized connections – including mobile devices – and spot potentially malicious activity. Non-commercial and open-source software is also available to provide similar monitoring. Both commercial and non-commercial monitoring technology will ingest network traffic for monitoring by either taking a direct data feed from a “span” port on a network switch or using network taps, which make a copy of data traversing a network cable.

For Consideration

While non-commercial low-cost or open-source solutions are an option, they will likely require more in-house technical administration to configure and maintain than a commercial solution with an available support contract. Implementing a cybersecurity monitoring capability involves much more than the acquisition of the technology – this is not a “set it and forget it” endeavor. Planning for knowledgeable personnel to review the monitoring data and technical staff to maintain the technology must be considered. It also important to note that the alert information that is sent from cybersecurity monitoring technologies will require a knowledgeable analyst to interpret and analyze the information to determine the severity, applicability, potential impact, and appropriate response.

Passive, Active, or Hybrid Monitoring

ICS monitoring solutions are either passive, active, or hybrid. *Passive monitoring* is essentially eavesdropping on the network and hoping to get useful information. Passive monitoring is considered non-intrusive and does not impact OT device operations, making it less risky. However, passive monitoring does require the interpreting of ICS/OT system operations and threats by dissecting and analyzing data communications over the wire between assets in the environment. In other words, passive technology requires the capability to understand the myriad of communication protocols used in each environment and the ability to inspect those communication packets for suspicious activity. Passive monitoring limitations include not being able to provide detailed endpoint data like software/firmware versions unless that data is present in network communications in an ingestible format.

Active monitoring involves directly scanning or polling the network and devices with requests for specific information. Due to direct polling, active monitoring can provide more granular details like software, configurations, and vulnerabilities. Some solutions are also able to perform active blocking/response actions. Active monitoring carries more risk due to the potential disruption of sensitive OT devices and processes, but this method also provides more complete data than passive monitoring.

Hybrid monitoring ostensibly offers the best of both world by combining passive and active techniques. Hybrid monitoring provides some benefits of active monitoring without some of the potential risks historically experienced in ICS/OT environments by active solutions.

Fundamentally, passive monitoring is considered well-suited for initial discovery and baselining OT networks, while active monitoring provides deeper endpoint details. A hybrid strategy balancing both techniques is often recommended for comprehensive ICS/OT cybersecurity monitoring. Additionally, once a detection solution is implemented, monitoring and analysis can be performed in-house by a security operations center (SOC) or outsourced to a managed security service provider (MSSP).



Practical Application

Independent Monitoring of Critical Instrument Values

If an adversary gains access to a control system, they can hide malicious activity by registering false readings on the control system displays. Utilities can counter this by identifying the most important process readings, such as a particular tank or wet well level, the pressure at an important distribution system location, or a specific water treatment chemical concentration. These critical measurement points can be monitored independently from the control system by connecting their milliamp signals to independent data loggers with real-time reporting and alerting. If the instrument is connected to a communications protocol that could be compromised, a separate instrument should be installed and monitored by the data logger.

In the event of a normal water or wastewater system problem, both the process control system alarms and the independent data logger alarms should trigger. If only the data logger alarms trigger, that could indicate a problem with the instrument, control system, or an active cybersecurity incident. Operations staff can check the alarm comparison manually and investigate discrepancies. Another approach is to establish automated divergence alarms outside of the control system for when the two instrument values exceed a predetermined value.

Host-based vs. Network-based Monitoring

Host-based and network-based cybersecurity monitoring are two fundamental approaches to protecting information systems. Host-based monitoring involves the event information available on individual devices or servers, including the deployment of security tools directly on them. Host-based monitoring allows for the close examination of system activities, such as file modifications, process activities, and system logs on the devices themselves. Host based logging provides detailed visibility into the actions on each host, enabling the detection of threats that might bypass network defenses, such as insider threats or malware that doesn't generate network traffic.

On the other hand, network-based monitoring focuses on the analysis of data flowing across the network. It uses tools like intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor traffic for signs of malicious activity. The key benefit of network-based monitoring is its ability to provide a broader view of traffic patterns and potential threats, including those targeting multiple hosts. Both approaches are complementary: host-based monitoring excels at in-depth, localized security, while network-based monitoring offers a wider perspective on external and lateral movement threats. Together, they form a comprehensive security posture that helps organizations detect and respond to a wide array of cybersecurity threats.

Security Operations Center

Ultimately, a utility without a security operations center (SOC) lacks the ability to quickly investigate or respond to suspicious activity and potential threats. One of the primary capabilities of a SOC is to gather, correlate and analyze network, host, and application security events. Analysis is typically aided through SIEMs and other event detection technologies that provide an interface for detecting and alerting on anomalous activity, indicators of compromise, and adversary behaviors.

Building an ICS/OT-centric SOC or incorporating ICS/OT-specific functions into an existing SOC, must combine the people, processes, and technology necessary to detect and prevent an ICS/OT impacting cyber incident. According to Dragos, building specialized industrial SOC competencies and toolsets and integrating them into a broader enterprise SOC program can create a defensible architecture and accelerate readiness for OT cybersecurity risks. However, that integration is not without its challenges.⁶

⁶ <https://www.dragos.com/blog/bridge-ot-it-cybersecurity-gap/>

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 (CPG | 2.T) is **more costly** and **complex (medium)** to implement, CISA has a free resource to assist. *Logging Made Easy* (LME)⁷ 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.⁸ Members of OT-CERT have access to a two-part series that provides more understanding 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.



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.

⁷ <https://www.cisa.gov/resources-tools/services/logging-made-easy>

⁸ <https://www.dragos.com/community/ot-cert/>

⁹ <https://www.energy.gov/ceser/considerations-icsot-cybersecurity-monitoring-technologies>

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
- [Considerations for ICS/OT Cybersecurity Monitoring Technologies](#) | Department of Energy

- [Bridging the IT-OT Cybersecurity Gap: Strengthening OT Cybersecurity with Advanced SOC Capabilities](#) | Dragos
- [Detecting OT Cybersecurity Threats Using the Known-Unknown Matrix](#) | Nozomi Networks
- [MITRE ATT&CK® Framework](#) | MITRE Corporation
- [MITRE ATT&CK® Matrix for ICS](#) | MITRE Corporation

WHY THIS IS IMPORTANT: 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.

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.

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.*’ However, it has been argued¹ that you *can* protect what you don’t know you have. In this argument, industrial cybersecurity expert Dale Peterson uses the illustration of a safe deposit box.

“You may not know what is in that box or drawer, and yet its contents are protected by the physical security of the building, office, and box or drawer.”

– Dale Peterson

Despite Dale’s contention, he does submit that “*You Can Provide Better Protection If You Know What You’re Protecting.*” OT network defenders do need to know which assets are on their networks and what information those assets provide. But as Dale eludes,² the juice may not be worth the squeeze regarding the amount of information we need to know. Additionally, because such cybersecurity

guidance is written to cover multiple critical infrastructure sectors, not only water/wastewater systems, this guidance is often more applicable to other sectors with larger, more complex OT environments.

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.

It is highly recommended for cyber mature utilities to undertake a more comprehensive asset management strategy for all IT, OT, and internet connected (IoT, IIoT, etc.) assets as outlined in the CPGs, IEC 62443-2-1, NIST Cybersecurity Framework, CIS Controls, and other authoritative guidance. Such an all-encompassing asset strategy greatly enables things like more efficient incident response and recovery, forensic investigations, vulnerability management, network security monitoring, etc.

¹ <https://dale-peterson.com/2023/11/14/wrong-you-cant-protect-what-you-dont-know/>

² <https://dale-peterson.com/2023/11/21/part-2-what-does-know-mean/>



Recommended Practice

The IEC 62443 standards emphasize that having a comprehensive, actively maintained asset inventory is crucial for enabling effective risk assessments, vulnerability management, patch management, incident response, and overall cybersecurity management within ICS/OT environments. The asset inventory should provide real-time visibility into all components, configurations, and interdependencies to support robust security controls and ongoing lifecycle management as per the IEC 62443 framework.

While the following CPGs map well to this Fundamental, given the greater cost and complexity to automate with technology, smaller systems may not find them as practical. In those cases, manual asset inventory process should be acceptable, as long as they are updated periodically (see Small Systems Guidance section below).

CPG | 2.0 Document Device Configurations

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

CPG | 2.P Document Network Topology

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

CPG | 2.Q Hardware and Software Approval Process

Implement an administrative policy or automated process that requires approval before new hardware, firmware, or software/software version is installed or deployed.

- Organizations maintain a risk-informed allowlist of approved hardware, firmware, and software that includes specification of approved versions, when technically feasible.
- For OT assets specifically, these actions should also be aligned with defined change control and testing activities.

Asset Inventory Database

An accurate and comprehensive asset inventory is much more than a list of devices. Data, processes, personnel, supporting infrastructure, and dependencies to other systems should also be identified. An asset repository should include all components on the IT and OT networks and in the field, including third party and legacy equipment. The inventory record should be granular enough for appropriate tracking and reporting. Details should include but not be limited to asset owner, location, vendor, device type, model number, device name, hardware/firmware/software versions, patch levels, device configurations, active services, protocols, network addresses, asset value and criticality. Furthermore, an asset inventory is not a singular task, but an ongoing process. One approach to keeping the asset inventory current is to incorporate it into change management processes.

Unauthorized Assets

Performing an inventory will help reveal blind spots by identifying things that do not belong, such as a rogue wireless access point or other unapproved devices or connections. Inventories also illuminate processes and procedures that could enable the detection of unauthorized configuration changes or other anomalies within the environment.

Obsolete Devices

The Canadian Centre for Cyber Security offers guidance on managing obsolete equipment and the importance for owners/operators to take a proactive approach in the planning for the replacement of ICS/OT systems and components well before they become obsolete. If a replacement strategy is not feasible, then a minimum set of mitigation measures should be in place to protect these systems.

For Consideration

ICS/OT product obsolescence mitigation plan:³

- Backup and spares policies that account for non-availability of replacement products due to market conditions.
- Programs to ensure sufficient in-house resources are available and trained to rebuild systems to a known-good configuration.
- Best practices for how to secure products requiring internet/cloud/wireless connectivity.
- Approved vetting process to select vendors that provide proactive lifecycle planning, especially Mean Time Between Failures (MTBF) estimates as well as advance notice of End of Support (EOS) dates.
- Required security controls to implement before the EOS date to protect the ICS/OT networks.

Physical Inspection

An asset inventory would be incomplete without physical inspection. Network scanning methods reveal what is connected to the network at the time of the scan but may not readily account for disconnected devices that could be connected later, such as rogue or wireless devices. Additionally, a network diagram showing the relative physical locations, criticality, and roles of the assets is essential for effectively documenting the system.

SANS ICS Cybersecurity Field Manual Vol. 2⁴

Physical Inspection: This involves physically walking through industrial facilities, documenting the hardware seen in racks and network cabinets, inspecting the software and protocols used, and taking other proactive steps. Physical inspection is time consuming and expensive if it involves traveling to remote sites. Some potential physical risk exists, so PPE will be required at sites.

Vital Data

Not only is asset inventory data a foundation for cyber defense, it is also vital information for incident response (Fundamental 1) and vulnerability management (Fundamental 9).⁵ In the same way asset inventory and network diagram documentation are of paramount importance to the asset owner, they are also very attractive to an adversary. Hence, this information needs to be as rigorously protected as the ICS/OT system itself (Fundamental 7).⁶

³ <https://www.cyber.gc.ca/en/guidance/obsolete-products-itsap00095>

⁴ <https://www.sans.org/mlp/ics-resources/>

⁵ Fundamental 9 | Embrace Vulnerability Management is scheduled to be released in September 2024

⁶ Fundamental 7 | Safeguard from Unauthorized Physical Access is scheduled to be released in September 2024

SMALL SYSTEMS GUIDANCE

As previously stated, most authoritative cybersecurity guidance leads with some sort of asset management strategy. CISA's *Cross-Sector Cybersecurity Performance Goals* (CPGs)⁷ 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 (**medium**) 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 the 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.** Manual asset

inventory processes can also be augmented with periodic validation using network traffic capture analysis and other automated discovery tools as point in time validations.



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.

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

⁷ <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>

⁸ <https://www.sans.org/mlp/ics-resources/>

Additionally, for quick jump-start on the asset inventory, Dragos OT-CERT⁹ 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*.

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.

RECOMMENDED RESOURCES

Understanding OT/ICS Asset Discovery: Passive Scanning vs. Selective Probing (Ralph Langner)

Wrong: “You Can’t Protect What You Don’t Know” | Dale Peterson

Part 2 – What Does “Know” Mean? | Dale Peterson

Part 3: Creating An OT Asset Inventory | Dale Peterson

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

Censys

Shodan

Shodan’s API For The (Recon) Win! | SANS Internet Storm Center

7 Steps to Start Searching with Shodan | DarkReading

Industrial Internet of Things Safety and Security Protocol | WEF

Securing the Industrial Internet of Things: Cybersecurity for Distributed Energy Resources (Draft) | NIST (NCCOE)

Guidelines for Managing the Security of Mobile Devices in the Enterprise - SP 800-124 Rev. 2 | NIST

Mobile Device Security: Cloud and Hybrid Builds – SP 1800-4A | NIST

Baseline Security Recommendations for IoT - in the context of Critical Information Infrastructures | ENISA

Good practices for Security of Internet of Things in the context of Smart Manufacturing | ENISA

Water/Wastewater Utilities Leveraging IIoT | IIoT World

Industry IoT Consortium

⁹ <https://www.dragos.com/community/ot-cert/>

WHY THIS IS IMPORTANT: 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. Security measures such as the separation of privileged accounts and zero-trust architectures help prevent unauthorized access and limit lateral movement.

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. Audit logs identify credentials associated with accidental, unapproved, or misconfiguration changes. The fewer credentials that have access, the more focused an investigation can be. Some important components of access control include role-based controls, principle of least privilege, zero trust, strong authentication, and off-boarding.

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. In addition, limiting employee permissions through RBAC can facilitate tracking network intrusions or suspicious activities during an audit.

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.

While the least-privilege approach is a defense against many types of malware, unpatched vulnerabilities can still be exploited to elevate privileges regardless of user access rights. Therefore, it is important to maintain an effective patch management regimen (Fundamental 7) to reduce vulnerabilities that could lead to privilege escalation attacks.

Zero Trust

Zero trust is a security model that assumes no user, device, or network is inherently trusted and requires continuous verification and validation before granting access. Implementing Zero Trust principles in OT environments presents unique challenges due to the distinct nature of OT systems.

Implementing Zero Trust principles across OT networks helps with challenges, such as:¹

- Controlling remote connections into OT systems, securing network jump hosts, and preventing lateral movement across the network.
- Reviewing and reducing interconnections between dependent systems, simplifying identity processes, such as for contractors signing into the network.
- Finding single points of failure in the network, identifying issues in specific network segments, and reducing delays and bandwidth bottlenecks.

For more on Zero Trust, refer to **Fundamental 2 | Minimize Control System Exposure**

Strong Authentication

In June 2017, NIST updated its password guidance to reduce the burden on the end user in an effort to improve password hygiene. While maintaining security, the current guidance seeks to reduce complexity requirements and encourage more user-friendly password policies. NIST updated the password guidelines to generally allow for longer passwords without the special character complexity restrictions. Essentially, this increased length and reduced complexity enables users to create longer but more memorable passwords or passphrases that are more difficult to crack. NIST also advises that requiring users to change their passwords regularly makes memorizing them difficult and makes it more likely users will record their passwords in an unsafe manner.

Longer is Stronger

Malicious actors use readily available software tools to effortlessly crack simple passwords or millions of known character combinations to attempt unauthorized logins. These are called “dictionary” and “brute force” attacks. In addition, users often make common character substitutions or additions that have become predictable, and those variations have been added to the brute force/dictionary tools. To keep systems and information secure, enforce the use of longer passwords or passphrases that accommodate any ASCII printable character, and unique passwords for each account. Use password management software to keep track of and create multiple passwords.

CPC | 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.

Unique Credentials

Countless breaches and data leaks continue to prove that the same leaked information keeps turning up over and over in giant data sets of stolen credential dumps that are widely accessible. These credential dumps are then used by cyber criminals in attempts to gain access to accounts by patiently stuffing these stolen credentials into various web sites and services. When passwords are reused across multiple sites, only one set of leaked credentials will unlock the keys to the entire kingdom.

¹ <https://learn.microsoft.com/en-us/azure/defender-for-iot/organizations/concept-zero-trust>

CPG | 2.C Unique Credentials

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

The best solution (MFA notwithstanding) to creating unique credentials is consistent use of password managers. Password managers can be used to create long and strong passwords to reduce some of the most common password pitfalls – simple password creation, password reuse, password predictability, and passwords on **Post-it®** notes.

For Consideration

PASSWORD MANAGER ADVANTAGES²

Password managers not only let you manage hundreds of unique passwords for your online accounts, but some of the services also offer other advantages:

- Saves time
- Works across all your devices and operating systems
- Protects your identity
- Notify you of potential phishing websites
- Alerts you when a password has potentially become compromised

Using unique credentials for every account or system access is a fundamental cybersecurity practice. Unique credentials are crucial safeguards against widespread account compromise, credential stuffing attacks, and unauthorized access.

Multifactor Authentication

Multifactor authentication (MFA) decreases the risk that an adversary could log in with stolen credentials. Organizations should consider requiring MFA by verifying identity when each user attempts to log in. Common MFA methods include biometrics, smart cards, FIDO2 (Fast IDentity Online) enabled hardware devices, or one-time passcodes sent to or generated by previously registered devices.

CPG | 2.H Phishing-Resistant Multi-Factor Authentication (MFA)

Organizations implement MFA for access to assets using the strongest available method for that asset (see below for scope).

MFA options sorted by strength, high to low, are as follows:

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

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

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

MFA fatigue. Despite the benefits, cyber threat actors use multiple techniques to bypass MFA. A popular technique is MFA fatigue, also known as MFA prompt bombing. MFA fatigue is the process of sending a high volume of push requests in short succession to a target's mobile device until the user accepts the authentication request, either by accident or to quell the repeated push notifications.

The important bit about MFA fatigue, perhaps more important than the potential victim accepting an unauthorized push request, is that the **threat actor already has the target user's valid credentials** which are required to prompt for the push in the first place.

² <https://staysafeonline.org/online-safety-privacy-basics/password-managers/>

“Call the employee 100 times at 1 am while he is trying to sleep, and he will more than likely accept it. Once the employee accepts the initial call, you can access the MFA enrollment portal and enroll another device.”

– According to a message captured from Lapsus\$ Telegram channel

To combat MFA fatigue and other MFA bypass tactics, CISA strongly urges organizations to implement phishing-resistant MFA as part of applying Zero Trust³ principles. While any form of MFA is better than no MFA and will reduce an organization's attack surface, phishing-resistant MFA is the gold standard and organizations should make migrating to it a high priority effort.⁴

No Default Passwords

When new devices or software are installed, it is imperative to change all default passwords, particularly for administrator accounts and control system devices. Many factory default passwords are widely known and discoverable through a simple Google or Shodan search. In addition, implement other password security features, such as an account lock-out that activates after too many incorrect password attempts. Likewise, MFA should be implemented wherever possible. However, for devices that don't support MFA, such as many control systems, use the strongest (longest, highest complexity) password the device will allow.

CPG | 2.A Changing Default Passwords

An enforced organization-wide policy and/or process that requires changing default manufacturer passwords for any/all hardware, software, and firmware before putting on any internal or external network. This includes IT assets for OT, such as OT administration web pages.

- In instances where changing default passwords is not feasible (e.g., a control system with a hard-coded password), implement and document appropriate compensating security controls, and monitor logs for network traffic and login attempts on those devices.

OT: While changing default passwords on an organization's existing OT requires significantly more work, CISA still recommends having such a policy to change default credentials for all new or future devices. This is not only easier to achieve, but also reduces potential risk in the future if threat actor TTPs change.

³ <https://zerotrust.cyber.gov/federal-zero-trust-strategy/#identity>

⁴ <https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf>



Exploitation of Default Passwords on Unitronics PLCs Across the U.S. Water and Wastewater Sector by CyberAv3ngers⁵

A series of attacks which largely began in November 2023 with news that a small water authority in Western Pennsylvania was the first to be impacted by a threat group known as CyberAv3ngers.

What happened: In late November 2023, the **Municipal Water Authority of Aliquippa** in western Pennsylvania was **attacked by an Iranian-backed cyber group known as CyberAv3ngers**. The water authority reported the actors were able to gain control of a remote booster station serving two townships, but stressed there was no known risk to the drinking water or water supply. An alarm reportedly went off as soon as the attack occurred. The system had been disabled and was operated manually. The compromised device was identified as a Unitronics V570 Vision Series PLC.*

**Unitronics PLCs are commonly used in the Water and Wastewater Systems (WWS) Sector and are additionally used in other industries including, but not limited to, energy, food and beverage manufacturing, and healthcare.*

Who did it? This activity is attributed to the Iranian Government Islamic Revolutionary Guard Corps (IRGC)-affiliated Advanced Persistent Threat (APT) cyber actors using the persona “CyberAv3ngers” (also known as CyberAveng3rs, Cyber Avengers). CyberAv3ngers is a threat group purportedly focused on targeting Israeli water and energy sites – including ten water

treatment stations in Israel as of Oct. 30, 2023, according to their X page. The group targeted and compromised Israeli-made Unitronics Vision Series PLCs that were **publicly exposed to the internet. This targeting set included several U.S.-based WWS facilities. All impacted devices were compromised using the default password “1111” and default TCP port 20256.** *Note: the PLCs may be rebranded and appear as different manufacturers and company names.*

On December 1, 2023, the FBI, CISA, NSA, EPA, and INCD (Israel National Cyber Directorate) released a joint Cybersecurity Advisory (CSA), **IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities** (Alert Code AA23-335A).⁶ **The CSA confirmed multiple investigations into similar activity impacting WWS across multiple U.S. states.** According to the CSA, since at least November 22, 2023, the IRGC-affiliated cyber actors **compromised default credentials in Unitronics devices**, leaving a defacement image on the HMI stating, “You have been hacked, down with Israel. Every equipment ‘made in Israel’ is CyberAv3ngers legal target.”

On December 11, 2023, CVE-2023-6448 was assigned to address the default passwords and CISA added the CVE to its Known Exploited Vulnerabilities Catalog. On December 12, Unitronics released VisiLogic version 9.9.00 software to address this CVE with the requirement for users to change default passwords.

5 <https://www.waterisac.org/portal/tlpclear-water-utility-control-system-cyber-incident-advisory-icsscada-incident-municipal>

6 <https://www.cisa.gov/sites/default/files/2023-12/aa23-335a-irgc-affiliated-cyber-actors-exploit-plcs-in-multiple-sectors-1.pdf>

The threat actors attributed to the Unitronics PLC defacements are considered low-skilled actors using unsophisticated tactics who thus far represent a low-impact risk. However, this activity was extremely high-profile and brought enormous and much needed attention to the larger issue of unsecured internet-connected PLCs (especially ones that the default passwords have not been changed) across all critical infrastructure sectors. It is understandable that there are many cybersecurity recommendations that are challenging, impractical, or nearly impossible to implement (such as patching), especially in smaller ICS/OT environments. However, changing default passwords cannot be ignored, especially by smaller systems that likely lack additional controls.

CISA’s Secure-by-Design⁷ efforts will hopefully make the default password vulnerability an issue of the past. Until then, it’s up to asset owners and their advocates, integrators, and other support vendors to make sure default passwords (and ports) do not get deployed in production environments, or worse, directly connected to the internet. Internet exposed PLCs are exceedingly trivial to discover and default passwords are widely known by attackers, making them easy to gain access to. Utilities who outsource SCADA support are urged to **consult with integrators and other support vendors to confirm/insist that this recommended practice is being followed.**

7 <https://www.cisa.gov/resources-tools/resources/secure-by-design>

Off-Boarding Process

Utilities can be proactive in reducing the risk of insider threats from former employees by implementing effective off-boarding (and onboarding) procedures. From recruitment through separation, it's important to establish clear physical and electronic access control policies, employ tools and resources to identify anomalous behaviors, and increase training and awareness activities across the organization to reduce the risk of an insider threat when employees leave.

To protect utility assets from unauthorized access, physical and cyber access should be disabled as soon as it is no longer required. Terminated and voluntarily separated employees, vendors, contractors, and consultants should have access revoked as soon as possible. Likewise, employees transferring into new roles will likely need to have unnecessary access removed.

A rigorous off-boarding procedure should be established with human resources and contract managers, as well as IT and OT staff. The off-boarding procedure should include an audit process to identify disabled and deleted accounts and to confirm appropriate access deprovisioning due to role transfers. The procedure should also incorporate a method to identify any shared accounts, like system administrator, development environment, application, and vendor accounts.

CPG | 2.D Revoking Credentials for Departing Employees

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

Effective deprovisioning of departing employees also reduces the risk posed by a former employee becoming an insider threat. As discussed in **Fundamental 3 | Create a Cyber Secure Culture and Protect from Insider Risks**, employees with ongoing access to systems and intent often will do harm if comprehensive termination/off-boarding procedures are not followed to disable access.



Real-World Incident⁸

TOPEKA, KAN. – A Kansas man pleaded guilty to tampering with the computer system at a drinking water treatment facility in Ellsworth County. Wyatt Travnichuk, 23, of Lorraine pleaded guilty to one count of tampering with a public water system and one count of reckless damage to a protected computer system during unauthorized access.

According to court documents, the Post Rock Rural Water District hired Travnichuk in January 2018, and his duties included monitoring the plant after hours using a remote login system. Travnichuk resigned his position in January 2019. On March 27, 2019, the remote log in system was used to shut down the plant and turn off one of its filters. Investigators established Travnichuk's cell phone was used to perpetrate the intrusion, and that the phone was in his possession at the time of the shutdown. He told investigators he was intoxicated and didn't remember anything about the night of March 27, 2019.

⁸ <https://www.justice.gov/usao-ks/pr/kansas-man-pleads-guilty-water-facility-tampering>

SMALL SYSTEMS GUIDANCE

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.

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.

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 Systems⁹ denotes the time it takes to brute force a password in 2024.

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3pd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years

**TIME IT TAKES
A HACKER TO
BRUTE FORCE
YOUR
PASSWORD
IN 2024**

How did we make this?
Learn at hivesystems.com/password



Hardware: 12 x RTX 4090 | Password hash: bcrypt

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.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.

9 <https://www.hivesystems.com/password>



Practical Application

Educating employees on the importance of strong passwords and the risks of using simple or common passwords will help to motivate personnel to comply with password policies where device configurations cannot automatically enforce them. Encourage or mandate the use of free, low-cost, or professional password management tools to help employees generate

and store complex passwords securely. **Regularly update and enforce password policies, ensuring that default passwords are changed immediately.** Additionally, conduct periodic audits to ensure compliance and to identify any weaknesses in the password management system.



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.

Finally, while *CPG 2.H, Phishing-Resistant Multifactor Authentication (MFA)*, is not low cost (\$\$\$\$) or low complexity (medium) to implement, it is practical for small systems to consider for significantly reducing risk. However, due to those same challenges, phishing-resistant MFA may still not be practical for some of the smallest utilities.

As such, CISA recommends enabling “number matching” on MFA configurations to prevent MFA fatigue. Number matching is a setting that forces the user to enter numbers from the identity platform into their app to approve the authentication request.¹⁰

¹⁰ <https://www.cisa.gov/sites/default/files/publications/fact-sheet-implement-number-matching-in-mfa-applications-508c.pdf>

RECOMMENDED RESOURCES

Multi-Factor Authentication (MFA) | CISA

What is FIDO? | FIDO Alliance

Passkeys | FIDO Alliance

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

Role Based Access Control | NIST

Security and Privacy Controls for Federal Information Systems and Organizations – SP 800-53 Rev. 5 | NIST

Implementing Least-Privilege Administrative Models | Microsoft

Digital Identity Guidelines – SP 800-63-3 | NIST

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

Zero Trust Maturity Model | CISA

5 Considerations to Implementing Zero-Trust in OT Environments | Claroty

Zero Trust and your OT networks | Microsoft

Advancing Zero Trust Maturity Throughout the Visibility and Analytics Pillar | NSA

Safeguard from Unauthorized Physical Access

WHY THIS IS IMPORTANT: Physical security is equally as important as cybersecurity in protecting data, computing, networking, other data center and control systems infrastructure. Weak physical security can undermine cybersecurity efforts, as attackers may exploit physical vulnerabilities to bypass digital defenses. By preventing unauthorized physical access to critical assets, utilities can reduce the risk of theft, tampering, or destruction that could compromise safety. Therefore, it is imperative to limit physical access to IT and OT environments, including communications equipment and assets at remote locations.

There is a common adage, “If you can touch it, you own it.” In the context of cybersecurity, this adage serves as a reminder that physical access to devices or systems can lead to unauthorized control or other cyber incidents. It highlights the importance of securing physical assets to prevent malicious actors from gaining access to sensitive information or critical systems. Utilities are encouraged to implement robust physical security measures to safeguard their infrastructure, as unauthorized physical access can compromise even the most secure digital systems.

Gaining Unauthorized Physical Access

Attackers may seek to gain unauthorized physical access for surveillance or other intelligence-gathering activities to facilitate a follow-on attack (physical or cyber). Therefore, it is imperative to limit physical access to restricted areas and networked environments only to those who need it. Non-technical, physical barriers, like fences, barricades, gates, guards, and locked doors should be used to establish a security defense around the physical perimeter of buildings containing IT and ICS/OT equipment. Locked cabinets, cabinet intrusion alarms, and conduits for network cables can be used to further protect IT and ICS/OT equipment and systems from unauthorized physical access and subsequent damage.

The use of identification badges, key cards, cameras, motion detectors, security personnel, and intrusion alarms are often used to preclude unauthorized physical access. However, those methods have limited to no effectiveness against persons who use social engineering methods such

as piggybacking/tailgating along with authorized personnel or non-employees who are otherwise treated as “trusted.”

Physical infiltration could lead to attackers having direct network access, allowing them to plant remote “hacking” software or hardware tools¹ to be leveraged later in the next phase of an attack.

Social Engineering Methods Used to Gain Unauthorized Physical Access

Attackers interested in accessing your facilities have no qualms about employing social engineering tactics to trick employees into unwittingly granting



Real-World Risk | Publicly Available Information

There is a lot of information on the internet about our water and wastewater systems. It's practical to become familiar with what is accessible/searchable. In some cases, you can work to remove detailed and sensitive information - it takes time and persistence, but it is possible. However, some information is intentionally part of the public record for citizens. We need to be aware of this class of data, so we are not fooled into trusting whoever has it because we believe only privileged sources have access to it.

While it may be difficult to remove some publicly available information, utilities should perform their own reconnaissance to learn what facility and employee information is publicly available. Unnecessary public disclosures should be mitigated.

¹ <https://attack.mitre.org/versions/v15/techniques/T1200/>

unauthorized physical access. Through social engineering techniques and by combing through social media and the internet, attackers can acquire knowledge of people and processes to create credible ruses to gain physical access to a facility.

We all want to be helpful. Unfortunately, attackers know this and will sometimes take advantage of (social engineer) this part of our human nature. A very common method to gain unauthorized access through a secured entry or restricted area is to piggyback or tailgate someone with valid access. Typically, attackers will employ a ruse by *impersonating* another employee, security guard, or service worker (delivery, utility, etc.). Impersonating IT staff is a particular favorite of attackers. Attackers may also disguise themselves as pregnant (women) or wear high-visibility clothing to create the impression of a public safety officer or other trusted figure.



Real-World Risk | Unescorted Visitors

Many companies' policies state that guests must be escorted by an employee at all times – often easier said than done. From delivery couriers, integrators, contractors, security personnel, janitors, and other professionals that regularly visit our workplaces, we tend to become complacent and trusting. In some work environments it may be an acceptable risk to allow regular/expected visitors to be unescorted, but what about total strangers?

It's important to encourage staff to ask and escort anyone they don't recognize – even if the visitor has a badge – and report unattended strangers they observe in restricted or sensitive areas.

Other physical security considerations to protect from prying eyes:

- **Always lock your workstation** to keep attackers from installing malware or stealing information or credentials.
- **Keep confidential information secure.** Use privacy screens and headphones if necessary and refrain from passwords on Post-it® notes displayed near computers.
- **Implement a clean desk policy** by removing business documents, notes, etc. to avoid sensitive information from being stolen from unlocked desk drawers or filing cabinets.

Physical Security Assessments and Penetration Tests

Physical security is essential in cybersecurity to prevent unauthorized access to sensitive systems and data. By addressing physical vulnerabilities through measures like penetration tests, utilities can ensure that physical and cyber defenses work together to protect critical resources. Conducting physical penetration tests helps identify and address physical security weaknesses, ensuring comprehensive protection. Penetration testing is valuable for discovering physical security gaps that may have been overlooked or lapsed over time.

For Consideration

Utilities are encouraged to perform physical security assessments, penetration tests, or ethical “hacks” of the physical security perimeter at all facilities. Physical penetration tests can be performed alone or in concert with any network-based penetration test engagements as an attempt to breach defenses through on-site physical access. Physical penetration tests are not just to test physical security, but to identify where a physical security breach could also lead to direct IT or OT system or other restricted access.

Physical security assessments evaluate an organization's physical security measures to identify potential risks and vulnerabilities that could compromise the safety and security of its people, assets, and facilities. The assessment typically involves a combination of physical inspections, lockpicking or other lock bypass methods, piggybacking/tailgating, and access control abuse. These methods assist in assessing the effectiveness of existing security measures and identifying areas for improvement. Utilities can use the results of physical penetration tests as part of security training to increase staff situational awareness of physical, environmental, and human vulnerabilities that contribute to physical security gaps.

While social engineering methods prove effective, there are also a lot of inexpensive tools and simple tricks that don't require social engineering humans to gain unauthorized physical access.

Testing Physical Security: Tools and Tradecraft

Hardware vulnerabilities and human error are arguably the most common physical security gaps. Most break-ins are enabled by a combination of both. Physical security is fairly mature today – with

things like card readers, cameras, locks, guards, etc. However, physical security controls can still be compromised by social engineering, ineffective installation, a cheap piece of metal, or a can of compressed air.



Real-World Vulnerability | REX (Request-to-Exit) Sensors

These simple, passive, infrared thermal sensors are one of the most common devices seen in buildings all over the world. If you are walking out of a badged area, and you hear a click as you approach the door, can hit a button to exit the door, or do not have to swipe your badge to exit, your environment probably has REX sensors installed.

Vulnerability: Technicians typically install REX sensors in a way to maximize the area in which movement can be detected. While there are several things to keep in mind, such as building code and Americans with Disabilities Act (ADA) regulations, REX sensors are often found to be insecurely installed. The problem is that REX sensors are often installed too close to a door frame, which leads to the ability to activate the sensor from the wrong side of the door. We have seen some that could be activated by pushing a thin item (printer paper, envelopes, etc.) through a gap in the door. The most common method is a can of compressed air. Turn it upside down and spray some cold air toward the sensor. Your \$200 REX sensor/magnetic lock setup can be bested by an inexpensive can of compressed air.

Remediate: This one is, admittedly, a bit tricky. Turning the sensor so that it is not directly accessible from the wrong side of the door is a good way to mitigate this issue. The addition of static charge push bars or installing a pressure-sensitive mat on the secured side of the door is another way to add additional security.



Further details on this example and several more can be found at TrustedSec.²

² <https://www.trustedsec.com/blog/three-most-common-physical-security-flaws-and-how-to-fix-them/>

Environmental Considerations

Awareness of the environment around the physical security perimeter is crucial. Being aware of the environment could be the key for not needing a

key or other tool to gain unauthorized physical access. In other words, just look at what it is you are assessing for clues.



Real-World Vulnerabilities | Environmental

More information on these examples is available at *Black Hills Information Security*.³

Sebaceous Oils.

Sebaceous oils are simply oils from your fingers that could cause discoloration on a keypad. Anyone could use this to guess the correct combination.

I'm Snow

Excited! Another use case is simply looking around your environment for a way in. Here is an interesting edge case where the snowbank was high enough to clear a barbed wire fence. *This doesn't apply to just snow. It could be new construction with dirt or even pallets that are high off the ground.*



Traveler Hook. Also known as a shrum tool, this tool is capable of bypassing dead latched locks. If not set properly, an attacker could simply insert the traveler hook in the door gap and push the locking mechanism in, opening the door in a matter of seconds.

Knife Bypass. A knife bypass tool is another simple bypass that could be used on certain padlocks. It's as simple as sticking the bypass tool into the lock, thus bypassing the locking mechanism.

Wafer Key Bypass. Warded locks, often located outside of a facility to secure power generators and other valuable assets, can be picked with a wafer key.

Double Door Tool. The double door tool allows an attacker to engage push bars located on double doors from the outside.

Thumb Turn Tool. Otherwise known as a J-Tool, this tool can fit in between door gaps and twist the handle that twists the bypass mechanism, allowing an attacker to open the door from the outside simply by turning the knob.

Under Door Tool. One of the oldest bypass tools, an under door tool can be leveraged by placing it under a door, rotating the hook, and pulling the door lever down. *Further details on this example and several more can be found at TrustedSec.*³

³ <https://www.blackhillsinfosec.com/tales-from-the-pick-intro-to-physical-security-tools/>

Protection of Hardware

Gaining physical access to control rooms or other sensitive areas often implies gaining access to IT or ICS/OT equipment, but this need not be the case if utilities apply additional physical security measures.

CPG | 2.V Prohibit Connection of Unauthorized Devices

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

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

Computers used for ICS functions should never be allowed to leave the ICS area, lest they be compromised when in less secure environments. Electronic devices that *must* be taken out of secured areas, such as laptops, portable engineering workstations, and handhelds should be tightly controlled and returned to secured areas when not in use.

Malicious actors are not the only threat to IT and ICS/OT hardware; natural disasters can threaten this equipment as well. Therefore, organizations should



Practical Application

To protect critical systems and equipment from unauthorized physical access, consider the following measures:

- Affixing hard drives and portable media drives with locks when not in use.
- Removing and store hard drives and portable media drives in secured containers when not in use.
- Disabling USB ports to prevent uploading/downloading of data.
- Disabling buttons that control important functions such as power.
- Using physical protection devices that prevent unauthorized use.
- Storing keys and fobs in locked areas when not in use.

implement measures that protect hardware from events like earthquakes, hurricanes, and floods which can damage equipment directly or have indirect impacts through the loss of power.

Unattended Equipment

Computing equipment, including storage media, should never be left unattended. Regardless of current storage state, computing equipment, hard drives, portable media drives, etc., can be affixed with locks or removed and stored in secured containers when not in use.

For Consideration

Unidentified USBs. USBs, those innocuous looking little portable storage devices, while useful in utility can contain malicious content. While they are practical for transferring legitimate files and documents, they are equally functional for transferring malware into and sensitive files out of production networks – including air-gapped environments. Attackers often plant portable USBs to lure employees to install malware on corporate computers. Even advanced threat actors have used USBs to attack businesses. *In January 2022, the FBI reported on several packages containing malicious USB devices sent by the FIN7 advanced persistent threat (APT) group to U.S. businesses in the transportation, insurance, and defense industries.⁴ The packages were sent using the United States*

Postal Service (USPS) and United Parcel Service (UPS). Along with the malicious USBs, some packages were accompanied by decorative gift boxes, letters, and counterfeit gift cards.

Options for blocking or limiting USB usage:

- Disable USB ports to prevent the ability to upload or download data.
- Install USB locking port blockers that physically prevent devices from being plugged in.
- Establish and communicate clear USB security policies. USB policies should include at the very least additional scrutiny on files, documents, and other digital content.

⁴ <https://therecord.media/fbi-fin7-hackers-target-us-companies-with-badusb-devices-to-install-ransomware>

- **Decommissioned equipment.** Computing equipment and storage media such as hard drives, back-up tapes, USB drives, CD-ROMs, DVDs, may contain sensitive data. Decommissioned equipment awaiting destruction should be placed in locked containers. Likewise, all data must be properly erased before disposal. *Simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools or services may be required to securely erase data prior to equipment disposal.*
- **New equipment.** If not properly secured, even new equipment without any data could be stolen and have malware placed on them – like a USB – and returned.

Protecting Design and Configuration Documents

If a threat actor cannot gain direct access to a control system, their next best option is to procure design and configuration documents. This type of information facilitates, and perhaps even guarantees, a successful campaign by a threat actor. Ways to protect these digital and paper documents include encrypting digital copies, keeping physical paper copies in a locked office and cabinet, limiting control room tours, and preventing visitor photography.

Likewise, it is important to limit the availability of sensitive documents during open procurements. Document access can be restricted through non-disclosure agreements, background checks, two-step procurement process with limited information provided during the qualification stage, secure file sharing with encryption, and document review only under supervision while onsite at the utility.

The importance of protecting control system design and configuration documentation was underscored by the North American Electric Reliability Corporation (NERC) in 2016. NERC fined one of its electric utility members \$2.7 million for not properly protecting its critical cyber asset documentation, thereby unintentionally enabling a contractor to expose the documents on the internet.⁵



Reconnaissance Techniques Used by Threat Actors

Threat actors use various methods to gather information about critical infrastructure design and configuration:

Open Source Intelligence (OSINT). Attackers collect publicly available information about the target organization's infrastructure, including:

- Technical documentation
- Job postings revealing technology used within the environment
- Public records and regulatory filings
- Social media posts from employees

Network Scanning. Threat actors probe networks to identify:

- Active systems and open ports
- Software versions and potential vulnerabilities
- Network architecture and segmentation

Social Engineering. Malicious actors may use tactics like phishing or pretexting to:

- Extract sensitive information from employees
- Gain unauthorized access to internal systems
- Obtain credentials for accessing design documents

Targeting of Specific Documents. Threat actors often focus on acquiring:

- Network diagrams and topology maps
- System configuration files
- Software and hardware inventories
- Security policies and procedures
- Operational technology (OT) documentation

⁵ [https://www.nerc.com/pa/comp/CE/Enforcement Actions DL/Public_CIP_NOC-2569 Full NOP.pdf](https://www.nerc.com/pa/comp/CE/Enforcement%20Actions%20DL/Public_CIP_NOC-2569_Full_NOP.pdf)

RECOMMENDED RESOURCES

SANS ICS Site Visit Plan | SANS Institute

Cyber Assurance of Physical Security Systems (CAPSS) | National Protective Security Authority (UK)

Understanding the Importance of Physical Security for Industrial Control Systems (ICS) | Applied Risk

Tales From the Pick: Intro to Physical Security Tools | Black Hills Information Security

If You Don't Ruse, You Lose: A Simple Guide to Blending in While Breaking In | Black Hills Information Security

Social Engineering Basics: How to Win Friends and Infiltrate Businesses | TrustedSec

2024 USB Threat Report | Honeywell Global Analysis, Research, and Defense

Technology Equipment Disposal Policy | SANS Institute

NERC Full Notice of Penalty regarding Unidentified Registered Entity | NERC

Install Independent Cyber-Physical Safety Systems

WHY THIS IS IMPORTANT: Despite the practical applications for automation in control systems environments, it's important to consider implementing non-digital solutions to limit the consequence of high-impact events from physical damage or destruction that could result from any intentional or accidental act or failure of critical components or processes.

If you can imagine a worst case cyber threat scenario that could cause physical damage to and impact safety of ICS/OT and SCADA equipment, so will the bad guys. By engineering solutions to limit physical damage that could occur due to a cyber attack – *or even an unintentional event/incident, or failure of a device, component, or process* – asset owners can significantly reduce the impact posed by dangerous conditions that could result in high-consequence events such as excessive levels of pressure or chemical additions.

Adversaries may compromise an IT or OT control system to seek monetary gain, perform reconnaissance, modify operations, weaken customer trust, injure people, or physically destroy equipment or infrastructure. Malicious cyber actors targeting the water sector may seek long-term physical service disruption by breaking pipes or damaging process equipment that have long replacement times. Cyber attacks resulting in physical impact represent a complex or blended threat and typically pose a risk to safety. To protect critical assets from these blended threats, utilities should consider non-digital, engineered solutions such as independent cyber-physical safety systems.

Engineering Can Limit Physical Consequences of a Cyber Incident

If we can protect our critical assets from physical damage, service disruption from a cyber attack may be limited to the time it takes to transition to manual operation. Blended/complex attacks with long-lasting impacts can be mitigated by physically preventing access to process equipment and by installing independent cyber-physical safety

systems. Such purpose-built engineered cyber-physical systems could be implemented to prevent conditions such as excessive levels of pressure, chemical additions, vibrations, or temperature change from occurring due to malicious or unintentional acts against or failures of a control system.



Real-World Proof-of-Concept

In 2007, Idaho National Labs dramatically demonstrated an example of a cyber-physical vulnerability in its experimental AURORA¹ attack by remotely damaging a large diesel generator. During the demonstration, the generator's circuit breaker was rapidly opened and closed to force it out of phase with line power, which in turn created destructive electrical torque that physically damaged the unit.

Independent Protections from Worst Case Scenarios

Few utilities have cybersecurity experts readily available, but every utility already has staff and consultants who understand the intricacies of water or wastewater processes and infrastructure. Existing staff can collaborate to identify ways that physical damage or hazardous situations can be created either intentionally or accidentally through imagining worst case scenarios. For example, *assuming a threat actor has full knowledge and total control of the OT system, what could they do to cause injury or lasting system damage?*

¹ <https://www.powermag.com/what-you-need-to-know-and-dont-about-the-aurora-vulnerability/>



Practical Application

Examples of Cyber-Physical Safety Systems Solutions and Potential Precautions

In the same way that a large generator can be protected from an AURORA style attack with a properly designed protection relay, and a boiler can be protected from a low-water-explosion with an independent low-water trip switch, vital components of water systems can also be protected. The following are examples of dangerous conditions to water infrastructure and a corresponding independently engineered cyber-physical solution to protect the process from physical damage – the dangerous conditions could be caused by an attack (cyber or physical), equipment failure, or accident:

- Attempts to break pipes by valve water hammer or harmonics can be mitigated with appropriately slow mechanical gearing of valve actuators.
- Attempts to break pipes by turning on too many pumps within a pressure zone can be handled by independent pressure switches wired to pump controllers, or by increasing tank overflow capacity.
- Dangerous overdosing of treatment chemicals can be mitigated by careful pump sizing and/or, as shown in Figure 1, hardwired shutdown interlocks between the chemical analyzer and pump control circuit.
- Attempts to damage large rotating equipment through variable frequency drive manipulation can be countered with independent vibration monitoring and thermal interlocks.
- Attempts to run wastewater pumps dry for extended periods by falsely presenting high wet-well levels to the control system might be managed by creating a combined high RPM and low electrical current triggered interlock.

Figure 1 depicts a simplified example of a cyber-physical safety system designed to prevent an overdose of Sodium Hydroxide into a drinking water system. In this example, a ‘hi-hi’ pH alarm contact is taken directly from an output contact of the pH analyzer/transmitter, wired via a relay panel, to halt the NaOH metering pump. When this system is engaged, it notifies the operator via an alarm to the

primary control system as well as independently to the control room. Thus, this example covers both an independent alarming strategy as well as a cyber-physical safety shutdown. A cyber-physical safety system such as this could prevent an advanced ICS/OT cyber attack from resulting in harm to the consumer.

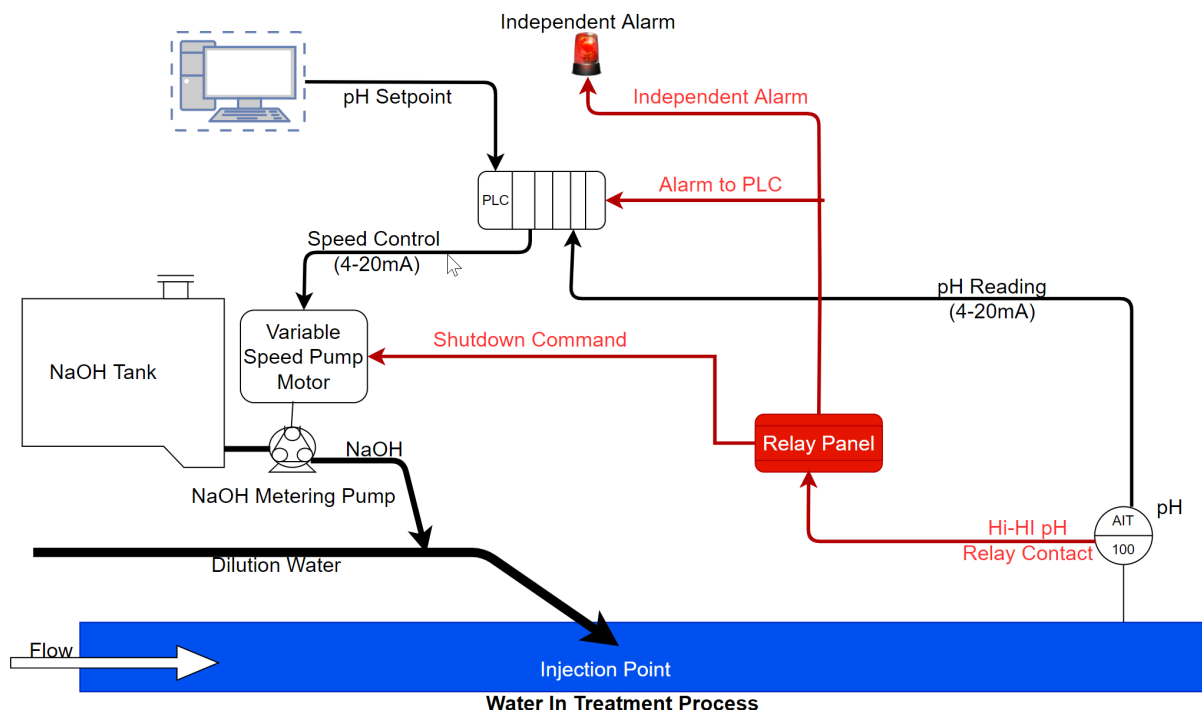


Figure 1 - Hardwired Hi-pH Shutdown and Independent Alarm Example

The independent and isolated aspects of a cyber-physical safety system are essential to its success. For example, in 2017, the TRITON/TRISIS² attack against a Saudi Arabian petrochemical plant demonstrated what could happen when a safety system is connected to a control system. In this case, the rigorous Safety Instrumented System (SIS) required for a petrochemical facility was compromised, presenting the potential for serious damage and injury if the control system had been subsequently attacked.

Likewise, while we carefully protect against adverse conditions, if the protection comes from logic built into the control system, the system can still be compromised. In other words, if the same PLC or digital controller contains both the normal process control logic and the process safety logic, then there is potential for both process manipulation and bypass of safety functions with the compromise of a single device. This potential exists even if there are two independent devices performing the function, but they are accessible with the same level of network access. Where consequences and risk require, it is critical to design and implement independent protections.

It is very important not to reduce the overall reliability of water and wastewater service

because of the design, implementation, or maintenance of a cyber-physical safety system.

Achieve simplicity and lower risk by using mechanical safety systems, such as a rupture disk. Use independent process monitoring alarms, as discussed in *Fundamental 4 | Implement System Monitoring for Threat Detection and Alerting*) and shown in Figure 2 in an initial, conservative approach. In some less time-sensitive cases, such as attempts to damage heat-sensitive electronic equipment by compromising an HVAC and building control system, use mechanical safety systems to reduce the likelihood of breach.

Figure 2 shows a simplified example of an independent alarming strategy. In this case, an analog copy of a critical system pressure is transmitted via an independent logging and telemetry system to the control center. The logger and associated logger server could generate an independent pressure reading and associated alarm. Ideally, a high-pressure alarm generated via the PLC (primary control system) would have a corresponding alarm generated via the logger and server. Any pressure value or alarms that were not within reasonable tolerances of one another would trigger further investigation and could help identify advance ICS/OT attacks that maliciously manipulate the process and primary control system.

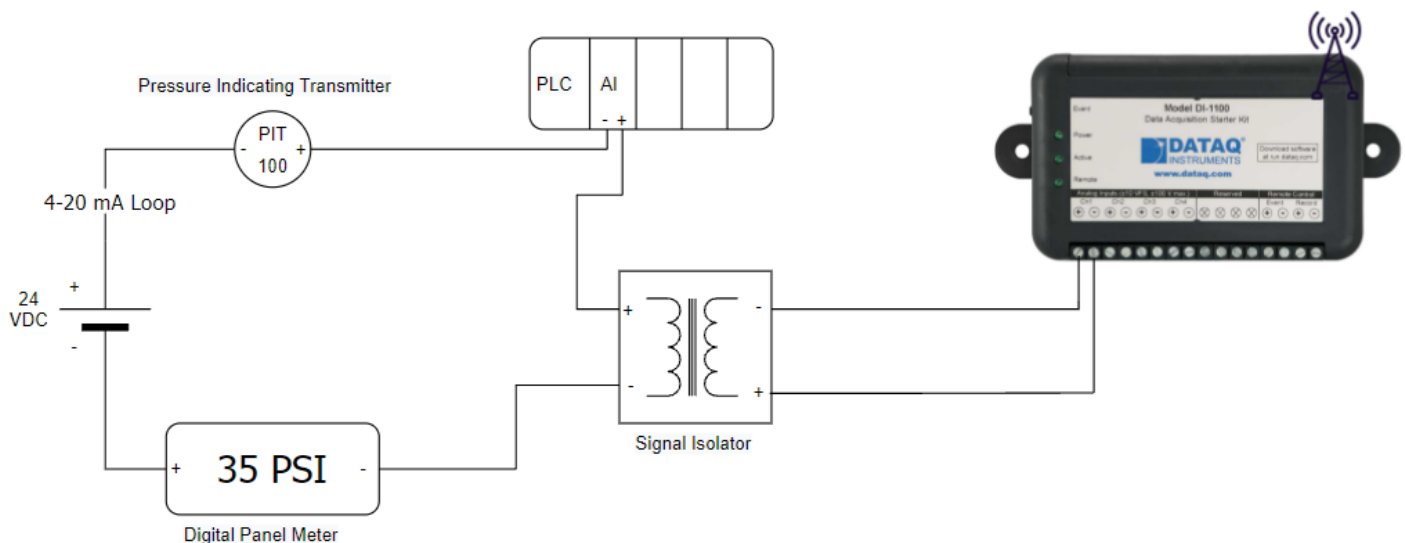


Figure 2 - Independent Pressure Alarm Example

2 <https://www.dragos.com/wp-content/uploads/TRISIS-01.pdf>

Cyber Informed Engineering

Finally, to advance the effort of engineering cyber-physical safety systems to limit physical consequences and increase safety, Idaho National Laboratory (INL) developed the Cyber Informed Engineering (CIE) framework and Consequence-

driven Cyber-informed Engineering (CCE) methodology focused on securing the nation's critical infrastructure systems. CIE and CCE have been incorporated into *NIST Special Publication 800-82r3*.⁴

Consequence-driven Cyber-informed Engineering (CCE)³

Developed at Idaho National Laboratory (INL), CCE begins with the assumption that if a critical infrastructure system is targeted by a skilled and determined adversary, the targeted

network can and will be penetrated. This “think like the adversary” approach provides critical infrastructure owners and operators a four-phase process for safeguarding their critical operations.



RECOMMENDED RESOURCES

Cyber-Informed Engineering | Idaho National Laboratory (INL)

Consequence-Driven Cyber-Informed Engineering | Idaho National Laboratory (INL)

Countering Cyber Sabotage – Introducing Consequence-driven, Cyber-informed Engineering (CCE) | Andrew A. Bochman and Sarah Freeman

Cyber Informed Engineering – SANS ICS Concepts | SANS Institute

Engineering-Grade OT Security – A Manager's Guide | Andrew Ginter

Engineering Out the Cyber-Risk to Protect What Matters Most | Idaho National Laboratory at RSA Conference 2019

What You Need to Know (and Don't) About the AURORA Vulnerability | Power Magazine

Triton/Trisis Attack was More Widespread Than Publicly Known | Dark Reading

TRISIS Malware – Analysis of Safety System Targeted Malware | Dragos

³ <https://inl.gov/national-security/cce/>

⁴ <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf>

Embrace Risk-Based Vulnerability Management

WHY THIS IS IMPORTANT: 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 actions. **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 Controls¹ | 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

CPG² | 1.E Mitigating Known Vulnerabilities

All known exploited vulnerabilities (listed in CISA's *Known Exploited Vulnerabilities Catalog*³ 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.

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,⁴ Censys,⁵ 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.

¹ <https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/>

² <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>

³ <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

⁴ <https://www.shodan.io/dashboard>

⁵ <https://censys.com/>

CPG⁶ | 1.F Third-Party Validation of Cybersecurity Control Effectiveness

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

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

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

Information on vulnerabilities is provided from various sources including vendors, cybersecurity firms, ISACs and federal agencies. To aid utilities in maintaining awareness of vulnerability disclosures, **WaterISAC regularly disseminates information on vulnerabilities and patches received from partners at CISA, other ISACs, vendors, cybersecurity firms, and others.** These curated advisories and bulletins are invaluable, but utilities need to have an internal program to further track, research, and effectively address disclosed vulnerabilities with a risk-based approach that is most appropriate and relevant to each networked environment.

REPORT | Dragos OT Cybersecurity The 2023 Year in Review⁷

According to the *OT Cybersecurity The 2023 Year in Review*, while Dragos Intelligence assessed 2,010 OT-related vulnerabilities, only 3% of vulnerabilities needed to be addressed immediately. Additionally, Dragos evaluates that the majority of vulnerabilities can be addressed through alternative means like monitoring and multi-factor authentication rather than urgent patching.

In 2023, 53% of the advisories Dragos analyzed were vulnerabilities that could cause both a loss of view and control of the process through a vulnerable OT system. A full 46% of all the vulnerabilities have no ability to impact the control or visibility of the industrial process. Of these vulnerabilities, 1% could only cause loss of view without impacting loss of control.

Remediate, Mitigate, or Accept Vulnerabilities

Once vulnerabilities are identified and prioritized using a risk-based approach, they should either be remediated, mitigated, or the associated risks must be accepted and documented. Ignoring a vulnerability that exists in your environment is not an option. Device vulnerabilities are frequently remediated through patches and software or firmware updates. However, even after patches and updates have been released by a vendor, many systems remain vulnerable because asset owners are either unaware of the patch or choose to not implement fixes due to lack of understanding or insufficient resources.

⁶ <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>

⁷ <https://www.dragos.com/ot-cybersecurity-year-in-review/>

Furthermore, some products have design “features” that are inherently insecure-by-design and will never have a patch. In instances where patches are not or cannot be applied, vulnerabilities should be mitigated through compensating security control methods such as “hardening” to remove unnecessary services and applications, replacing devices when they are no longer supported by the vendor, enforcing policies and procedures (Fundamental 10 | Develop and Enforce Cybersecurity Policies and Procedures)⁸, and providing cybersecurity awareness and technical training (Fundamental 3 | Create a Cyber Secure Culture and Protect from Insider Risks). Impacts can be further reduced by installing independent cyber-physical safety systems (Fundamental 8 | Install Independent Cyber-Physical Safety Systems), interrupting threat actors early in the attack cycle through successful threat detection (Fundamental 4 | Implement System Monitoring for Threat Detection and Alerting), and applying lessons learned post-incident response (Fundamental 1 | Plan for Incidents, Emergencies, and Disasters).

RESOURCE | ICS-Patch⁹

The ICS-Patch decision tree will lead to one of three results for each cyber asset/security patch pair.

Defer Do not apply or schedule to apply the security patch on the cyber asset for risk reduction. (The asset owner may choose to apply the security patch as part of cyber maintenance to keep the system under support.)

Scheduled The security patch should be applied on the cyber asset during the next scheduled patch window. For some ICS, this may be a scheduled outage that occurs annually or semiannually. For others they may choose a quarterly or monthly patching interval.

ASAP Apply the security patch on the cyber asset as soon as possible in a safe manner.

SMALL SYSTEMS GUIDANCE

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*. While **CPG 4.C Deploy Security.txt Files** meets that criteria, **CPG 1.E Mitigating Known Vulnerabilities** is an exception that is strongly recommended. Despite its medium complexity to implement, mitigating known vulnerabilities, especially on critical assets has a high impact on risk reduction that cannot be overstated. Mitigating vulnerabilities significantly reduces the attack surface available for exploitation.

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.

⁸ Fundamental 10 | Develop and Enforce Cybersecurity Policies and Procedures will be released in December 2024

⁹ https://dale-peterson.com/wp-content/uploads/2020/10/ICS-Patch-0_1.pdf

¹⁰ <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

¹¹ <https://securitytxt.org/>

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. Organizations should use the KEV catalog as an input to their vulnerability management prioritization framework. CISA and WaterISAC strongly **recommend all stakeholders include a requirement to immediately address KEV catalog vulnerabilities as part of their vulnerability management plan.** Doing so will build collective resilience across the cybersecurity community. 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	ICS Advisory Project Dan Ricci
Known Exploited Vulnerabilities Catalog CISA	Cybersecurity Incident & Vulnerability Response Playbooks CISA
ICS-Patch - What To Patch When In ICS? A Decision Tree Approach Dale Peterson	National Vulnerability Database (NVD) NIST
The OT Vulnerability Management Handbook Langner, Inc.	Common Vulnerabilities and Exposures (CVE) MITRE

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

Develop and Enforce Cybersecurity Policies and Procedures (Governance)

WHY THIS IS IMPORTANT: Documented cybersecurity policies and procedures are necessary for organizations to protect assets and mitigate risks. Policies provide a framework for identifying potential vulnerabilities, outlining security measures, and managing threats. Procedures should be detailed, step-by-step instructions that describe how to carry out policies by addressing the “who,” “when,” and “how” of policy implementation.

Developing policies and procedures can be one of the most straightforward and yet challenging fundamentals to implement. Regardless of difficulty, it is essential to develop and enforce clear and actionable cybersecurity policies and procedures for all OT and IT systems. Policies and procedures should plainly define an organization's cybersecurity expectations and instructions on compliance for each subject area.

Once formalized, policies and procedures can only be effectively operationalized across an organization through dissemination, communication, education, and enforcement. Distributing and communicating cybersecurity policies throughout the entire organization is vital. All staff must be made aware of their responsibility to uphold policy and follow procedures, as well as the consequences of any violation.

Policies and procedures fall under the overarching framework of governance. Policies support governance objectives as high-level principles that describe the “what” and “why” of organizational actions and guide behavior. Governance is important. So much so that it was incorporated into the NIST Cybersecurity Framework (CSF) 2.0 released in February 2024. According to NIST, the CSF's governance component emphasizes that cybersecurity is a major source of enterprise risk that senior leaders should consider alongside others such as finance and reputation.¹

Rinse, Repeat, and Audit

Governance is a continuous endeavor. Organizational environments and cybersecurity requirements are dynamic. Like all



recommendations in these fundamentals, policies and procedures are not one-and-done. These documents need to be reviewed regularly, updated when necessary, and subsequently communicated as changes are made. Furthermore, policies and procedures must be regularly audited for accuracy, understanding, efficiency, and compliance among staff.

Policy Examples

The whole of this document, WaterISAC's *12 Cybersecurity Fundamentals for Water and Wastewater Utilities* include practical subject areas (the fundamentals) to inform the development of cybersecurity policies and procedures for your utility. Specific policy examples could include (but are not limited to) data breach response, acceptable use of equipment and computing

¹ <https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework>

systems (including email), remote access, artificial intelligence, and disaster recovery.

The SANS Institute provides a free set of templates covering important security requirements that can be customized to jump-start your policy development and implementation. At the time of this writing, SANS² has 64 policy templates across subject areas of email security, password creation and protection, artificial intelligence, server security, network security, incident handling, and more.

RECOMMENDED RESOURCES

How Do Cybersecurity Policies and Procedures Protect Against Cyberattacks? | Trellix

Security Policy Templates | SANS Institute

OT/ICS policy templates that will save you time, labor, and project risk | Langner

Simple Cyber Governance Program (SCGP) | Langner *(licensing is required for full access, but asset owners are able to request an evaluation copy)*

Kansas Unveils Cyber Program to Safeguard Water Systems | government technology

State Cybersecurity Governance Case Studies CROSS SITE REPORT (December 2017) | CISA

² <https://www.sans.org/information-security-policy/>

Secure the Supply Chain (service providers, integrators, and other “trusted” third parties)

WHY THIS IS IMPORTANT: 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.

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. The MITRE ATT&CK® Framework describes the technique of abusing trusted relationships¹ as *adversaries that may breach or otherwise leverage organizations who have access to intended victims. Access through trusted third-party relationship abuses an existing connection that may not be protected or receives less scrutiny than standard mechanisms of gaining access to a network.* 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.



Notable Third-Party Cyber Attacks

Target. The Target breach in 2013 is still one of the most highly referenced examples of how the compromise of a small vendor was used to infiltrate a major corporation and remains a significant cybersecurity case study highlighting the importance of robust third-party risk management. This breach was carried out due to a successful spear phishing attack against a small, less cyber-prepared vendor. Threat actors used the network credentials of a heating and ventilation company to infiltrate Target’s network.

SolarWinds. Arguably the most impactful cyber incident in 2020, where over 18,000 SolarWinds customers installed a compromised SolarWinds Orion network management platform update, potentially exposing their systems to the attackers. Victims included U.S. government departments, as well as private companies like Microsoft, Intel, and Cisco. The SolarWinds attack raised concerns about supply chain vulnerabilities, potential risks associated with widely-used software platforms, and the need for improved security measures.

Log4Shell. In 2021, a critical vulnerability (CVE-2021-44228) was discovered in the widely used

¹ <https://attack.mitre.org/versions/v16/techniques/T1199/>

open-source Java logging library, Apache Log4j 2. Log4j is widely used by enterprise applications, cloud services, Internet-of-Things, and SCADA systems across many industries including the water and wastewater sector – *Log4j is often an embedded component of Java-based ICS hardware and software*. Given common use of log4j, experts believe the full scope and impact may not be realized for years.

Unitronics Vision Series PLC with HMI. In late November 2023, a pro-Iranian hacktivist group known as CyberAv3ngers were observed targeting and compromising unsecured Israeli made Unitronics Vision Series programmable logic controllers (PLCs) across multiple water and wastewater utilities across the U.S. The actors gained access to the components using the well-known default credentials (“1111”) of the Unitronics devices. See *Fundamental 6 | Enforce Access Controls* for more on *Exploitation of Default Passwords on Unitronics PLCs Across the U.S. Water and Wastewater Sector* by CyberAv3ngers.

MOVEit. Also in 2023, the MOVEit Managed File Transfer application that provides secure file transfer services used by thousands of organizations and government agencies, was impacted by the CL0P ransomware group. The group was able to exploit a security flaw and deploy ransomware, leaking confidential data of approximately 77 million individuals and over 2,600 companies globally, with U.S. companies being the most impacted (*reportedly 78% of breached companies*) including U.S. Department of Energy, Johns Hopkins, the University System of Georgia, and in Louisiana (LA), the Office of Motor Vehicles.

“As a nation, we have allowed a system where the cybersecurity burden is placed disproportionately on the shoulders of consumers and small organizations and away from the producers of the technology and those developing the products that increasingly run our digital lives. Americans need a new model to address the gaps in cybersecurity—a model where consumers can trust the safety and integrity of the technology that they use every day.”²

– CISA

That statement from CISA speaks to the *Secure by Design*³ effort currently underway to significantly reduce the risk from third parties. As CISA suggests, the balance of cybersecurity risk should be shifted. While, asset owners cannot ultimately be absolved from cybersecurity risk, it's not fair to put the total cost on customers for securing products they use or for manufacturers to charge more to deliver a secure product. Until the technology ecosystem takes more responsibility for manufacturing and delivering secure products and services out of the box, all organizations still have a responsibility to manage third party risk. However, in the meantime, we all have a role to play in hopes of hastening the shift in burden – asset owners can make strides by demanding secure by design and secure by default products and services.

Demand Secure by Design and Secure by Default

Each utility is responsible for its own cybersecurity, but we aren't all experts. It's impractical for asset owners and operators to understand everything there is to know about the devices and software used to build our infrastructure – *all the features, functions, secure configurations, vulnerabilities, etc.* – especially for smaller or less resourced utilities. Therefore, we all must work with manufacturers, suppliers, and integrators to demand *secure by design* products and *secure by default* configurations for the systems we use.

A Better Way to Mitigate Third Party Risks

The graphic, *Real-World Incidents | Notable Third-Party Cyber Attacks* highlights the significant challenges in managing third-party risks. While current cybersecurity measures have improved the ability to detect and mitigate cyber attacks that leverage trusted relationships, they are not foolproof. Organizations must continually adapt strategies, combining technological solutions with human vigilance and robust security policies to effectively combat this evolving threat landscape. *But what if there was another way?*

² <https://www.cisa.gov/securebydesign>

³ Ibid.

You can help prevent insecure products

Water and wastewater utilities are encouraged to proliferate the *Secure by Design* effort. When shopping for products and services, consider the 256 (at the time of this writing) organizations that have taken the *Secure by Design Pledge*.⁴ If working with one of the pledge signers is not possible, do your part to drive a secure technology ecosystem through *Secure by Demand*.⁵ The *Secure by Design* guidance includes information that can **help customer organizations demand security when in procurement discussions, including questions⁶ that customers should ask** hardware and software manufacturers, integrators, service providers, resellers, etc. to understand the extent to which the products and services have been designed with security in mind.

Until We Achieve Secure by Design and Default

Until products are secure by design, robust third-party risk management is still necessary to identify, assess, and control risks that arise from interactions with external parties.

NIST Cybersecurity Framework (CSF) 2.0 | Cybersecurity Supply Chain Risk Management (C-SCRM)

In recognizing the compound and complex nature of cybersecurity risk from third parties, as part of the new Govern (GV) function, the NIST CSF 2.0 has placed added emphasis on supply chain risk management (SCRM). Cybersecurity SCRM (C-SCRM) is a systematic process for managing exposure to cybersecurity risk throughout supply chains and developing appropriate response strategies, policies, processes, and procedures.⁷ Utilities are encouraged to use the CSF 2.0 to foster cybersecurity risk oversight and communications with stakeholders across supply chains.

RESOURCE | NIST CSF 2.0 | Cybersecurity Supply Chain Risk Management (GV.SC):

Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders⁸

- **GV.SC-01:** A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders
- **GV.SC-02:** Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally
- **GV.SC-03:** Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes
- **GV.SC-04:** Suppliers are known and prioritized by criticality
- **GV.SC-05:** Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties
- **GV.SC-06:** Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships
- **GV.SC-07:** The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship
- **GV.SC-08:** Relevant suppliers and other third parties are included in incident planning, response, and recovery activities
- **GV.SC-09:** Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle
- **GV.SC-10:** Cybersecurity supply chain risk management plans include provisions for activities that occur after a the conclusion of a partnership or service agreement

⁴ <https://www.cisa.gov/securebydesign/pledge>

⁵ <https://www.cisa.gov/resources-tools/resources/secure-demand-guide>

⁶ https://www.cisa.gov/sites/default/files/2024-08/SecureByDemandGuide_080624_508c.pdf

⁷ <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>

It's important for utilities to effectively manage third party risk by conducting comprehensive risk assessments of third-party vendors and implementing strong contractual obligations that include specific security requirements. Relevant CISA *Cross-Sector Cybersecurity Performance Goals (CPGs)*⁸ to manage third-part risk include:

CPG | 1.G Supply Chain Incident Reporting⁹

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

CPG | 1.H Supply Chain Vulnerability Disclosure¹⁰

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

CPG | 1.I Vendor/Supplier Cybersecurity Requirements¹¹

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

Beyond the Inherent Risk Posed from Third Parties

Beyond the inherent risk posed to organizations via third parties from the use of hardware, software, etc., threat actors also usurp trusted relationships that exist due to human interactions. Attackers use social engineering methods such as various phishing techniques to exploit human vulnerabilities to gain unauthorized access to systems, finances, and sensitive information. According to member reports captured in the *WaterISAC Quarterly Water Sector Incident Summaries* – TLP:AMBER reports offering a look at incidents impacting water and wastewater utilities during a specific quarter – most member reported

incidents consistently highlight phishing attacks, particularly those involving impersonation of a trusted entity, such as business email compromise (BEC) and vendor email compromise (VEC). These phishing attacks often include a range of deceptive themes like invoice fraud.



Notable WaterISAC Member Reports of Third-Party Incidents

Incidents at trusted third-party vendors had impacts on multiple members.

There was a report of **QR code phishing** involving impersonation of a trusted vendor and several other reports of **vendor impersonation** attempts and **indirect impacts** on a utility from ransomware incidents at a vendor. One of the more notable incidents involved the compromise of a **third-party paper check processing vendor** which led to some of the utility's customers having images of their checks posted on the dark web.

Insufficient employee awareness about third-party risk management can increase the risk to these types of attacks. As such, employee awareness (*Fundamental 3 | Create a Cyber Secure Culture and Protect from Insider Risks*) cannot be overstated in helping curb threats from third parties. Additionally, it is crucial to establish policies and procedures (*Fundamental 10 | Develop and Enforce Cybersecurity Policies and Procedures*) to verify communications from vendors. Internal staff must be empowered by leadership to be extra vigilant and not blindly trust requests that appear to come from a trusted partner. Staff that manage vendor relationships, especially financial aspects, should be immersed in advanced training regarding these threat actor tactics.

8 <https://www.cisa.gov/cybersecurity-performance-goals>

9 <https://www.cisa.gov/cybersecurity-performance-goals-cpgs#SupplyChainIncidentReporting1G>

10 <https://www.cisa.gov/cybersecurity-performance-goals-cpgs#SupplyChainVulnerabilityDisclosure1H>

11 <https://www.cisa.gov/cybersecurity-performance-goals-cpgs#VendorSupplierCybersecurityRequirements1I>

Small Systems Guidance

Managing third-party relationships 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.

RESOURCE | Secure by Demand Guide: How Software Customers Can Drive a Secure Technology Ecosystem¹²

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.

- 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?

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.

¹² https://www.cisa.gov/sites/default/files/2024-08/SecureByDemandGuide_080624_508c.pdf

RECOMMENDED RESOURCES

Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (SP 800-161 Rev. 1) | NIST

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

Hardware Bill of Materials (HBOM) Framework for Supply Chain Risk Management | CISA

Securing OT against Log4j; Is it really a thing? | CISA

Participate in Information Sharing and Collaboration Communities

WHY THIS IS IMPORTANT: No single organization can sustainably identify and address all cyber threats alone. Trusted and secure information sharing is fundamental for enhancing cybersecurity and building resilience given the rapidly changing digital landscape and the increasing sophistication of cyber threats. Information sharing allows organizations to leverage collective knowledge and experience to gain a more comprehensive understanding of potential threats and risks. By exchanging threat information and intelligence, utilities gain faster awareness of developing threats to improve proactive (rather than reactive) threat detection and response.

Participating in information sharing and collaboration communities is individually and collectively very effective. The more utilities collaborate and share with regional peers and the community at-large, the more the sector benefits. Water and wastewater utilities and other critical infrastructure sectors all face the same cyber threats. Involvement with organizations that focus on cybersecurity and resilience enables the community to learn and share knowledge and experience to help one another become more resilient.

History of Information Sharing

The importance of cyber information sharing was deemed so important that multiple federal efforts have been established to provide a framework.

Presidential Decision Directive 63 (PDD-63).¹

In May 1998, Presidential Decision Directive 63 (PDD-63) established a comprehensive framework for cyber information sharing and critical infrastructure protection in the United States. Specifically, **PDD-63 encouraged the creation of sector-specific Information Sharing and Analysis Centers (ISACs)** to facilitate information sharing between the government and private sector. Additionally, recognizing the increasing interdependence of critical infrastructures and the growing threat of cyber attacks, PDD-63 emphasized the importance of public-private partnerships and sought voluntary participation from private industry to meet common goals for protecting critical systems.

For Consideration

Key benefits of cyber information sharing:

- **Faster awareness of developing threats.** Utilities can learn about new threats as they emerge, providing more time to upgrade defenses.
- **Improved threat detection and response.** Sharing enables utilities to identify potential indicators of compromise (IoCs) and threat actor behaviors for better understanding of threats.
- **Cost reduction.** Collaborative efforts spread out the cost of cyber intelligence and security measures across multiple entities. This benefit can be especially useful for small less resourced utilities to provide awareness.
- **Enhanced collaboration.** Information sharing fosters reciprocal relationships and trust among participating organizations.
- **Proactive security measures.** Early warnings allow for more strategic use of IT, OT, and security staff, enabling a proactive rather than reactive approach.
- **Strengthened overall security.** By sharing knowledge, utilities contribute to improving security measures across industries and the internet.

¹ <https://www.ojp.gov/ncjrs/virtual-library/abstracts/white-paper-clinton-administrations-policy-critical-infrastructure>

While PDD-63 initially introduced the concept of ISACs, Executive Order (EO) 13636² in 2013 further emphasized and expanded the role of information sharing in cybersecurity. **EO 13636 sought to focus on increasing the volume, timeliness, and quality of cyber threat information sharing and improve information sharing between government agencies and between government and the private sector.**

Executive Order 13691³ | Formation of Information Sharing and Analysis Organizations (ISAOs). In 2015, Executive Order 13691 focused on enhancing cybersecurity information sharing within the private sector and between the private sector and government by promoting and encouraging the development of Information Sharing and Analysis Organizations (ISAOs). ISAOs were designed to serve any community, sector, or subsector, *not limited to critical infrastructure*, making them more inclusive than existing ISACs.

NIST Guide to Cyber Threat Information Sharing (SP 800-150).⁴ Once again emphasizing the importance of information sharing, in 2016 NIST published *Guide to Cyber Threat Information Sharing* (SP 800-150). According to NIST, the *Guide to Cyber Threat Information Sharing* provides guidelines for establishing and participating in cyber threat information sharing relationships.

Stronger Together

WaterISAC offers a prime opportunity for utilities and other stakeholders to collaborate, share ideas, successes, incident details, and lessons learned. Other respected information sharing organizations with different strengths include the Multi-State ISAC; the Electricity ISAC; U.S. EPA's Office of Water; national, regional, and state water and wastewater associations; InfraGard; urban and regional law enforcement agencies, and intelligence fusion centers.

Share experiences. Another way to share with your peers is to develop case studies and presentations about challenges your utility has overcome. WaterISAC always welcomes content in the form of articles and webinar presentations. If you have a story to tell, or you just have a possible topic of interest to suggest, please get in touch with WaterISAC.

H2OEx. Roundtable discussions are ideal venues for peer-to-peer sharing and collaboration. In December 2024, WaterISAC hosted its first *in person discussion-based regional exercise* to a sold-out crowd in Washington D.C. (Region 3⁵). With over 70 attendees representing 21 utilities, federal partners from the EPA, FBI, and the White House Office of Cybersecurity, along with industry sponsors and sector supporters. After the success of this pilot event, plans are under way to bring similar events to additional regions⁶ in 2025 and beyond. Keep an eye out for more at <https://www.waterisac.org/>, or reach out to WaterISAC at 1-866-H2O-ISAC (1-866-426-4722), or our contact form to find out more.

Conferences. Participating in association conferences is another valuable sharing/collaboration method. For example, AWWA's annual Water Infrastructure Conference (WIC) and NRWA's WaterPro offer numerous security and resilience presentations and opportunities to network with peers. Consider attending, or even presenting at WIC, WaterPro, or at events hosted by other associations.

Share Cybersecurity Incidents and Suspicious Activity with WaterISAC

Reporting suspected or confirmed incidents is extremely valuable to the sector and, in many cases, national security. Reporting incidents helps WaterISAC and government security agencies learn which threats utilities are facing. This, in turn, influences the development of knowledge, intelligence, and resources to prevent future compromises and to assist with recovery and response. Reporting OT and IT compromises also allow analysts to glean threat indicators and observed behaviors from an incident or suspicious activity. These observables can be shared to help network defenders identify and block future attacks. Potential observables include malware signatures, malicious IP addresses, suspicious URLs and files – any artifacts that can signify potentially nefarious activity.

2 <https://www.govinfo.gov/content/pkg/FR-2013-02-19/pdf/2013-03915.pdf>

3 <https://obamawhitehouse.archives.gov/the-press-office/2015/02/12/fact-sheet-executive-order-promoting-private-sector-cybersecurity-inform>

4 <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-150.pdf>

5 <https://www.cisa.gov/about/regions/region-3>

6 <https://www.cisa.gov/about/regions>

Report Incidents and Suspicious Activity to WaterISAC and Authorities

“It takes a community to protect a community.” That is the underlying theme of the Department of Homeland Security’s **“If You See Something, Say Something®”** program. It is also the foundation of information sharing and it is what motivates WaterISAC’s mission to help protect the security and resilience of our members and the water and wastewater sector at large.

WaterISAC urges utilities and others sector stakeholders to report incidents and suspicious activity to our analysts. Reporting incidents and suspicious activity helps strengthen sector resilience, because it allows WaterISAC to identify threats and vulnerabilities and to warn other members and partners. The information you share also helps WaterISAC shape products and services, including advisories, webinars, and reports that can help utilities stay safe, secure, and resilient.

Reports are Kept Confidential

WaterISAC maintains confidentiality of the information provided by submitters. If WaterISAC wishes to share your incident in an analysis or other product, we would first secure your express permission to do so, then would anonymize the information you have shared. As a private non-profit, WaterISAC is not subject to public records law, further preserving the security of your report.

In some cases, it may necessary or preferable to also report your incident or suspected incident to federal authorities, especially if you intend to seek help with an investigation or recovery. Crimes should always be reported to the appropriate authorities.

How do I make a report?

You can file reports of incidents and suspicious activity to WaterISAC in three ways:

1. Submit a confidential report at www.waterisac.org/report-incident.
2. Email analyst@waterisac.org.
3. Call our analyst desk at 866-H2O-ISAC.

What do I report?

WaterISAC seeks reports of both cyber and physical incidents, as well as suspicious activity.

Cybersecurity Incidents. Cybersecurity incidents are cyber attacks or compromises of your

DIRECTOR'S NOTE

Everyone wants to know; few are willing to share

Rarely a day goes by without seeing a headline about a disclosed/discovered cyber incident or disclosed product vulnerability. Often the impacted organizations are global brands (think Cisco, OKTA, MGM, major banks, federal/state governments, etc.) that perhaps have a duty to the world to be as transparent as possible about their experience. In the spirit of information sharing, this transparency helps all organizations know what to look for to protect their systems and infrastructure from similar attacks. These disclosures also highlight that cyber attacks can happen to anyone – regardless of organizational size, type, or cyber maturity.

But does that mean everyone has to be public about cyber attacks – absolutely not! There are other ways to share information about your cyber incident or observed suspicious activity without being so public.

Non-attributable community reporting. Non-attributable reporting is why the ISACs/ISOs exist. **ISACs/ISOs thrive on being able to help their sectors/communities understand the threats facing them. We do that best when we receive member reports that we anonymize and report out for the benefit of all members.**

Often, less global organizations/entities are reticent to report cyber incidents for a variety of reasons. Unfortunately, too often, news of the incident ends up leaking from elsewhere – and that’s unfortunate to first hear something about a sector organization’s cyber incident from the mass-media news.

I encourage all water and wastewater utilities to stop keeping your cyber incidents so close to the vest *until a reporter calls*. Once you get things under control, consider making WaterISAC your next call. We’re happy to assist as able, but we also value the opportunity share what you experienced for the benefit of other utilities and sector stakeholders. As shared in the **Report Incidents and Suspicious Activity to WaterISAC and Authorities** section, your reports are kept confidential and only shared in an anonymous fashion to help others protect their systems from similar activity.

— Jennifer Lyn Walker
Director of Infrastructure
Cyber Defense | WaterISAC

enterprise IT system or your industrial control system (ICS/OT). These events/incidents could be:

- Successful ransomware attacks or close calls.
- Successful install of malware that had or may have had an impact on the utility's ability to conduct business and/or operations.
- Phishing campaigns, including successful or attempted spear phishing of executives, executive assistants, SCADA engineers, IT administrators, financial staff, or other privileged users.
- Successful or attempted business email compromise or vendor email compromise incidents, including account takeover or impersonation of executives.
- Data thefts.
- Social engineering attempts to gather sensitive information from personnel.

Physical Security Incidents. Reportable physical security incidents include those that are intended to cause any of the following:

- Bodily harm to employees or customers.
- Public health impacts.
- Significant harm to the environment.
- Impacts to the operations of your utility.
- Financial losses to your organization of \$10,000 or more (per instance.)

Specific examples of physical incidents could include:

- Intentional water supply or wastewater contamination.
- Sabotage/tampering.
- Theft.
- Assault.
- Surveillance or suspicious questioning.
- Threats.

What happens next?

Once you advise us of the incident or suspicious activity, we will follow up with you for more information. We will intentionally ask for your permission to use the information in WaterISAC reports.

*If the answer is yes, **we will anonymize the information you shared by removing any details that would attribute the incident to you or your utility.** The information you share is stored in a protected database.*

The anonymized information will be used to inform various WaterISAC reporting – typically at a **TLP:AMBER**⁷ sharing level, including (but limited to) any relevant notices/advisories, *Quarterly Water Sector Incident Summary*, or *Threat Analysis for the Water and Wastewater Sector*.

Federal and Other Reporting and Assistance Mechanisms

United States

CISA Services Portal. CISA provides a secure means for constituents and partners to report incidents, phishing attempts, malware, and vulnerabilities. You can create an account and track the progress of your issue or submit your issue anonymously for CISA's review. Other CISA contact information includes CISA Central at 1-844-Say-CISA and SayCISA@cisa.dhs.gov.

RESOURCE | CISA Security Advisors

Water and wastewater utilities are encouraged to maintain relationships with CISA's Security Advisors, including regional Protective Security Advisors (PSAs), Cyber Security Advisors (CSAs), Emergency Communications Coordinators (ECCs), and Chemical Security Inspectors (CSIs). *You may also contact WaterISAC for an introduction to CISA's Security Advisors.*

Additionally, should you require assistance, CISA offers **no-cost** Cyber Incident Response and Cyber Threat Hunting services for critical infrastructure organizations and Government entities at the Federal, State, Local, Tribal, and Territorial (FSLTT) levels.

⁷ <https://www.first.org/ttp/>

⁸ <https://www.cisa.gov/resources-tools/services/cyber-incident-response>

response, management and coordination activities for cyber incidents occurring in the critical infrastructure sectors as well as Government entities at the Federal, State, Local, Tribal, and Territorial levels.

Cyber Threat Hunting.⁹ For assets related to National Critical Functions and which align to government priorities, CISA provides cyber hunting services focused on specific threat actors and their associated tactics, techniques, and procedures for the purposes of greater understanding of threat actor capabilities as well as assisting owners in securing at-risk assets.

The Protected Critical Infrastructure Information (PCII) Program enhances information sharing on the security of critical infrastructure between the public and private sectors with the government by protecting sensitive critical infrastructure information from disclosure per the Critical Infrastructure Information Act of 2002. To learn more visit [Protected Critical Infrastructure Information \(PCII\) Program | CISA](#) or email PCII-Assist@mail.cisa.dhs.gov.

Federal Bureau of Investigation (FBI). The FBI encourages victims of internet crimes to contact an **FBI field office**. Crime complaints can also be made to the bureau's Internet Crime Complaint Center (IC3) at www.ic3.gov.

MS-ISAC and E-ISAC. Members of the Multi-State ISAC and the Electricity ISAC should report incidents through established channels.

Fusion Centers. State or regional **Fusion Centers** are another possible reporting option. Fusion centers are effective at appropriately sharing information and have strong relationships with DHS and other organizations.

⁹ <https://www.cisa.gov/resources-tools/services/cyber-threat-hunting>

Australia

Utilities in Australia may report incidents to Australian Cyber Security Centre (ACSC) via **ReportCyber**, the Australian Government's online cybercrime reporting tool, or by calling 1300-CYBER1. If there is a threat to life or risk of harm, call 000 immediately.

Canada

Utilities in Canada may report incidents to the Canadian Centre for Cyber Security by visiting <https://www.cyber.gc.ca/en/incident-management>, calling 1-833-CYBER-88, or by emailing contact@cyber.gc.ca. If you believe a cyber incident is an imminent threat to life or of a criminal nature, please contact your local police services (**911**) or the RCMP. All victims are encouraged to report cybercrime activities to law enforcement.

RECOMMENDED RESOURCES

WaterISAC

Multi-State ISAC (MS-ISAC)

Electricity ISAC (E-ISAC)

Oil and Natural Energy ISAC (ONE-ISAC)

Drinking Water and Wastewater Resilience | U.S. EPA Office of Water

Information Sharing | CISA

InfraGard

National Fusion Center Association

Guide to Cyber Threat Information Sharing (SP 800-150) | NIST

WaterPro Conference | NRWA

Water Infrastructure Conference | AWWA



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



waterisac.org/fundamentals