American Water Works Association

Water Sector Cybersecurity Risk Management Guidance Version 4.0

Tool and Guidance Revision History		
Version	Date	Description
1.0	4/4/2014	Initial Release
2.0	2/22/2017	Revised to match updated Cybersecurity Guidance tool. The Use Case descriptions were revised for clarity. Use cases were added to address wireless communications. An additional 12 cyber controls were added.
3.0	9/4/2019	Revised to improve user interface. Explicitly supports Safe Drinking Water Act §1433 compliance as amended by section 2013 of Americas Water Infrastructure Act of 2018. Updates to the use cases and controls, and alignment with NIST Cybersecurity Framework v1.1. Provide Microsoft Excel-based output to allow for self-assessment of controls and development of an improvement plan.
4.0	5/12/2025	The major changes to this guidance document include: 1. Updated standard and guidance references. 2. Integration of the Small Systems Getting Started Guide into this document. 3. Updated control mapping to NIST CSF 2.0. 4. Development of companion documents including: a. Cyber Risk Management Plan Template b. Cyber-Incident Response Plan Template c. Cybersecurity Getting Started Guide

Disclaimer

The authors, contributors, editors, and publisher do not assume responsibility for the validity of the content or any consequences of its use. In no event will AWWA be liable for direct, indirect, special, incidental or consequential damages arising out of the use of information presented herein. In particular, AWWA will not be responsible for any costs, including, but not limited to, those incurred as a result of lost revenue.

TABLE OF CONTENTS

Figures

Tables

Appendices

Acknowledgements

This project was supported by an advisory committee and subject matter experts (SMEs), consisting of water system staff, consulting engineers, product manufactures, service providers and federal partners. The committee and SMEs provided technical input and review based on field experience and evolving threats that shaped revisions to the guidance and assessment tool.

Project Advisory Committee

John Brosnan, Santa Clara Valley Water District
Bill Johnson, East Bay Municipal Water District
Robert Raffaele, American Water
Doug Short, Trinity River Authority of Texas
Angela Sims-Ceja, City of Aurora (CO)

Subject Matter Experts

Victor Atkins, 1898 & Co.
David White, Axio Global, Inc.
Jim Livermore, CDMSmith
Garret Armentrout, Cybersecurity & infrastructure Security Agency (CISA)
Muhammad Mian, CISA
John Lucas, Citizens Energy Group
Scott Miller, Citizens Energy Group
Chad Donnelly, City of Richfield (MN) Public Works
Charley Cunningham, City of Sacramento (CA) Utilities
Jacques Brados, Direct Defense
Jeff Colson, EMA
Chris Sistrunk, Google Cloud
Patrick Norton, Interra
Ben Stirling, Jacobs
Andrew C. Krapf, Loudoun Water
Kevin Reifsteck, Microsoft
Jake Margolis, The Metropolitan Water District of Southern California
CheeYee "Chee" Tang, National Institute of Standards and Technology (NIST)
Chad Humphries, Rockwell Automation
Mel Hernoud, SNS/Layered Defense
Dave Espy, TetraTech
Nushat Thomas, US Environmental Protection Agency (USEPA)
Jennifer Lyn Walker, WaterISAC
Griffin Harrison, Xylem Inc.

Project Contractor

Andrew Ohrt, Joel Cox, Daniel Groves, Amanda Jones, David Garrison, Derek Zohner, Jeff Pelz
West Yost Associates
Davis, CA

Project Funding

Funding for this project was provided by the American Water Works Association.

PREPARED BY WEST YOST ASSOCIATES

American Water Works Association
6666 West Quincy Avenue
Denver, CO 80235-3098
303.794.7711
www.awwa.org

Acronym/ Abbreviation	Description
ANSI	American National Standards Institute
CCE	Consequence-driven Cyber-informed Engineering
CIE	Cyber-Informed Engineering
CFR	Code of Federal Regulations
CIA	Confidentiality, Integrity, and Availability
CIE	Cyber-Informed Engineering
CIR	Committed Information Rate
CISSP	Certified Information Systems Security Professional
CMM	Cybersecurity Maturity Model
CSF	Cybersecurity Framework
CPG	Cybersecurity Performance Goal
ERP	Emergency Response Planning
FOIA	Freedom of Information Act
HIPAA	Health Insurance Portability and Accountability Act
INL	Idaho National Laboratory
ISA	International Society of Automation
IT	Information Technology
LAN	Local Area Network
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology
OPSEC	Operations Security
OT	Operational Technology
PCI	Payment Card Industry
PII	Personally identifiable information
PLC	Programmable Logic Controller
QoS	Quality of Service
RRA	Risk and Resilience Assessment
SCADA	Supervisory Control and Data Acquisition
SLA	Service Level Agreement
SSO	Single Sign On
TTPs	Tactics, techniques, and procedures.
VLAN	Virtual Local Area Network
WAN	Wide Area Network

Executive Summary

Cybersecurity threats, including such things as cyber-terrorism and ransomware attacks, have grown from the esoteric practice of a few specialists several decades ago to a national security priority today. Critical infrastructure systems serving the people of the United States are vulnerable to such attacks and as a result, are being targeted. As noted in Cybersecurity Risk and Responsibility in the Water Sector[1]:

> "*Government intelligence confirms the water and wastewater sector is under a direct threat as part of a foreign government's multi-stage intrusion campaign, and individual criminal actors and groups threaten the security of our nation's water and wastewater systems' operations and data*."

In response to these evolving threats the American Water Works Association (AWWA) has prepared this guidance and assessment tool in given the water sector role as an essential lifeline function. These resources were originally issued in 2014 to facilitate use of the National Institute of Standards and Technology (NIST) Cybersecurity Framework version 2.0 (CSF) pursuant to Executive Order 13636 – Improving Critical Infrastructure Cybersecurity.[2] In addition, AWWA's resources support water and wastewater systems of all sizes, including those required to comply with Safe Drinking Water Act §1433, as amended by §2013 of Americas Water Infrastructure Act (AWIA) of 2018.[3]

What Does This Resource Provide to System Leadership?

- Method to exam potential cyber vulnerabilities based on how a system implements technology to support operations.
- Generates a risk-informed prioritization of actionable recommendations for cybersecurity controls to inform executive risk management decisions.
- Demonstration of due diligence based on standards from NIST and others that create a foundation for a Cybersecurity Risk Management Plan, which can also inform credit ratings and insurance underwriting.

---

[1] Cybersecurity Risk and Responsibility in the Water Sector. https://www.awwa.org/wp-content/uploads/AWWA-Cybersecurity-Risk-and-Responsibility.pdf

[2] Executive Order 13636 - Improving Critical Infrastructure Cybersecurity, https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity

[3] America's Water Infrastructure Act of 2018, Public Law 115-270, October 23, 2018. https://www.congress.gov/bill/115th-congress/senate-bill/3021/text

- An accessible and logical starting point for systems to quickly improve their cybersecurity posture through the implementation of the cybersecurity controls and capabilities that enhance resilience to cyberattacks.

Use of this Guidance to Support AWIA §2013 (SDWA §1433) Compliance

A key objective of the AWWA Water Sector Cybersecurity Risk Management Guidance (AWWA Guidance) and associated AWWA Cybersecurity Assessment Tool (AWWA Cybersecurity Assessment Tool) is to support systems with AWIA §2013 (SDWA §1433) compliance. In addition, the Operational Guide to AWWA Standard J100-21 provides potential ways to integrate the results of an analysis based on this guidance and assessment tool with the quantitative approach defined in the J100-21 Standard.[4]

Water system staff responsible for AWIA §2013 (SDWA §1433) compliance may not be cybersecurity technologists or responsible for the OT (operational technology) and/or enterprise IT (information technology) systems.[5] Therefore, it is recommended that a system convene internal and external support staff, including, but not limited to:

- Staff responsible for AWIA §2013 (SDWA §1433) compliance.
- Staff responsible for and knowledgeable of the design, operation, and maintenance of the OT and enterprise IT systems.
- Leadership responsible for overall operation of the system (i.e. staff with the authority to accept operational risks).
- Staff responsible for budgeting, including operations and maintenance, and capital improvement projects.
- External support as appropriate, including integrators, cybersecurity vendors, engineering firms, etc.

[4] AWWA. Operational Guide to AWWA Standard J100 Risk & Resilience Management of Water & Wastewater Systems. https://store.awwa.org/Operational-Guide-to-AWWA-Standard-J100-Risk-Resilience-Management-of-Water-Wastewater-Systems

[5] The term Operational Technology (OT) is used to represent all control system hardware, software, and firmware. The term enterprise Information Technology (IT) is defined as the computer, data storage, and networking infrastructure and processes that are used to create, process, store, secure, and exchange all forms of electronic data.

This approach improves the quality and timeliness of data collection and analysis. In addition, it is expected to reduce the overall time required to complete compliance actions while improving the cybersecurity posture[6] of the organization.

Use of this Guidance to Support Additional Compliance or Audit Requirements

In addition to AWIA §2013 (SDWA §1433) compliance, this guidance and assessment tool supports state compliance obligations, insurance underwriter and rating agency evaluations. The assessment tool output also provides a mapping to the cybersecurity controls prioritized by the EPA.[7]

Use of the EPA's checklist has increased through their technical assistance program and §1433 enforcement inspections completed by EPA regions. In addition, some state primacy agencies may use the EPA checklist for educational outreach and in some cases state regulatory requirements. Note that there is not always a direct one-to-one mapping. Where appropriate, the AWWA guidance notes where multiple controls map to a single EPA Priority Cybersecurity Practice. Once the user completes an assessment using the AWWA Tool, a tab with the mapping will be populated as part of the assessment tool output.

AWWA's Cybersecurity Guidance, Resources, and Tool Output Information Security

The output of the Assessment Tool and associated resource completed by a system should be classified as critical infrastructure security information. In many states, this means that it is protected from public information requests. To maintain a high level of information security after the output is generated, AWWA strongly recommends the following:

- If the system has a data classification system in place, treat the output and associated information as the most protected type of information. It is recommended that this be done with consideration to the FOIA/sunshine laws in the system's jurisdiction.

[6] The cumulative strength of a system's cybersecurity policies, controls, and how effectively they mitigate risk.

[7] EPA Guidance on Improving Cybersecurity at Drinking Water and Wastewater Systems (EPA 817-B-23-001) https://www.epa.gov/system/files/documents/2024-08/epa-guidance-on-improving-cybersecurity-at-drinking-water-and-wastewater-systems-1.pdf

- If the system does not have a data classification system in place, store the data, outputs and associated plans in a secure location.

Restrict access to this information as much as possible. For example: do not email files containing sensitive information. AWWA's *Protecting the Water Sector's Critical Infrastructure Information* provides a state-specific assessment of statutes protecting systems' sensitive information.[8]

[8] Systems should always consult with legal counsel regarding disclosures of security sensitive information, which is often protected by state law. A summary of state laws is provided in AWWA's report "Protecting the Water Sector's Critical Infrastructure Information".

Introduction and Background

In February 2013, the AWWA Water Utility Council initiated a project (WITAF #503) to address the absence of practical, step-by-step guidance for protecting OT in water systems from cyber-attacks. This project was timely as it corresponded with the development of the NIST Cybersecurity Framework (CSF) as called for in Executive Order (EO) 13636. The NIST CSF includes a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks.

This AWWA Guidance and associated AWWA Cybersecurity Assessment Tool, collectively referred to as AWWA Cybersecurity Guidance and Assessment Tool, represent a voluntary, sector-specific approach for adopting the NIST CSF as expressed by the Water Sector Coordinating Council. The original goal of this guidance was to provide water system owners/operators with a consistent and repeatable assessment tool and recommended course of action for mitigating vulnerabilities to cyber-attacks as recommended in the NIST CSF per EO 13636 and ANSI/AWWA G430: Security Practices for Operations and Management. The guidance also communicates a "call to action" for water system executives to acknowledge the importance of securing OT and enterprise IT given their role in sustaining the continuity of operations.

Updates to the AWWA Cybersecurity Guidance and Assessment Tool have been developed to assist community water systems (i.e. systems) in complying with AWIA §2013 (SDWA §1433).[9] AWIA requires all community water systems serving populations of 3,300 or more persons to conduct and certify completion of an assessment of the risks to, and resilience of their systems, including an emergency response plan. The requirement places emphasis on assessing and mitigating cybersecurity risks that could impact the following:

- Electronic, computer, or other automated systems (including the security of such systems) which are utilized by the system;
- The monitoring practices of the system [including network monitoring]; and
- The financial infrastructure of the system [accounting and financial business systems operated by a utility, such as customer billing and payment systems].

[9] The full text of the Safe Drinking Water Act §1433 Risk and Resilience Assessment and Emergency Response Plan Provisions is included in Appendix A.

Systems may have OT and enterprise IT systems that are physically or logically connected. In addition, many business applications that systems rely on to support critical day-to-day operations reside within enterprise systems. To account for this, business applications are explicitly included in the AWIA §2013 (SDWA §1433) requirements for the risk and resilience assessment (RRA) and emergency response plan (ERP).

AWWA consulted a panel of subject matter experts (SMEs) to identify the most pressing cybersecurity issues facing water systems in the development of these resources. In response, the subject matter experts crafted groupings of cybersecurity practices that are prioritized based on criticality in addressing cybersecurity risks in the water sector. This guidance provides a discussion of the recommended practice areas and why they are important to supporting a robust cybersecurity risk management strategy.

The recommended practices are defined by a set of 100 cybersecurity controls, primarily from the NIST CSF. The controls are organized in a manner intended to facilitate the implementation of actionable tasks. The NIST CSF controls are supplemented by other best practices as appropriate and noted in relevant sections of the guidance. The outputs of the AWWA Cybersecurity Assessment Tool are designed to present these controls to users in a concise, straightforward manner that facilitates documentation, supports implementation as appropriate, and informs future cybersecurity risk management plans.

The AWWA Cybersecurity Assessment Tool generates a prioritized list of recommended controls based on specific characteristics of the system being assessed. The user provides information about how the system uses technology with the OT and enterprise IT systems. Based on the system's use of technology, the assessment tool maps a response that corresponds to the relevant cybersecurity controls and associated priority. For each recommended control, specific references to existing cybersecurity standards are also provided.

The AWWA Cybersecurity Assessment Tool emphasizes actionable recommendations with the highest priority assigned to controls that are expected to provide the greatest and most immediate risk reduction value, if implemented. It should be noted, however, that the tool does not assess the extent to which a system has implemented any of the recommended controls. It is the responsibility of the system to make that determination.

This resource is a living document and is subject to periodic revisions and enhancements based on the evolving cyber-threat landscape and user feedback.

Water Sector Cybersecurity Maturity Model

To support water and wastewater systems with benchmarking improvements to cybersecurity practices, a maturity model was developed to guide a systems' progress. *Maturity* is a concept that is widely used by practitioners to characterize various stages of growth and strength. Generally, the maturity of a system's cybersecurity posture is based on the extent to which a system has implemented and maintained the recommended cybersecurity controls. A successful cybersecurity program balances the need to maintain defensive capabilities that are components of cyber-risk management. This means a cybersecurity program should include cybersecurity controls from each of the NIST CSF function categories to effectively manage cyber-risk to the system. The NIST CSF functions are shown in Figure 1.

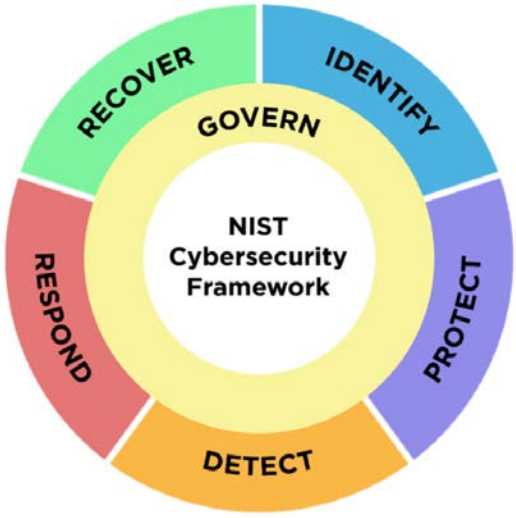


Figure 1 – NIST CSF v2.0 Functions

A core objective of the maturity model is to support water and wastewater systems with practical guidance on how to both create secure and resilient operations and maintain those operations over the long-term. The water sector cybersecurity maturity model developed by AWWA as shown in Figure 2 include three specific phases of action to be taken by a system. Regardless of where a system is in their cybersecurity maturity, a system should always begin with Phase 1 to ensure that the fundamentals have been implemented and sustained. The three phases are described in the following sections.

Figure 2 – Water Sector Cybersecurity Maturity Model

Phase 1 – Getting Started on Cybersecurity Fundamentals: "The First Mile"

Phase 1 is designed to support systems that are getting started with cybersecurity planning and improvements. This part of the process applies to all systems, including those with more mature cybersecurity programs with the intent of ensuring that the relevant Phase 1 practices are in place. These practices are recognized a being foundational to the successful implementation of a cybersecurity risk management program. The technical practices in Phase 1 have been demonstrated to provide the most immediate protection against common cyber-attacks. The organizational and cultural practices ensure programs sustainability. In the Phase 1 portion of the Assessment Tool the system will examine current practices and capabilities using a set of questions that will automatically generate a Getting Started Guide tailored to the systems response. A template of the Getting Started Guide is provided in Appendix B.

Every system, regardless of size and type, should complete Phase 1 and 2 prior to implementing Phase 3. The practices included in Phase 1 are consistent with CISA's *Primary Mitigations to Reduce Cyber Threats to Operational Technology*.[10]

Phase 2 – Cybersecurity Risk Management Planning

In this phase the system will complete two steps:

1. Conduct a cybersecurity assessment.
2. Complete and Implement a Cybersecurity Risk Management Plan.

Each step is explained in more detail in the following sections.

Conduct a Cybersecurity Assessment

After completing Phase 1, the system should conduct a cybersecurity assessment. When the user navigates to Phase 2 within the Assessment Tool, there are three options for conducting a cybersecurity assessment:

- **Option 1: AWWA Small System Assessment** – This option is designed for systems serving less than 10,000 people. It is based on six cybersecurity practice categories, covering 28 controls that are typically the most applicable within small systems. When implemented these controls provide immediate risk reduction value to the systems cybersecurity posture.
- **Option 2: AWWA Assessment** – This option directly aligns with the controls in the NIST CSF and other relevant controls as described in the Cybersecurity Tool User Guidance section below.
- **Option 3: CSET® Integration** – For systems that would like an option that provides an even broader cyber vulnerability assessment, the completed AWWA Assessment Tool Excel file may be uploaded to CSET®.[11] CSET® is maintained by the Department of Homeland Security (DHS). AWWA and DHS collaborated on a process that allows users to upload the completed Excel spreadsheet to access additional features and continue to evolve the user's cybersecurity assessment

[10] *Primary Mitigations to Reduce Cyber Threats to Operational Technology.* https://www.cisa.gov/resources-tools/resources/primary-mitigations-reduce-cyber-threats-operational-technology. Last Accessed: May 8, 2025.

[11] Cyber Security Evaluation Tool (CSET). https://www.cisa.gov/resources-tools/services/cyber-security-evaluation-tool-cset. Last Accessed: December 11, 2024.

efforts. Once uploaded, CSET® will automatically populate the relevant and comparable controls. The user will then have additional controls to evaluate.

Completion of a cybersecurity assessment provides the system with important context to conduct both capital and operations planning to better manage cyber-risk.

Develop and Implement a Cybersecurity Risk Management Plan

Once the assessment is complete, the system should proceed in developing a Cybersecurity Risk Management Plan (CRMP). A CRMP may contain a variety of information, but generally it establishes the cybersecurity goals and an associated plan for the system to improve cybersecurity practices and be responsive to an evolving threat environment. To support systems with the development of a CRMP, a template is included as Appendix C. In addition, a Microsoft Word version of the template is available at https://www.awwa.org/cybersecurity.

Systems should download the CRMP template to support their cybersecurity risk management planning effort. The CRMP is adaptable to meet the needs of the system regardless of its maturity. The goal is to provide a repeatable process that a system can follow to support cyber-risk management and compliance.

Phase 3 – Cybersecurity Risk Management Plan Implementation

Once a system has completed Phase 2, including developing a CRMP, they should move into Phase 3. In this phase, the CRMP previously developed in Phase 2 will be implemented and sustained for continuous improvement. This will include iterative implementation and planning processes to support the changing needs of the system within the evolving threat environment.

Resources to Support Maturity

The maturity model presented on Figure 2 provides three distinct phases that any water or wastewater system can mature through to create a risk-based cyber-risk management program. There are numerous cybersecurity resources and assessment methodologies available to systems from AWWA and various federal agencies. This guidance and the AWWA resources align to the NIST CSF. In version 2.0 of the NIST CSF, four tiers of maturity are presented. The NIST CSF and accompanying resources can provide additional guidance and insights into establishing a sustainable cyber-risk management program.

The Tiers range from Tier 1 – Partial to Tier 4 – Adaptive. The NIST Tiers describe the degree to which a system's cyber-risk management practices exhibit the characteristics defined in the NIST CSF.[12] The tier descriptions are tailored for the water sector, as follows:

1. **Tier 1 – Partial** – There is limited awareness of cybersecurity risks at the organizational level.
2. **Tier 2 – Risk-Informed** – There is an awareness of cybersecurity risks at the organizational level, but an organization-wide approach to managing cybersecurity risks has not been established.
3. **Tier 3 – Repeatable** – There is an organization-wide approach to managing cybersecurity risks. Cybersecurity information is routinely shared throughout the organization.
4. **Tier 4 – Adaptive** – The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. Through a process of continuous improvement that incorporates advanced cybersecurity technologies and practices, the organization actively adapts to a changing technological landscape and responds in a timely and effective manner to evolving, sophisticated threats.

Figure 3 provides a mapping of AWWA resources, other resources, and NIST Tiers and how they align with the Water Sector Maturity Model.

Summary – Water Sector Cybersecurity Maturity Model

Using this guidance and the Assessment Tool, systems should assess the controls in place and their associated implementation status (i.e. maturity) on a recurring basis. This should consider the current and anticipated needs of the system, the current cybersecurity posture of the system, and the threat landscape. Broadly, the objective should be to continuously move from the minimum controls applied *ad hoc* to adaptive management.

The Water Sector Cybersecurity Maturity Model provides a clear and repeatable decision support process to guide a water systems evaluation of cybersecurity vulnerabilities and actions that, if implemented, will mitigate risks and enhance resilience. Systems mature through the implementation and maintenance of cybersecurity practices and controls. These improve the risk and resilience

[12] NIST. The NIST Cybersecurity Framework (CSF) 2.0. February 26, 2024. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf. Last Accessed: December 9, 2024.

management of the system to ensure continuity of operations and service to customers. The next section provides a background on the types of cybersecurity controls relevant to water and wastewater systems.

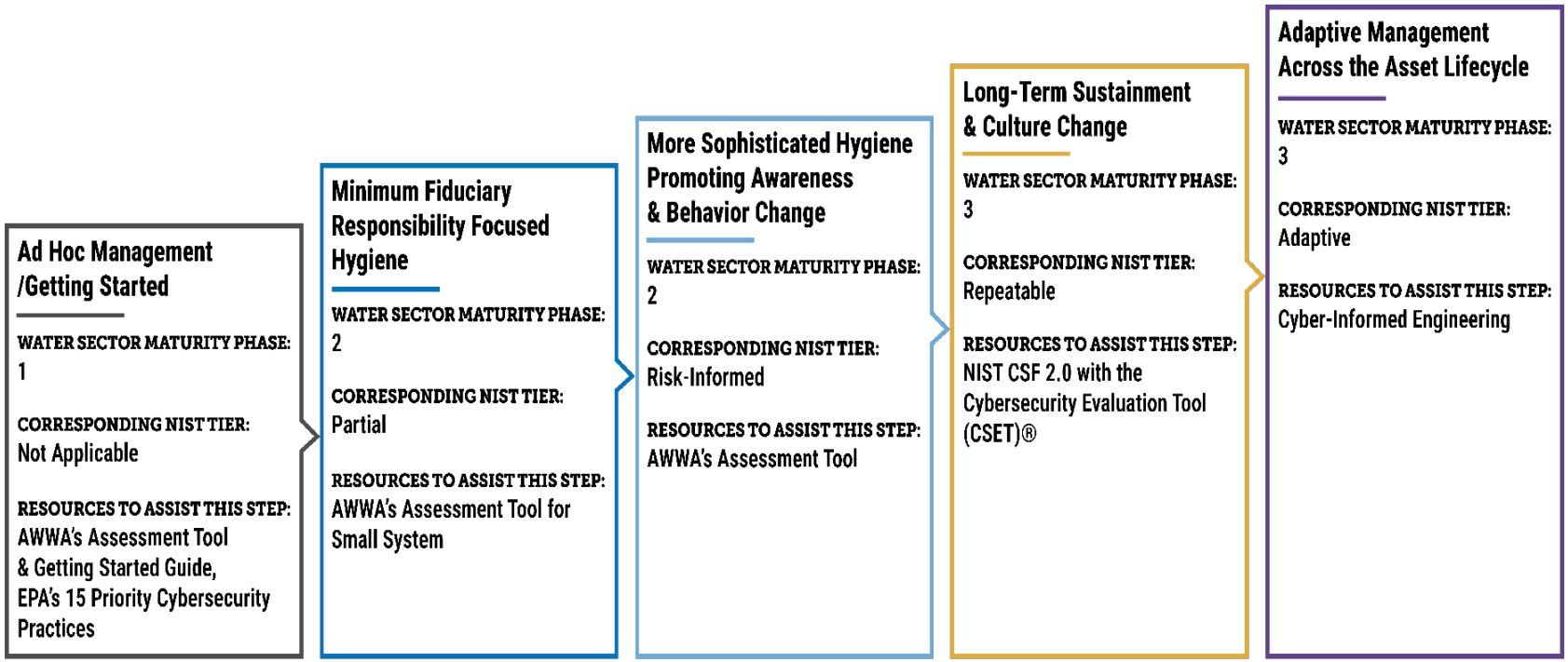


Figure 3 – Water Sector Cybersecurity Maturity, NIST CSF v2.0 Tiers, and Associated Resources

Cybersecurity Controls

A security control is a measure to support effective cyber-resilience. Most of the controls in this document are measures designed to increase resilience and reduce risk; they were developed primarily from the NIST CSF. In some cases, closely associated controls were merged into a single, more comprehensive control. Some controls are complex and might resemble an administrative program, a technical solution, or an engineering design methodology. Many cybersecurity vendors provide programs, packages, and services to support the implementation of controls with greater complexity (e.g., network monitoring tools). Appendix D provides a list of the cybersecurity controls developed for this guidance. A table mapping the Appendix D controls to the controls presented in the NIST CSF v2.0 is included as Appendix E.

Cybersecurity Control Priority Categories

Every control has been assigned a priority level based a review by water sector SMEs considering the criticality and potential impact to the security of the system. The recommended controls are categorized into priorities 1, 2, 3, and 4, with Priority 1 being the highest. The intent is to focus system resources on foundational controls that successively build a defense-in-depth cybersecurity posture. For each recommended control, a reference is provided to a set of existing cybersecurity standards. Priority levels are defined as follows:

- **Priority 1 Controls** – These controls represent the highest priority for the security for OT and enterprise systems. If not already in place, these controls should be implemented immediately to eliminate critical cyber vulnerabilities that are known to be frequently exploited. Generally, these are fundamental cyber-hygiene measures that help the system maintain secure operations.
- **Priority 2 Controls** – These controls build on those in the Priority 1 category and provide an additional level of risk mitigation that can immediately increase in the security of the system. Generally, these are more sophisticated cyber-hygiene measures focused on improving the process, architecture, and technical capabilities of the system. These improvements include capabilities such as monitoring of networks and computer systems to detect attack attempts, locate points of entry, interrupt infiltrated attackers' activities, identify compromised assets, and gain information about the sources of an attack.
- **Priority 3 Controls** – These controls improve cyber-hygiene practices to reduce the number and magnitude of vulnerabilities and improve the operations of networked computer systems. They focus on protecting against poor security

practices by system administrators and end-users that could give an attacker access and an advantage. These controls are essential for sustained implementation of a cyber-risk management program . These typically include more advanced controls that require longer-term actions necessary to address cyber-risks, such as Cyber-Informed Engineering (CIE) and cyber supply chain risk management.

- **Priority 4 Controls** – These controls are more intricate and when implemented demonstrate a mature and sophisticated cybersecurity program. These controls provide greater protection against more sophisticated attacks. These include integrated technologies, policies, and practices that may be more resource-intensive to implement and maintain.

Each of the cybersecurity controls falls into a practice category. These are described in the following section.

Practice Categories

The practice categories were chosen by subject matter experts during a Definition Workshop held during the original project in 2013. Since then, these practice categories have been maintained and expanded upon. Each team identified important areas of cybersecurity to be addressed and policies, activities, and systems that should be implemented. The recommendations from the subject matter experts were collected, integrated (to avoid duplication), and loosely organized into the ten domains of the Certified Information Systems Security Professional (CISSP) Common Book of Knowledge. Several reviews and additions followed until there was consensus that the practice categories and recommendations were comprehensive. The categories (like their NIST framework counterparts) are not mutually exclusive and contain significant overlap. In addition, the AWWA Assessment Tool output categorizes the recommended controls into these practice areas. The following is a description of each practice category and some potential improvement projects.

Governance and Risk Management

This category is concerned with the management and executive control of the security systems of the system; it is associated with defining system boundaries and establishing a framework of security policies, procedures, and systems to manage the confidentiality, integrity, and availability (CIA) of the system. One of the key components of system governance is developing and maintaining an accurate, up-to-date inventory of OT and enterprise system components.

Cyber supply chain risk management and is an important component in the design, operation, and maintenance of OT enterprise systems. This includes such things as establishing cybersecurity requirements for suppliers, communication of these requirements, and verifying the requirements are met.

From the perspective of long-term security, this is the most important category because it creates a managed process for increasing security. It also engages the executive team by including security risks as an important part of enterprise risk management. Some potential improvement projects are provided below:

1. Develop a formal, written Cybersecurity Policy that addresses the specific operational needs of OT and enterprise systems.
2. Establish an Enterprise Risk Management strategy that associates cybersecurity investments with enterprise business plans.

This practice category aligns with the new NIST CSF 2.0 Govern function.

Business Continuity and Disaster Recovery

This category is concerned with ensuring that critical systems continue running even when faults occur and with rapid recovery after a service disruption.

Business Continuity Planning is a structured method for a system to prepare for and reduce the probability and impact of systems and operational failure. A key component of Business Continuity Planning is the Disaster Recovery Plan, which deals with longer disruptions from more impactful events.

Both plans require a managed process that identifies potentially disruptive events, estimates their impact, and then develops and monitors mitigation strategies.

Some potential improvement projects are provided below:

1. Develop resilience plans including Emergency Response Plan, Continuity of Operations Plan, and/or Disaster Recovery/Business Continuity Plan. These plans should include:
    a. Crisis Management Team (including at least one representative from executive management) – with authority to declare an alert or a disaster and who monitors and coordinates the necessary recovery activities.
    b. Manual overrides to allow temporary manual operations of key processes during an outage or a cyber-attack.

    c. Strategies for system redundancy (or offline standby) to ensure key system components can be restored within acceptable timeframes.
2. Conduct exercises to test and revise plans and build response capabilities.
3. Test backup and recovery plans regularly.

AWWA G440-22 standard and M19 manual provide extensive response planning guidance. A Cyber-Incident Response Plan (CIRP) template is included in Appendix F and at https://www.awwa.org/cybersecurity.

Server and Workstation Hardening

This category is concerned with securing servers and workstations against cyber-attacks; it identifies best practices to minimize the probability of unauthorized access to servers, and to maintain the CIA properties of the servers and the systems within them. For example, this category includes following the Center for Internet Security (CIS) Benchmarks that provide a prescriptive list of configuration recommendations.

Some potential improvement projects are provided below:

1. Remove local administrator rights, delete/disable default accounts (OS and application).
2. Rename Administrator account.
3. Disable USB, DVD, and other external media ports.
4. Disable auto-scan of removable media.

Access Control

This category is concerned with ensuring that only authorized personnel are permitted to access computing resources within the system; it pertains to best practices for restricting access to computing resources and information to authorized users. Care should be taken to ensure that different passwords are used to access OT and enterprise systems. For example, implementing centralized authentication (e.g. Microsoft Active Directory) for OT systems.

Some potential improvement projects are provided below:

1. Physical access to facilities and equipment.
2. Vendor, contractor system access on plant (incl. package systems). Vendor or contractor access to system should be manually initiated.
3. Require multifactor authentication (e.g. tokens) for any remote access.

Application Security

This category is concerned with ensuring that computer programs do only what they are supposed to do; for example, suppose that a module of a Supervisory Control and Data Acquisition (SCADA) system is supposed to receive data from a Programmable Logic Controller (PLC) and save it. Application security contains best practices to ensure that the module is not susceptible to buffer-overflow attacks and that the data it receives does not get corrupted as it is handled by the module.

Application Security is a complex and extensive area involving the design, implementation, and testing of program modules as well as the testing and monitoring of integrated systems after implementation. Systems should develop standard design and implementation requirements that define the testing required by software vendors and system integrators, as well as doing their own testing of the integrity of results.

Some potential improvement projects are provided below:

1. Require each OT or enterprise system user to utilize unique credentials (usernames and passwords) which provide only the required level of access needed to perform their job.
2. Provide separate accounts for administrator and user functions. Do not allow users to operate with administrator rights unless they are administering the system.
3. Implement audit controls such as logging and monitoring of system access and modification.

Encryption

This category is concerned with ensuring that only appropriate encryption schemes are used within an system's security systems and that the cryptography is used wherever it is needed. For example, there is general confusion of what is an appropriate encryption scheme: sometimes packing or compression algorithms are called encryption. Also, cryptographic systems must be used wherever they are needed, for example, if the data will be traveling on a public channel or via a wireless circuit, or if there is a need to provide non-repudiation of a message or a document (by using a cryptographic signature).

Weak encryption schemes are particularly dangerous because they provide little protection and create a false sense of security and complacency. Proprietary encryption schemes should be avoided since they typically have not gone through comprehensive

testing and often contain flaws. Also, only encryption schemes that are referenced by appropriate standards and use keys of proper length should be considered secure.

Some potential improvement projects are provided below:

1. Implement communications encryption:
    a. Wireless communications should be encrypted where possible, regardless of type or range.
    b. Wired communications over shared infrastructure (e.g. leased, shared) should be encrypted using VPN technologies to protect sensitive information in transit.

Data Security

This category is concerned with various types of protected data that a system may collect, transfer and store. This includes payment information like credit and debit cards (PCI), personally identifiable information (PII), and health information protected according to Health Insurance Portability and Accountability (HIPAA) requirements. These requirements are included in this category.

Some potential improvement projects are provided below:

1. Implement appropriate measures to accept, process, store, and/or transmit customer billing information.
2. Implement controls to protect Personally Identifiable Information (PII).
3. Implement controls to achieve and maintain HIPAA compliance.

Telecommunications, Network Security, and Architecture

This category is concerned with the security of the network infrastructure from the data connector on the wall to the enterprise switches, routers, and firewalls. This includes the physical security of the cables, the telecom closets, and the computer rooms, and the protection of the data as it travels on public channels and wireless circuits. Spam filtering and website blocking are also included in this category.

The focus of this category is establishing a “defense-in-depth” network architecture with the network at its core. It also addresses adherence to new standards for OT network security, particularly network topology requirements within the vicinity of OT systems and PLC controls. Another area addressed in this category is network management, including port level security.

Some potential improvement projects are provided below:

1. Implement multiple levels of network security protection (firewalls, anti-virus, etc.).
2. Implement network segmentation.
3. Implement security information and event management (SIEM) to provide real-time monitoring of all OT systems.

A network architecture reference diagrams illustrating the Purdue Model for Industrial Control System security is presented in Appendix G. Network architecture drawings for small water and wastewater systems are included in Appendix H. In addition, the adoption of cloud technologies within or in support of system's operations require additional consideration. The SCADA in the Cloud: Risk and Resilience Management report is included as Appendix I.

Physical Security of OT Equipment

Physical security is a basic requirement for all OT and enterprise systems. Once physical access to a network device or server is achieved, compromising equipment or systems is usually a trivial matter. The recommended practices in this category focus on preventing and restricting physical access to only authorized personnel with a need to perform some action on the hardware. The recommendations in this group are also related to monitoring, detecting, and responding to unauthorized physical access.

Some potential improvement projects are provided below:

1. Control and monitor access to:
    a. Control rooms.
    b. Equipment cabinets and closets.

AWWA's G430-2024 provides guidance on physical security practices.

Service Level Agreements (SLA)

This category is concerned with the definition and management of contracts that specify services requirements to the system. The contract manager under the direction of the executive team is responsible for defining, negotiating, executing, and monitoring these contracts to ensure appropriate service delivery to the system.

An SLA is a contract which requires minimum levels of performance for services provided. For example, the Committed Information Rate (CIR) is part of a typical Wide-Area Network (WAN) SLA and specifies the minimum bandwidth that a data circuit may have.

SLAs for OT network systems typically focus on quality of service (QoS) rather than bandwidth. OT systems do not require high bandwidth but cannot operate properly if the bandwidth falls below certain known thresholds. Conversely, SLAs for enterprise systems will focus on confidentiality and integrity of information stored or in transit on the network.

Some potential improvement projects are provided below:

1. Establish SLAs with staff and contracted employees for responsiveness and agreement to respond in emergency conditions.
2. Identify all external dependencies and establish written Service Level Agreements and support contracts with support providers to clearly identify expectations for response time and restoration of services.

Operations Security (OPSEC)

OPSEC is concerned with refining operational procedures and workflows to increase the security properties (CIA) of a system. For example, a system may want to restrict what employees post on their social media pages about the system's security procedures. OPSEC also includes access granting policies and procedures, security guard rotation schedules, backup recovery procedures, etc.

Some potential improvement projects are provided below:

1. Provide clear demarcation between enterprise and OT functions. Isolate all non-OT functions and block access from OT equipment to:
    a. Internet browsing
    b. Email
    c. Any other non-OT access to remote systems or services

Education

This category is concerned with bringing security awareness to the employees, clients, and service providers of the system.

Education involves identifying best practices and providing formal training on the security policies and procedures of the enterprise as well as security awareness and incident response. It involves test practice of the key security processes and actions to ensure quick and accurate response to security incidents within the enterprise.

Some potential improvement projects are provided below:

1. Implement a cybersecurity awareness program that includes social engineering.
2. Promote information sharing within the system.
3. Participate in water sector programs that facilitate cybersecurity knowledge transfer.

Personnel Security

This category is concerned with the personal safety of employees, clients, contractors, and the general public. Personnel security starts as part of the hiring process and ends after the employee leaves the system. It handles periodic reaccreditation of employees and updates of the policies and procedures that govern staff. The purpose of personnel security is to ensure the safety and integrity of staff within the system. Personnel security also applies to external contractors and service personnel, with the objective to ensure appropriate, lower privileged access to facilities.

Some potential improvement projects are provided below:

1. Implement a personnel security program for internal and contracted personnel that includes:
   a. Training
   b. Periodic background checks
2. Require annual and new employee signoff on cybersecurity policies.

Cyber-Informed Engineering

Cyber-Informed Engineering (CIE)[13] and the associated Critical Function Assurance (CFA)/Consequence-driven, Cyber-informed Engineering (CCE)[14,15] are methodologies developed and promulgated by Idaho National Laboratory (INL). The methodologies emphasize the integration of cyber risk considerations into the full engineering life-cycle to reduce current and future cyber-risk. These approaches recognize that, while cyber-hygiene controls are essential, they cannot address the rapidly evolving cyber threats

[13]Wright, Virginia L., et al. Cyber-Informed Engineering Implementation Guide. https://www.osti.gov/biblio/1995796. September 5, 2023. Last Accessed: December 9, 2024.

[14] Gellner, Jeffrey R. et al. Critical Function Assurance: Understanding Critical Function and Critical Function Delivery is Foundational for Meaningful ICS Security Improvement and Policy Efforts. https://inldigitallibrary.inl.gov/sites/STI/STI/Sort_75387.pdf. Last Accessed: December 9, 2024

[15] Bochman, Andy. The End of Cybersecurity. Harvard Business Review. May 2018.

facing critical infrastructure. Therefore, systems need to take additional measures to ensure that their systems are cyber-resilient.

Common approaches for water and wastewater systems include being able to operate the system systems in the absence of automation and including cyber-physical controls (e.g. electro-mechanical relays) within the engineering design and construction of the system. However, CIE goes into much greater depth on a wide range of cybersecurity topics shown in the table below.

Table 1 – CIE Principles

Consequence-focused design	**Interdependency evaluation**
Engineered controls	Digital asset awareness
Secure information architecture	Cyber-secure supply chain controls
Design simplification	Planned resilience
Resilient layered defenses	Engineering information control
Active defense	Cybersecurity culture

Extensive discussion of each of these topics may be found in the CIE Implementation Guide.

Cybersecurity Assessment Tool User Guidance

The Assessment Tool uses several steps to apply user responses regarding the system's current cybersecurity posture and maps that input to the relevant controls recommended for cybersecurity improvements and facilitate AWIA §2013 (SDWA §1433) compliance.

NOTE: AWWA DOES NOT COLLECT OR RETAIN ANY DATA ENTERED IN THE ASSESSMENT TOOL OR ABOUT USERS OF THE TOOL

Together this guidance, the Assessment Tool, and supporting templates provide the user with a set of controls and potential actions requiring implementation based on how the system describes the application of certain technologies and practices in their day-to-day operations. No sensitive information is required or shared by the user.

Process Overview

The Assessment Tool is design to help systems progress through the three phases of the Cybersecurity Maturity Model as shown in Figure 4. When a system works through each of the phases, they also help satisfy the AWIA §2013 (SDWA §1433). In the Microsoft Excel File box shown on Figure 4 and the output fil generated by the Tool, each tab has a color to indicate it's intended function:

- Blue – Supports compliance with the RRA provisions.
- Green – Supports compliance with the ERP provisions.
- Yellow – Provides user guidance and background information on the use of the output.

Regardless of the size and sophistication of the system, each new user should start with Phase 1. The following sections provide additional detail on the individual inputs, processing steps, and outputs of the Assessment Tool.

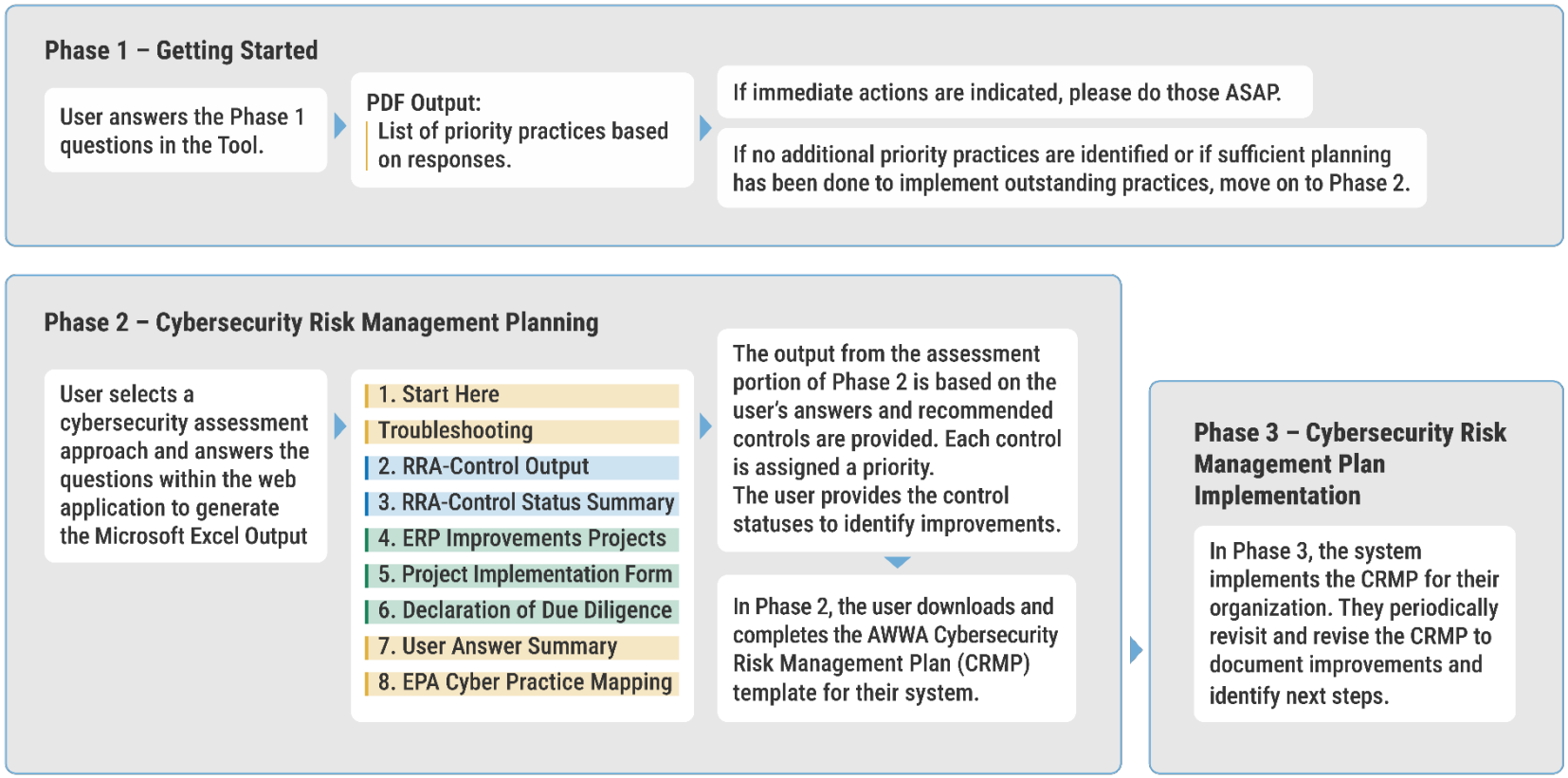


Figure 4 – AWWA Cybersecurity Assessment Tool Process

User Interface

The Assessment Tool opens to a welcome page that provide users with a summary of the purpose and recommendations on system staff that may contribute to the cybersecurity assessment. It is recommended that users review the summary of questions in Appendix C to prepare appropriate responses directly or based on feedback from others, as needed. Once a user begins answering questions within the tool, they must complete the session since no input data is retained by AWWA. The only record of the session is in the output report generated and sent to the user.

Following the welcome page, users have the option to select Phase 1 or Phase 2. It is recommended that all users complete Phase 1 prior to initiating Phase 2. Training that supports use of this guidance and tool can be accessed at https://www.awwa.org/cybersecurity.

Additional details on users' actions taken within these phases are described below.

Phase 1 – Getting Started on Cybersecurity Fundamentals: "The First Mile"

This phase requires used to answer 11 questions focused on cybersecurity practices considered to be fundamental to cyber-risk management for any system. Seven of these questions are based on essential technical practices. Four questions target key organizational and cultural practices that help a system create a sustainable cyber-risk management plan. The questions are described below with additional details provided in Appendix J.

Implement the Technical Basics

Phase 1 directs the system to focus on implementing fundamental technical cybersecurity practices. These practices have been demonstrated to provide the most immediate protection against common cyber-attacks. The system will examine current practices and capabilities using the following questions to generate a Getting Started Guide tailored to the responses provided. The first seven Phase 1 questions are focused on fundamental technical practices that support good cyber-hygiene:

1. Does the system have public internet facing devices/surfaces?
    1.1 Does the system currently conduct vulnerability scanning of public internet facing devices?
2. Does the system use remote access to access systems?
    2.1 Does the system enforce multi-factor authentication for remote access?
3. Does the system require unique usernames and passwords for each user?
    3.1 Does the system enforce password management best practices?
4. Does the system have a cyber-incident response plan (CIRP)?
5. Does the system update default passwords on all network devices and have policy indicating staff/contractors must do this?
6. Does the system monitor internal network traffic via firewalls or another monitoring solution?
7. Does the system have backups of all critical software and programs?
    7.1 Does the system test recovery of critical software and programs

These should be answered with input from system staff and support contractors as necessary.

Establish a Cultural and Organizational Foundation

The last four Phase 1 questions are related to establishing a cultural and organizational foundation that supports a cyber-secure and resilient system. These questions include:

1. Does the system leadership team (board, council, etc.) address cybersecurity at least once, annually?
2. Does the system budget for cybersecurity improvements?
3. Does the system have a defined risk management leader?
4. Does the system provide cybersecurity training to all employees?

After all questions are answered, the Assessment Tool generates a report based on the user's response and provides recommendations on why implementation is important and provides suggestions on how to approach implementation if the user indicates a practice is not currently in place.

These Phase 1 practices have been shown to provide the most immediate protection and sustainable planning benefits to the system, therefore these practices should be prioritized for implementation as soon as possible. Upon completion of Phase 1 the system should conduct a cybersecurity assessment as described in Phase 2. Several assessment options are available to the system in Phase 2 as discussed in the following section.

Additional details on each of these Phase 1 questions, including how to determine if the system is currently practicing these controls, are provided in Appendix B.

Phase 2 – Cybersecurity Risk Management Planning

In this phase the system will complete two steps:

1. Complete a Small System Assessment or AWWA Cybersecurity Assessment
2. Complete and implement a Cybersecurity Risk Management Plan

Each step is explained in more detail in the following sections.

Complete a Cybersecurity Assessment

When the user navigates to Phase 2 within the Assessment Tool, the user has three options for conducting a cybersecurity assessment. Each of these options and guidance on the use of each option is discussed in more detail in the following sections.

- **Option 1: AWWA Small System Assessment** – This option is designed for systems serving less than 10,000 people. It is based on six cybersecurity practice categories and 28 controls that are typically the most applicable to small systems and provide immediate risk reduction value.
- **Option 2: AWWA Assessment** – This is described in the Cybersecurity Tool User Guidance section, below. This option directly aligns with the controls in the NIST CSF and other relevant controls.

- **Option 3: CSET® Integration** – For systems that would like an option that provides an even more in-depth cyber vulnerability assessment, the completed AWWA Assessment Tool Excel file may be uploaded to CSET®.[16] CSET® is maintained by the Department of Homeland Security (DHS). AWWA and DHS collaborated on a process that allows users to upload the completed Excel spreadsheet to reduce duplication of data entry and provide access to additional features, such as constructing network diagrams, and continuing to evolve the user's cybersecurity assessment efforts. Once uploaded, CSET® will populate the relevant and comparable controls. The user will then have additional controls to evaluate for implementation status.

Option #1 – AWWA Small System Assessment

AWWA developed the Small System Assessment approach as a supplement to the larger AWWA Assessment approach. This approach is intended to support small systems serving a population less than 10,000 people improve their cybersecurity practices. This may also be used for systems who serve more than 10,000 people and are quickly maturing their cybersecurity practices. However, a system like that should consider maturing into the AWWA Assessment approach as soon as possible to ensure due diligence and risk management of the system.

There are six cybersecurity practices categories that provide baseline controls as a starting point for any system working to improve cybersecurity practices. These six cybersecurity practice categories are where small systems should focus efforts for mitigating cyber risks to their system. The relative importance of these baseline controls is based on the professional experience of subject matter experts supporting water systems with cybersecurity, and are informed by the Center for Internet Security's (CIS) Top 18 Controls and Resources[17]. For small systems the 14 practice categories provided in the AWWA Guidance document are reduced to the following six:

1. Training Staff to be Cybersecurity Aware
2. Knowing What Hardware and Software are Connected to and Operating on Your Networks
3. Protecting Systems from Unauthorized Access or Use

---

[16] Cyber Security Evaluation Tool (CSET). https://www.cisa.gov/resources-tools/services/cyber-security-evaluation-tool-cset. Last Accessed: December 11, 2024.

[17] The 18 CIS Critical Security Controls & Resources. https://www.cisecurity.org/controls/cis-controls-list/.

4. Maintaining Data Security Compliance
5. Physical Security
6. Good Network Design

Within the Assessment Tool, when the user selects this option, they are provided with an Excel workbook prepopulated with 28 small system baseline controls. A table of the baseline controls is included in Appendix K. Examples of implementation for each small system controls and resources to support implementation are in Appendix L. Once a system completes implementation of the 28 small system baseline controls, it is recommended that they progress to completing the Option 2 - AWWA Assessment to continue building their cyber defenses.

Option #2 – AWWA Assessment

The AWWA Assessment option guides a user thru 22 yes/no questions that characterize how the system has deployed technology to support operations. These inputs guide identification and prioritization of up to 100 recommended cybersecurity controls. These questions are included in Appendix J. Each question has corresponding details to support the systems determination of how technology is used, including examples of common applications in water systems.

Once the user answers the 22 yes/no questions, an Excel workbook can be generated. Detailed information about this is provided in the *Phase 2 AWWA Assessment Tool Output* section, below.

Option #3 – CSET® Assessment

AWWA collaborated with the Department of Homeland Security (DHS) and INL to integrate the AWWA Tool output with the Cyber Security Evaluation Tool (CSET®). This integration allows a user to seamlessly move into a more intricate cybersecurity assessment methodology.

The user must have used the AWWA Assessment approach and populated the control status field. Once that is complete, the user uploads the AWWA Assessment Excel sheet into the CSET® software application. Instructions for uploading the Excel sheet are provided within the application. Information on CSET® may be found here: https://www.cisa.gov/resources-tools/services/cyber-security-evaluation-tool-cset.

Phase 2 AWWA Assessment Tool Output

The AWWA Small System Assessment and AWWA Assessment automatically generate an output file to help systems achieve both compliance and improve their cybersecurity posture. This file is designed to facilitate a cycle of improvement through an easily repeatable and documentable process. These outputs are detailed in the following sections.

The Assessment Tool output is automatically generated as a Microsoft Excel workbook. This file is designed to support systems with compliance requirements of AWIA §2013 (SDWA §1433). In addition, the output file is formatted in a manner to support building an improvement plan. Use of this output file involves the following steps:

- *Step 1*. Select the implementation status of each recommended control from a drop-down list on the RRA-Control tab.
- *Step 2*. Review the results on the RRA-Control Status Summary tab.
- *Step 3*. On the ERP-Improvement Projects tab, select the table column headers, navigate to the Data tab at the top of the spreadsheet, and select the Filter tool in the Excel ribbon. On the Improvement Project column, click the filter icon in the cell and select "Partially Implemented" and "Planned and Not Implemented." On the Priority column select "Sort Smallest to Largest." Sorting by Control Status and Priority allows the user to identify the highest priority recommended controls for implementation. Additional grouping of the recommended controls may be done by sorting of the "Improvement Projects" column.
- *Step 4*. Use the project implementation plan to design cybersecurity improvement projects.
- *Step 5*. Complete the Declaration of Due Diligence for communication with system leadership and for documenting compliance.
- *Step 6*. Print the results for inclusion with compliance documentation, communication with stakeholders, and improvement project/risk and resilience management strategy development.

There are eight numbered tabs and one troubleshooting tab in the Microsoft Excel output file, including:

Tab 1 – Start Here

This tab provides context and high-level instructions for the use of the output file. There are no user inputs to this tab or outputs from this tab.

Troubleshooting Tab

This tab provides troubleshooting guidance based on commonly asked questions AWWA has received. This tab will be updated as additional user questions are received. There are no user inputs to this tab or outputs from this tab.

Tab 2 – RRA-Control Output

This tab summarizes the recommended cybersecurity controls based on user response to the 22 questions and provides users a field to document the implementation status of each recommended control. The RRA-Control Output tab is designed to facilitate compliance with the RRA requirements included in AWIA §2013 (SDWA §1433) by supporting "…assessment of the risks to, and resilience of, its system." System staff should use the tab to document controls already in place and those that are most important to implement. Improvement project categories are preassigned for each control. The recommended controls are categorized into Priorities 1, 2, 3, and 4, with Priority 1 being the highest.

NOTE: IF DATA IS NOT VISIBLE, PRESS CTRL-ALT-Function 9 KEYS.

TO ENSURE PROPER FUNCTION OF THIS TAB AND UPLOAD FUNCTION FOR CSET, DO NOT ADD ROWS OR COLUMNS TO THIS TAB

- **User Input –** Within this tab, document each controls implementation status in the blue Control Status column. The blue control status column and supporting information provided by the Tool is shown on Figure 5. The user must select one of the following the implementation status options for each recommended control under evaluation.
    1. **Not Planned and/or Not Implemented** – Risk Accepted – The control is not currently implemented or planned for implementation. The system accepts risks associated with the control not being implemented.
    2. **Planned and Not Implemented** – The control has not been implemented. However, implementation of the control is planned.
    3. **Partially Implemented** – The control is partially implemented by internal or external resources.
    4. **Fully Implemented and Maintained** – The control is fully implemented and actively maintained by internal or external resources.
- **Tab Outputs–** The information Tab 2 is used to populate subsequent Tabs as explained in the following sections.

Control ID	Control description	Priority	Control Status	Improvement Project	Control References
AT-3	A forensic program established to ensure that evidence is collected/handled in accordance with pertinent laws in case of an incident requiring civil or criminal action.	1	Fully Implemented and Maintained	Governance and Risk Management	*NIST CSF2.0 RS.AN-03, NIST CSF2.0 RS.AN-06, NIST CSF2.0 RS.AN-07, NIST CSF2.0 RS.MA-03*
AU-1	Audit program established to ensure information systems are compliant with policies and standards and to minimize disruption of operations.	1	Fully Implemented and Maintained	Application Security	*NIST800-53r5.3.3.AU-1, NIST800-82r2.6.2.3*
AU-2	Framework of information security policies, procedures, and controls including management's initial and periodic approval established to provide governance, exercise periodic review, dissemination, and coordination of information security activities.	1	Fully Implemented and Maintained	Governance and Risk Management	*CISA CPG2023 1.B, CISA CPG2023 1.C, NIST CSF2.0 GV.OV-01, NIST CSF2.0 GV.OV-03, NIST CSF2.0 GV.PO, NIST CSF2.0 GV.PO-01, NIST CSF2.0 GV.PO-02, NIST CSF2.0 ID.IM-01, NIST CSF2.0 ID.IM-02*

Figure 5 – RRA Control Status Table (Tab 2)

Tab 3 – RRA-Control Status Summary

This tab summarizes the control status entries from Tab 2 – RRA-Control Output. The inputs/outputs for this tab include:

- **User Inputs –** No tab-specific user inputs are required.
- **Tab Outputs –** This tab provides two tables. The first summarizes the recommended controls' status by priority. This is shown in a "heat map" format to visually indicate the number of controls of various priority and their associated status, including percentage that are fully, partially or not implemented. The second table identifies the number of controls associated with each improvement project categories as identified in the guidance document. These projects account for recommended controls where the user indicated "Partially Implemented" or "Planned and Not Implemented" on the RRA-Control Output tab. This provides a snapshot that is helpful for communicating how priority controls are distributed by implementation status with leadership and other stakeholders.

An example of the information provided in the first table on this tab is included on Figure 6.

Control Status Summary:

The second table summarizes the user defined implementation status of the recommended controls from the RRA- Control Output tab. The colors provide a the recommended controls with the associated status.

	Total Controls Not Fully Implemented	Not Planned and/or Not Implemented - Risk Accepted	Controls Planned and Not Implemented	Controls Partially Implemented	Controls Fully Implemented and Maintained
Priority 1 Controls	17	0	0	17	14
Priority 2 Controls	0	0	0	0	11
Priority 3 Controls	13	0	0	13	6
Priority 4 Controls	8	0	6	2	0

% of Recommended Controls Currently "Fully Implemented and Maintained":	45	%
% Recommended Controls that are "Partially Implemented" or "Planned and not Implemented":	55	%
% Recommended Controls that are "Not Planned and/or Not Implemented - Risk Accepted":	0	%
Controls Missing Implementation Status:	0	

Figure 6 – Control Status Summary Heat Map (Tab 3)

Tab 4 – ERP-Improvement Projects

This tab is designed to facilitate compliance with the AWIA §2013 (SDWA §1433) ERP provisions. Specifically, the user may use the Excel output to identify cybersecurity improvements and risk management strategies to address the ERP provisions requiring the inclusion of "…strategies and resources to improve the resilience of the system, including the physical security and cybersecurity of the system…"

The inputs/outputs for this tab include:

- **User Input –** No tab-specific user inputs are required.
- **Tab Output –** There are two tables within this output tab. The first is the Cyber Resilience Improvement Projects table. This table identifies improvement projects and the associated number of controls. Additional rows are available for user-identified projects. These projects address all recommended controls where the user indicated "Partially Implemented" or "Planned and Not Implemented." The second table is the Control Summary. This table provides a summary of controls and levels of implementation from user input on the RRA-Control Output tab.

An example of the information provided on this tab is included on Figure 7 and Figure 8. Figure 7 shows a summary of all controls that require additional implementation while Figure 8 shows only a sample of Priority 1 controls that require additional implementation. The system should take these projects and implement the controls included within each. Implementation of the individual projects will require engagement between system staff and support contractors to develop the final implementation plan specific to that system.

Cyber Risk Management Improvement Projects

Projects by total number of controls

Project Number	Improvement Project	Number of controls project addresses
1	Governance and Risk Management Improvements	19
2	Business Continuity and Disaster Recovery Impro	2
3	Server and Workstation Hardening Improvements	1
4	Access Control Improvements Projects	14
5	Application Security Improvements Projects	2
6	Encryption Improvements Projects	3
7	Data Security Improvements Projects	0
8	Telecommunications, Network Security, and Arch	10
9	Physical Security of PCS Equipment Improvemen	2
10	Service Level Agreements (SLA) Improvements P	4
11	Operations Security (OPSEC) Improvements Proj	1
12	Cyber-Informed Engineering Improvements Proje	0
13	Education Improvements Projects	2
14	Personnel Security Improvements Projects	1

Figure 7 – Cyber Risk Management Improvement Projects Table (Tab 4)

Controls Addressed by Project

Improvement Project	Recommended Controls	Priority	Control Status	Control References
Access Control	Access control for diagnostic tools and resources and configuration ports.	1	Partially Implemented	*ISOIEC27.27001.AA.A.13 .1.1, NIST800-53.F-AC.AC-3*
Access Control	Access control for networks shared with other parties in accordance with contracts, SLAs and	1	Partially Implemented	*NIST800-53.F-AC.AC-17, NIST800-82.5.15*
Access Control	Multifactor authentication system established for critical areas.	1	Partially Implemented	*ISA62443-1-1.5.3, ISA62443-3-3.5.3, NIST800-34.3.2, NIST800-82.6.2.7*
Physical Security	Security perimeters, card controlled gates, manned booths, and procedures for entry control.	1	Partially Implemented	*DHSCAT-2.4.3, ISOIEC27.27001.AA.A.11 .1.1, NIST800-53.F-PE.PE-3*

Figure 8 – Example Priority 1 Controls Addressed by Improvement Project (Tab 4)

System staff should use this output and the Project Implementation Form on Tab 5 to create an implementation strategy for the most important controls identified by the RRA

Support Output. It is important to note that this will likely require working with additional stakeholders to document a strategy for implementation of additional controls.

Tab 5 – Project Implementation Form

This tab provides a sample project planning form. For those systems who do not have an equivalent form, it provides a template that may be helpful in capital and operational budgeting and planning. The inputs/outputs for this tab include:

- **User Input –** The blue cells shown on Figure 9 each require user input. This information is all user-defined but may be informed by the results of the assessment summarized on the prior tabs that indicate which cybersecurity controls are not fully implemented and maintained. Grouping of cybersecurity controls into individual projects will need to be done with the system staff responsible for maintaining secure operations and capital/operational planning.
- **Tab Output –** Completion of the template with the information indicated in this form will facilitate planning, resource allocation, and successful project delivery.

An example of the information provided on this tab is included on Figure 9.

	Date	4/29/2025
	Facility/System/Utility:	ACME Water Utility
Project Name		
Project No.		
Project Owner (dept./name)		
Project Description		
Priority		
# of Priority 1 Controls Addressed		
Anticipated Start Date		
Duration	# of weeks/months/years	
Additional Description	The project will…	
Impacted Stakeholders	Example: IT, Operations, Engineer, etc.	
Cost Estimate to Implement and Maintain	IMPLEMENTATION COSTS	$
	ANNUAL MAINTENANCE COSTS	$
	PROJECT USEFUL LIFE	# of years
Potential Funding Source/s	Example: Capital budget, grants, etc.	

Figure 9 – Project Implementation Form (Tab 5) Example

Tab 6 – Declaration of Due Diligence

This tab is intended to facilitate communication with system decision makers and support long-term cybersecurity risk management. The inputs/outputs for this tab include:

- **User Input –** No tab-specific user inputs are required.
- **Tab Output –** An example of the information provided on this tab is included on Figure 10. This tab may support periodic communication that is part of a sustainable cybersecurity risk management program.

Declaration of Due Diligence Template:

Recently, used the AWWA Cybersecurity Tool to assess our current cybersecurity practices. Based on the findings of the assessment, we have 45% of the recommended controls currently 'fully implemented and maintained.' At the same time, we have 55% recommended controls that are either 'partially implemented' or 'planned and not implemented.'

As noted in the Cybersecurity Risk and Responsibility in the Water Sector :
"Government intelligence confirms the water and wastewater sector is under a direct threat as part of a foreign government's multi-stage intrusion campaign, and individual criminal actors and groups threaten the security of our nation's water and wastewater systems' operations and data."

Therefore, our department/group/division strongly recommends implementation of the highest priority controls recommended by the AWWA Tool with a current status of "Partially Implemented" or "Planned and Not Implemented."

We recommend that the following steps be taken to improve our cybersecurity risk management:
1. Develop well-defined projects for implementation.
2. Fund the projects.
3. Procure equipment and/or contractors, as needed, to support implementation of the projects.
4. Implement the projects and maintain the new controls.
5. Revisit the AWWA Cybersecurity Tool on a regular basis to document our progress relative to the industry standard.

The attached output from the AWWA Cybersecurity Tool provides a list of recommended controls for implementation. In addition, projects were developed to provide additional cyber risk mitigation.

Control Status Summary:

	Total Controls not Fully Implemented	Not Planned and/or Not Implemented - Risk Accepted	Controls Planned and Not Implemented	Controls Partially Implemented	Controls Fully Implemented and Maintained
Priority 1 Controls	17	0	0	17	14
Priority 2 Controls	0	0	0	0	11
Priority 3 Controls	13	0	0	13	6
Priority 4 Controls	8	0	6	2	0

% of Recommended Controls Currently "Fully Implemented and Maintained":	45	%
Recommended Controls that are "Partially Implemented" or "Planned and not Implemented":	55	%
% Recommended Controls that are "Not Planned and/or Not Implemented - Risk Accepted":	0	%
Controls Missing Implementation Status:	0	

Figure 10 – Declaration of Due Diligence (Tab 6) Example

Tab 7 – User Answer Summary

This tab provides a summary user response to the questions associated with each Assessment Tool option. This is provided for the system's reference during future assessments. The inputs/outputs for this tab include:

- **User Input –** No tab-specific user inputs are required.
- **Tab Output –** A summary of the 22 questions within the AWWA Assessment or the 7 questions in the small system assessment.

An example of the information provided on this tab is included on Figure 11.

AWWA Tool Questions	Answer
Are any data transferred to or from your PCS network, by any electronic means?	Yes
Do users manually transfer any electronic data to or from your PCS environment?	Yes
Are any electronic data transferred to or from your PCS environment using an automated process, without user interaction?	Yes
Are any users allowed to access your PCS environment remotely?	No
Is remote access to your PCS network allowed via mobile devices?	No
Is remote access to your PCS allowed at physically secured fixed location(s)?	No
Do you use resources outside your organization to support and/or maintain your PCS environment?	Yes
Do resources (e.g. service providers) outside your organization provide PCS support via remote access?	Yes
Do internal staff provide support for your PCS via remote access?	No
Are all changes or updates made to your PCS environment first tested in a development, testbed, non-production, and/or training environment prior to being deployed and implemented in the field/production environment?	Yes
Does your PCS include 3rd party network communication services?	No
Does your PCS network use licensed or unlicensed wireless radios between	Yes
Does your PCS share a LAN or WAN with non-PCS equipment?	Yes
Do you use Wi-Fi within the PCS environment to transfer data in support of operations or monitoring?	No
Do you use virtualization technology for your PCS?	Yes
Is the virtualization technology dedicated to PCS only?	Yes
Does your organization accept, process, store or transmit credit card or debit card information, or accept payment with pre-paid cards branded with American Express, Discover, JCB, MasterCard or Visa International logos?	Yes
Does your organization own, license, acquire or maintain any personally identifiable information (PII)?	Yes
Is your organization an employer that creates or receives health information that is HIPAA protected?	Yes
Is your organization responsible for the engineering design and implementation of critical infrastructure?	Yes
Does your organization have a supply chain risk management program?	Yes
Does your organization have a supply chain risk management program that specifically addresses cybersecurity?	Yes

Figure 11 – User Answer Summary (Tab 7) Example

Tab 8 – EPA Cyber Practice Mapping

This tab is designed to support systems with both cybersecurity risk management and preparation for enforcement inspections by the EPA or another jurisdictional authority that may be using the EPA's Priority Cybersecurity Practices checklist. Modeled after the cybersecurity portion of the EPA's Guidance on Risk and Resilience Assessments for Small Community Drinking Water Systems, this tab provides a mapping of both Phase 1 cybersecurity practices and Phase 2 cybersecurity controls that a system may use to support §1433 enforcement inspections.

- **User Input –** Since the Excel output file does not have macros for security reasons, the user manually enters the previously identified statuses into the tab from both Phase 1 and Phase 2. In addition, a column is provided to answer the EPA's questions with Yes, No, In Progress, or Not Applicable.
- **Tab Output –** Documentation of how the AWWA Assessment controls map to the EPA Priority Cybersecurity Practices and their assigned implementation statuses.

An example of the information provided on this tab is included on Figure 12.

#	EPA Priority Cybersecurity Practice	Phase 1 Cybersecurity Practice Mapping		Phase 2 Cybersecurity Control Mapping		Answer for the EPA
Reduce Exposure to Public-Facing Internet						
1	Ensure assets connected to the public Internet expose no unnecessary exploitable services (e.g., remote desktop protocol) and eliminates connections between OT assets and the Internet?	1. Does the system have public internet facing devices?	Yes	SC-15 - Logically separated control network. Minimal or single access points between corporate and control network. Stateful firewall between corporate and control networks filtering on	Fully Implemented and Maintained	Yes
		1.1. Does the system currently conduct vulnerability scanning of public internet facing devices?	Yes	SC-10 - Program for hardening servers workstations routers, and other systems using levels of hardening based on criticality established. Program should include policies and procedures for whitelisting (deny-all, allow by exception).	Fully Implemented and Maintained	

Figure 12 – EPA Cyber Practice Mapping (Tab 8) Example

Develop and Implement a Cybersecurity Risk Management Plan

Once a cybersecurity assessment is complete, the system should proceed in developing a Cybersecurity Risk Management Plan (CRMP). A CRMP establishes the cybersecurity goals and an associated plan to achieve those goals for the system to improve cybersecurity practices and be responsive to an evolving threat environment. To support systems with the development of a CRMP, a template is included as Appendix C. In addition, a Microsoft Word version of the template is available at https://www.awwa.org/cybersecurity. The template includes the following sections:

1. **Introduction –** This section defines the purpose and scope of the CRMP.
2. **Cybersecurity Team –** This section defines who is on the cybersecurity team and their roles and responsibilities.

3. **Risk Assessment, Monitoring, and Reporting –** This section defines how the system is periodically reassessing vulnerabilities, threats, and cyber-risk.
4. **Employee Training and Awareness –** This section defines the general and role-specific cybersecurity training for system staff and contractors.
5. **Third-Party Risk Management –** This section defines how the system manages third-party cyber-risk through such things as contractual requirements.
6. **Incident Response Plan –** This section identifies resources and plans for the utility to use in cyber-incident response.
7. **Business Continuity and Disaster Recovery –** This section identifies resources, plans, and capabilities to ensure business and operational continuity.
8. **Plan Maintenance and Review –** This section describes the maintenance of the CRMP.

Questions and example answers are provided within each section of the CRMP to help the system populate the CRMP sections.

Systems should download the CRMP template to support their cybersecurity risk management planning effort. The CRMP is adaptable to meet the needs of the system regardless of its maturity. The goal is to provide a repeatable process that a system can follow to support cyber-risk management and compliance.

Phase 3 – Cybersecurity Risk Management Plan Implementation

Once a system has completed Phase 1 and Phase 2, they should move on to Phase 3. In this phase, they should implement the Cybersecurity Risk Management Plan developed in Phase 2.

It is critical for a system to ensure successful implementation of the organizational and cultural practices presented in Phase 1. These practices provide the foundation for successful implementation of the Cybersecurity Risk Management Plan. Those practices include:

- Does the system leadership team (board, council, etc.) address cybersecurity at least once, annually?
- Does the system budget for cybersecurity improvements?
- Does the system have a defined risk management leader?
- Does the system provide cybersecurity training to all employees?

As the Cybersecurity Risk and Responsibility in the Water Sector[18] emphasizes:

> *"A robust approach to cybersecurity will help prevent cyber incidents, enable a far better response to incidents that do happen, and provide a far better explanation of preparedness and response when confronted by customers, constituents, investors, boards, regulators, civil litigants, legislators, and the media."*

Implementation of the cybersecurity practices and controls through the use of AWWA resources helps systems become adaptable and resilient to an evolving cyber-threat environment.

[18] Cybersecurity Risk and Responsibility in the Water Sector. https://www.awwa.org/wp-content/uploads/AWWA-Cybersecurity-Risk-and-Responsibility.pdf.

Reference Standards

To provide the user with more detailed information on the steps necessary to implement the recommended cybersecurity controls, primary references include AWWA and NIST with other less-referenced standards as needed. Table 3 provides a list of the referenced standards. Generally, AWWA endeavored to provide publicly available reference standards.

Table 2 – List of Reference Standards and Guidance

Standard/Resource	Name	Version/Revision Date
AWWA G430-24	Security Practices for Operation and Management	2024
AWWA G440-22	Emergency Preparedness Practices	2022
AWWA J100-21	Risk and Resilience Management of Water and Wastewater Systems	2021
AWWA Manual M19	Emergency Planning for Water and Wastewater Utilities, Fifth Edition	2018
CISA CPGs	Cyber Performance Goals	March 2023
Cyber-Informed Engineering	Cyber-Informed Engineering Implementation Guide	September 2023
EPA's Priority Cybersecurity Practices	Guidance on Risk and Resilience Assessments for Small Community Drinking Water Systems	July 2024
HIPAA	45 Code of Federal Regulations (CFR) Part 160 and Part 164	August 2003
ISOIEC27.27001:2022	ISO/IEC 27001:2022 Control Mapping	2022
NIST Cybersecurity Framework	Cybersecurity Framework v2.0	February 2024
NIST 800-53r5	Security and Privacy Controls for Information Systems and Organizations	September 2020
NIST 800-82r2	Guide to Operational Technology (OT) Security	September 2023
PCI-DSS v4.0.1	Payment Card Industry – Data Security Standard	June 2024

Appendix A: Safe Drinking Water Act §1433 Risk and Resilience Assessment and Emergency Response Plan Provisions[1]

[1] 42 U.S. Code § 300i-2 - Community water system risk and resilience https://www.law.cornell.edu/uscode/text/42/300i-2. Last Accessed: May 8, 2025.

SEC. 2013. COMMUNITY WATER SYSTEM RISK AND RESILIENCE.

(a) Risk and Resilience Assessments.-

(1) In general.-- Each community water system serving a population of greater than 3,300 persons shall conduct an assessment of the risks to, and resilience of, its system. Such an assessment—

(A) shall include an assessment of—

(i) the risk to the system from malevolent acts and natural hazards;

(ii) the resilience of the pipes and constructed conveyances, physical barriers, source water, water collection and intake, pretreatment, treatment, storage and distribution facilities, electronic, computer, or other automated systems (including the security of such systems) which are utilized by the system;

(iii) the monitoring practices of the system;

(iv) the financial infrastructure of the system;

(v) the use, storage, or handling of various chemicals by the system; and

(vi) the operation and maintenance of the system; and

(B) may include an evaluation of capital and operational needs for risk and resilience management or the system.

(2) Baseline information.--The Administrator, not later than August 1, 2019, after consultation with appropriate departments and agencies of the Federal Government and with State and local governments, shall provide baseline information on malevolent acts of relevance to community water systems, which shall include consideration of acts that may--

(A) substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water; or

(B) otherwise present significant public health or economic concerns to the community served by the system.

(3) Certification.—

(A) Certification.--Each community water system described in paragraph (1) shall submit to the Administrator a certification that the system has conducted an assessment complying with paragraph (1). Such certification shall be made prior to—

(i) March 31, 2020, in the case of systems serving a population of 100,000 or more;

(ii) December 31, 2020, in the case of systems serving a population of 50,000 or more but less than 100,000; and

(iii) June 30, 2021, in the case of systems serving a population greater than 3,300 but less than 50,000.

(B) Review and revision.--Each community water system described in paragraph (1) shall review the assessment of such system conducted under such paragraph at least once every 5 years after the applicable deadline for submission of its certification under subparagraph (A) to determine whether such assessment should be revised. Upon completion of such a review, the community water system shall submit to the Administrator a certification that the system has reviewed its assessment and, if applicable, revised such assessment.

(4) Contents of certifications.--A certification required under paragraph (3) shall contain only--

(A) information that identifies the community water system submitting the certification;

(B) the date of the certification; and

(C) a statement that the community water system has conducted, reviewed, or revised the assessment, as applicable.

(5) Provision to other entities.--No community water system shall be required under State or local law to provide an assessment described in this section (or revision thereof) to any State, regional, or local governmental entity solely by reason of the requirement set forth in paragraph (3) that the system submit a certification to the Administrator.

(b) Emergency Response Plan.--Each community water system serving a population greater than 3,300 shall prepare or revise, where necessary, an emergency response plan that incorporates findings of the assessment conducted under subsection (a) for such system (and any revisions thereto). Each community water system shall certify to the Administrator, as soon as reasonably possible after the date of enactment of America's Water Infrastructure Act of 2018, but not later than 6 months after completion of the assessment under subsection (a), that the system has completed such plan. The emergency response plan shall include—

(1) strategies and resources to improve the resilience of the system, including the physical security and cybersecurity of the system;

(2) plans and procedures that can be implemented, and identification of equipment that can be utilized, in the event of a malevolent act or natural hazard that threatens the ability of the community water system to deliver safe drinking water;

(3) actions, procedures, and equipment which can obviate or significantly lessen the impact of a malevolent act or natural hazard on the public health and the safety and supply of drinking water provided to communities and individuals, including the development of alternative source water options, relocation of water intakes, and construction of flood protection barriers; and

(4) strategies that can be used to aid in the detection of malevolent acts or natural hazards that threaten the security or resilience of the system.

(c) Coordination.--Community water systems shall, to the extent possible, coordinate with existing local emergency planning committees established pursuant to the Emergency Planning and Community Right-To-Know Act of 1986 (42 U.S.C. 11001 et seq.) when preparing or revising an assessment or emergency response plan under this section.

(d) Record Maintenance.--Each community water system shall maintain a copy of the assessment conducted under subsection (a) and the emergency response plan prepared under subsection (b) (including any revised assessment or plan) for 5 years after the date on which a certification of such assessment or plan is submitted to the Administrator under this section.

(e) Guidance to Small Public Water Systems.--The Administrator shall provide guidance and technical assistance to community water systems serving a population of less than 3,300 persons on how to conduct resilience assessments, prepare emergency response plans, and address threats from malevolent acts and natural hazards that threaten to disrupt the provision of safe drinking water or significantly affect the public health or significantly affect the safety or supply of drinking water provided to communities and individual.

(f) Alternative Preparedness and Operational Resilience Programs.—

(1) Satisfaction of requirement.--A community water system that is required to comply with the requirements of subsections (a) and (b) may satisfy such requirements by—

(A) using and complying with technical standards that the Administrator has recognized under paragraph (2); and

(B) submitting to the Administrator a certification that the community water system is complying with subparagraph (A).

(2) Authority to recognize.--Consistent with section 12(d) of the National Technology Transfer and Advancement Act of 1995, the Administrator shall recognize technical standards that are developed or adopted by third-party organizations or voluntary consensus standards bodies that carry out the objectives or activities required by this section as a means of satisfying the requirements under subsection (a) or (b).

(g) Technical Assistance and Grants.—

(1) In general.--The Administrator shall establish and implement a program, to be known as the Drinking Water Infrastructure Risk and Resilience Program, under which the Administrator may award grants in each of fiscal years 2020 and 2021 to owners or operators of community water systems for the purpose of increasing the resilience of such community water systems.

(2) Use of funds.--As a condition on receipt of a grant under this section, an owner or operator of a community water system shall agree to use the grant

funds exclusively to assist in the planning, design, construction, or implementation of a program or project consistent with an emergency response plan prepared pursuant to subsection (b), which may include—

(A) the purchase and installation of equipment for detection of drinking water contaminants or malevolent acts;

(B) the purchase and installation of fencing, gating, lighting, or security cameras;

(C) the tamper-proofing of manhole covers, fire hydrants, and valve boxes;

(D) the purchase and installation of improved treatment technologies and equipment to improve the resilience of the system;

(E) improvements to electronic, computer, financial, or other automated systems and remote systems;

(F) participation in training programs, and the purchase of training manuals and guidance materials, relating to security and resilience;

(G) improvements in the use, storage, or handling of chemicals by the community water system;

(H) security screening of employees or contractor support services;

(I) equipment necessary to support emergency power or water supply, including standby and mobile sources; and

(J) the development of alternative source water options, relocation of water intakes, and construction of flood protection barriers.

(3) Exclusions.--A grant under this subsection may not be used for personnel costs, or for monitoring, operation, or maintenance of facilities, equipment, or systems.

(4) Technical assistance.--For each fiscal year, the Administrator may use not more than $5,000,000 from the funds made available to carry out this subsection to provide technical assistance to community water systems to assist in responding to and alleviating a vulnerability that would substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water (including sources of water for such systems) which the Administrator determines to present an immediate and urgent need.

(5) Grants for small systems.--For each fiscal year, the Administrator may use not more than $10,000,000 from the funds made available to carry out this subsection to make grants to community water systems serving a population of less than 3,300 persons, or nonprofit organizations receiving assistance under section 1442(e), for activities and projects undertaken in accordance with the guidance provided to such systems under subsection (e) of this section.

(6) Authorization of appropriations.--To carry out this subsection, there are authorized to be appropriated $25,000,000 for each of fiscal years 2020 and 2021.

(h) Definitions.--In this section—

(1) the term `resilience' means the ability of a community water system or an asset of a community water system to adapt to or withstand the effects of a malevolent act or natural hazard without interruption to the asset's or system's function, or if the function is interrupted, to rapidly return to a normal operating condition; and

(2) the term `natural hazard' means a natural event that threatens the functioning of a community water system, including an earthquake, tornado, flood, hurricane, wildfire, and hydrologic changes.''.

(b) Sensitive Information.—

(1) Protection from disclosure.--Information submitted to the Administrator of the Environmental Protection Agency pursuant to section 1433 of the Safe Drinking Water Act, as in effect on the day before the date of enactment of America's Water Infrastructure Act of 2018, shall be protected from disclosure in accordance with the provisions of such section as in effect on such day.

(2) Disposal.--The Administrator, in partnership with community water systems (as defined in section 1401 of the Safe Drinking Water Act), shall develop a strategy to, in a timeframe determined appropriate by the Administrator, securely and permanently dispose of, or return to the applicable community water system, any information described in paragraph (1).

Appendix B: Getting Started Guide Template

AWWA Cybersecurity Risk Management Getting Started Guide Version 1.0

Tool and Guidance Revision History		
Version	Date	Description
1.0	5/12/2025	Initial Release

Cover Photo Source: Naval Sea Systems Command
(https://www.navsea.navy.mil/Media/Images/igphoto/2001963531/)

Disclaimer

The authors, contributors, editors, and publisher do not assume responsibility for the validity of the content or any consequences of its use. In no event will AWWA be liable for direct, indirect, special, incidental or consequential damages arising out of the use of information presented herein. In particular, AWWA will not be responsible for any costs, including, but not limited to, those incurred as a result of lost revenue.

TABLE OF CONTENTS

Background and Guidance on the Use of this Resource

The Getting Started Guide is a companion document to the AWWA Water Sector Cybersecurity Risk Management Guidance and Assessment Tool. These resources may be found at: https://www.awwa.org/cybersecurity.

As a system and/or third-party contractor uses the AWWA Tool, a subset of 11 cybersecurity practices described in this Getting Started Guide will be presented. These are part of Phase 1: Getting Started on Cybersecurity Fundamentals shown on Figure 1 – AWWA Cybersecurity Maturity Model. Within the maturity model, this Getting Started Guide was prepared to guide a system through Phase 1. The near-term goal of this document is to provide any water or wastewater system with concise, practical guidance to support implementation of the highest priority cybersecurity practices to mitigate cyber threats facing the organization. The long-term goal is to help a system progress from tactical action in Phase 1 to a sustainable and strategic Cybersecurity Risk Management Plan in Phase 3 that meets the needs of their system.

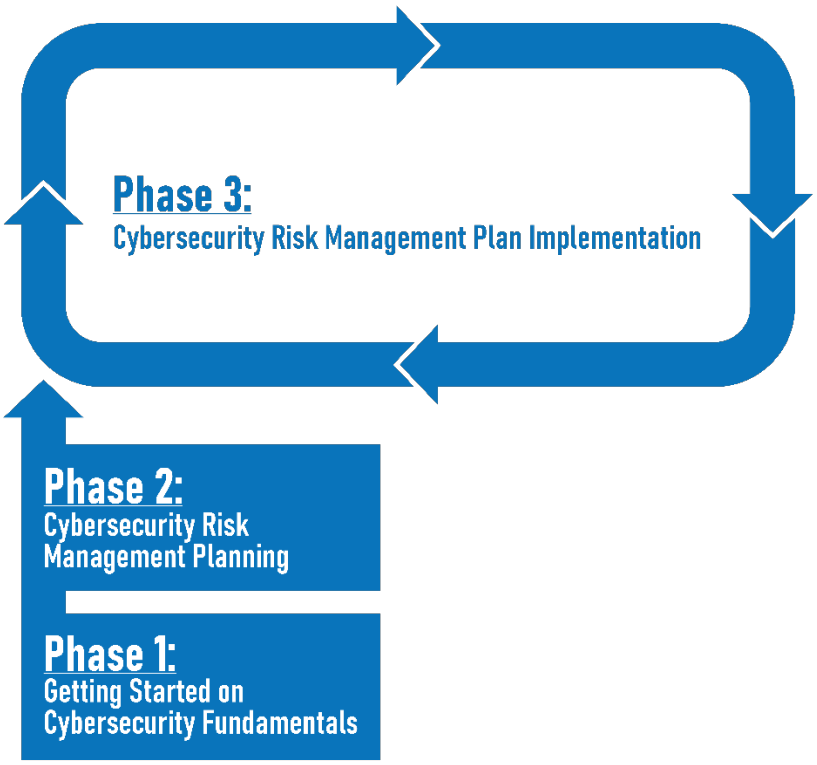


Figure 1 – Water Sector Cybersecurity Maturity Model

Document Organization

The 11 cybersecurity practices in this Getting Started Guide are applicable to both IT and OT (e.g. SCADA) environments.

The discussions of each cybersecurity practice include the following components:

- **Desired End State** – This is the goal statement for each system who has this practice implemented and maintained.
- **Key Question** – These are the questions asked within the AWWA web-based self-assessment tool.
- **What does this mean?** – This section provides a brief explanation on what the cybersecurity practice is and some of the key features that should be in place for the practice to be fully implemented and maintained.
- **How to Determine if this Practice is in Place** – This section provides context if a system needs to evaluate if and how the practice is currently in place.
- **How to Implement this Practice** – This section provides suggestions on how to implement this practice.
- **Additional Information** – This section provides additional information that may be helpful as a system sets out to implement or refine their implementation of a cybersecurity practice.

Moving to Cybersecurity Risk Management Plan Development and Implementation

Once a system has implemented the practices included in this Getting Started Guide, it should move on to Phase 2 – Cybersecurity Risk Management Planning. Phase 2 of the AWWA Cybersecurity Maturity Model begins with conducting a cybersecurity assessment using either the AWWA full assessment approach or AWWA small systems approach. Once that is complete, the system should develop a Cybersecurity Risk Management Plan for implementation in Phase 3.

Phase 3 of the AWWA Cybersecurity Maturity Model is Cybersecurity Risk Management Plan Implementation. All systems implementing and maintaining a sustainable cybersecurity risk management program tailored to their organizational needs is the ultimate end-state goal. Each of the practices listed below provides an excellent start to both the technical implementation of cybersecurity practices and the cultural and organizational practices that provide the foundation to a sustainable cybersecurity risk management program.

Phase 1 – Questions and User Answers

The following table was populated by the AWWA Tool with the standard questions and user-provided answers. Based on the user-provided answers, the AWWA Tool provides feedback on any action required by the system to successfully move through Phase 1 in to Phase 2 of the AWWA Cybersecurity Maturity Model shown on Figure 1. This table provides a summary for comparison to future assessments using the AWWA Self-Assessment Tool.

Question	User Answer	Action Required?

Based on these answers the system should prioritize any practice where an action is noted as required per the guidance below.

Cybersecurity Practice #1: Remove Non-Essential Devices from the Public Internet

Desired End State

All nonessential devices are removed from public internet connectivity. For devices that must have public internet connectivity, periodic, (e.g. monthly) vulnerability scanning of Internet connected devices/services and results are reviewed and mitigation actions are implemented.

Known unpatched vulnerabilities were the initial attack vector for 6% of IT data breaches. (IBM 2024)

Key Questions

- Does the system have public internet facing devices/surfaces?
- Does the system currently conduct vulnerability scanning of public internet facing devices?

What does this mean?

According to CISA (Cybersecurity and Infrastructure Security Agency), "public internet facing OT devices" refers to any operational technology (OT) devices that are directly accessible from the public internet, meaning anyone can potentially connect to them and potentially exploit vulnerabilities. This would include any public facing IT devices/services.

Using tools such as Nessus or CISA services that scan Internet facing devices/services for vulnerabilities that can be exploited to cause damage.

How to determine if this practice is in place:

Questions that help determine if the system is currently implementing this practice include, but are not limited to:

1. Do any OT devices have access to the Internet? Can any OT devices be accessed from the Internet? Is this connectivity required for process monitoring/control? If yes, are the OT devices protected by a firewall?
2. Does the system have any assigned public IP addresses? If yes, are they used to provide any Internet services (e.g., email, website, billing portal, etc.)? If yes, how are these services monitored for vulnerabilities?
3. Has the system signed up for CISA Cyber hygiene services?
4. Does the system have on-premise tools that regularly scan Internet facing devices/services?

How to implement this practice:

Implement this practice through the following actions:

1. Create a list of all Internet connected devices and public IP addresses assigned to the system.
2. Remove Internet access to any devices that don't absolutely require it.
3. Make sure all essential Internet connected devices are behind a firewall.
4. Sign up for CISA cyber hygiene services or purchase a solution that provides vulnerability scanning services. Perform vulnerability scanning on a regular basis and implement mitigation steps based on the findings. Information on CISA services may be found at www.cisa.gov/water.

Additional Information:

Additional information may be found at:

- CISA. Cyber Hygiene Services. https://www.cisa.gov/cyber-hygiene-services. Last Accessed: April 24, 2025.
- CISA. Stuff Off Search. https://www.cisa.gov/resources-tools/resources/stuff-search. Last Accessed: April 24, 2025.

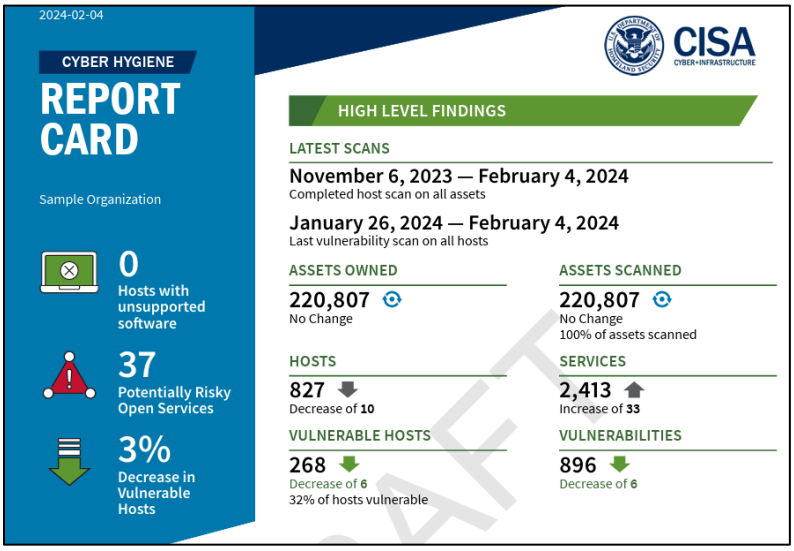


Figure 1 – Example CISA Cyber-Hygiene Report Card

Cybersecurity Practice #2: Secure Remote Access

Desired End State

All remote access to OT devices is implemented following industry best practices for using multi-factor authentication (MFA) to successfully authenticate.

Weak passwords, insecure VPNs, and inadequate access controls are common vulnerabilities that can compromise remote access security.

Key Questions

- Is remote access used by the system to access OT assets?
- Does the system enforce multi-factor authentication for remote access?

What does this mean?

System personnel can monitor and/or control operational technology outside the plant using the Internet. Contractors/integrators can monitor or make programming changes outside the plant using the Internet.

MFA is a security measure that requires multiple forms of identification to access an account for access to OT systems. It's also known as two-factor authentication (2FA) or two-step verification. Even if a password to an account is known, access is not possible without the second form of identification. The second form of identification changes the authentication code on a regular basis.

How to determine if this practice is in place:

Questions that help determine if the system is currently implementing this practice include, but are not limited to:

1. Does the system have an Industrial demilitarized zone (IDMZ) and require remote access to use a server that acts as a secure gateway for accessing and managing OT systems (i.e. jumpbox) in the IDMZ?
2. Does the system use TeamViewer, LogMeIn, etc.? If yes, is this installed on a secure gateway for accessing and managing OT systems (i.e. jumpbox) in the IDMZ?
3. Does the system know where contractors/integrators have cellular devices connected to OT equipment?
4. Are services such as Okta, Duo, Microsoft Authenticator, or a YubiKey device required to successfully authenticate the remote access solution?

How to implement this practice:

Implement this practice through the following actions:

- Remote network access should be architected following the Purdue Model Reference Architecture where all connections are terminated in an IDMZ. The IDMZ should provide a secure gateway for accessing and managing OT systems (i.e. jumpbox) or proxy service. Authentication mechanisms should be unique for IT and OT environments.
- Multi-Factor authentication (MFA) should be required for all remote access.

This will vary depending on the remote access solution so the system will need to understand which services the remote access solution is compatible with to select and implement a supported MFA solution.

Additional Information:

The Purdue Architecture Reference Model[1] is a common network architecture model used across critical infrastructure sectors. Additional information may be found at:

- National Institute of Standards and Technology (NIST) SP800-63B Section 5.1 – Authenticator and Verifier Requirements. https://pages.nist.gov/800-63-3/sp800-63b.html. Last Accessed April 24, 2025.

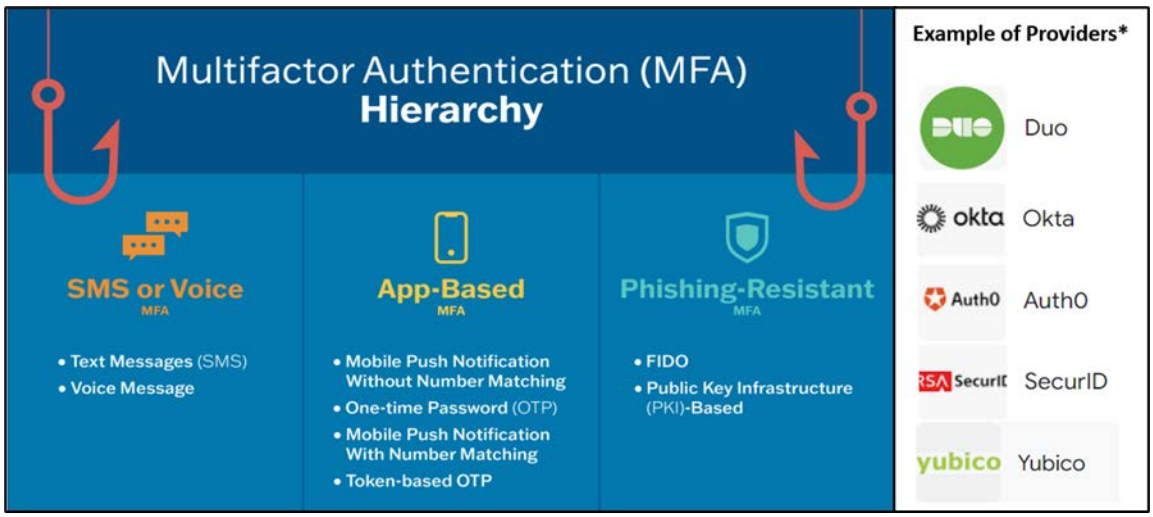


Figure 2 – MFA Hierarchy (*https://www.cisa.gov/MFA*)

[1] ANSI/ISA-62443-2-1 (99.02.01)-2009 pg. 102

Cybersecurity Practice #3: Usernames and Passwords

Desired End State

Each user has unique login credentials (username and password) for both IT and OT systems.

> Leveraging stolen credentials has been one of the common ways into an organization for the last several years. (Verizon 2025)

Key Questions:

- Does the system provide each user with a unique username and password?
- Does the system enforce password management best practices?

What does this mean?

There shouldn't be any generic user accounts (e.g., operator) and no accounts should be shared. Each approved user should have an assigned account that is for their use only. Passwords rules should follow NIST password guidelines.

How to determine if this practice is in place:

Questions that help determine if the system is currently implementing this practice include, but are not limited to:

1. Does each user have a unique account?
2. Is a central authentication service implemented that supports password rules such as, minimum length?
3. Does a policy on user account and password management exist?

How to implement this practice:

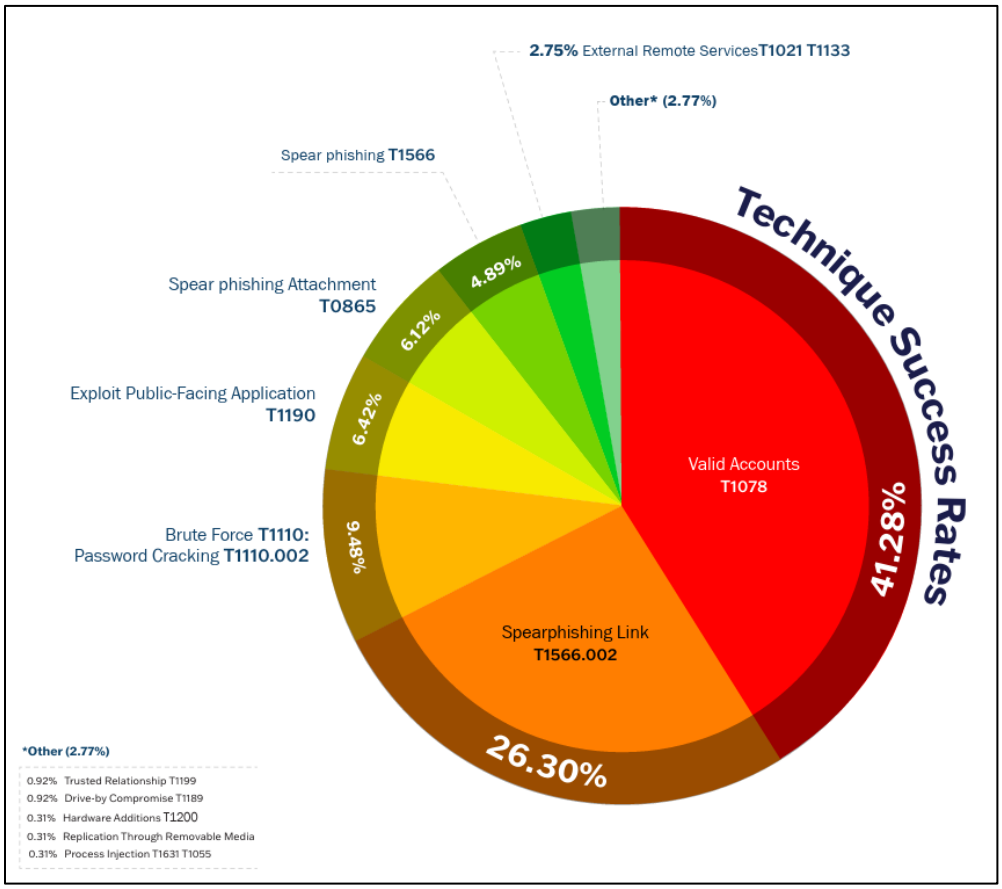
Implement this practice through the following actions:

- Implement an authentication solution such as Microsoft Active Directory to centralize user account and password management. Some applications provide authentication functionality and support password rules, so this could be implemented if a central authentication solution is not viable.

Additional Information:

Additional information may be found at:

- CISA Cyber Essentials. https://www.cisa.gov/sites/default/files/publications/Cyber%2520Essentials%2520Starter%2520Kit_03.12.2021_508_0.pdf. Last Accessed: April 24, 2025.
- NIST SP800-63-3 – Digital Identity Guidelines. https://csrc.nist.gov/pubs/sp/800/63/3/upd2/final. Last Accessed: April 24, 2025.



This graphic indicates the importance of strong usernames and passwords.

Figure 3 – CISA FY23 Risk and Vulnerability Assessment Results MITRE ATT&CK™ Tactics and Techniques

Cybersecurity Practice #4: Cyber-Incident Response Plan

Desired End State

The system has a Cyber-Incident Response Plan (CIRP) that staff are trained to exercise and implement the plan.

Key Questions

- Does the system have a Cyber-Incident Response Plan?
- Has the Cyber-Incident Response Plan been exercised?

Cyber-incident response planning is one of the top 4 greatest factors in reducing the consequences of an IT cyberattack. (IBM 2024)

Multiple utilities who experienced OT cyberattacks manually operated their systems to ensure no impact to customers. (Wisdiam 2024)

What does this mean?

The system has developed a CIRP. This document may stand alone or be incorporated into other incident response or emergency response plans. In some cases, this may be a limited initial effort. For example, if a system determines what to do in the first 15 minutes after an incident occurs to ensure service to customers is uninterrupted. Development of a strategy to operate the water system in the absence of automation is often part of this plan. In addition, staff must be trained on the plan and the plan must be exercised.

How to determine if this practice is in place:

Questions that help determine if the system is currently implementing this practice include, but are not limited to:

- Does the system have incident response plans in place for both IT and OT cyber-incidents?
- Are these plans reviewed regularly (at least annually) to ensure they are current?

How to implement this practice:

Develop a CIRP to include the following content:

- Roles and responsibilities during a cyber-incident.
- How to respond to a cyber-incident to minimize impact to operations and customers.

- How to recover from a cyber-incident to minimize the impact on staff and return systems to normal operations as soon as possible.
- After-action reporting and improvement planning guidelines to support post-incident hot-wash discussions.

Systems should also check with cyber-insurers for additional recommendations and requirements for CIRP development.

Additional Information:

Additional information may be found at:

- CISA Cyber Essentials. https://www.cisa.gov/sites/default/files/publications/Cyber%2520Essentials%2520Starter%2520Kit_03.12.2021_508_0.pdf. Last Accessed: April 24, 2025.
- JCDC Water and Wastewater Systems Sector Federal Roles and Resources for Cyber Incident Response: https://www.cisa.gov/resources-tools/resources/water-and-wastewater-systems-sector-federal-roles-and-resources-cyber-incident-response. Last Accessed: April 24, 2025.

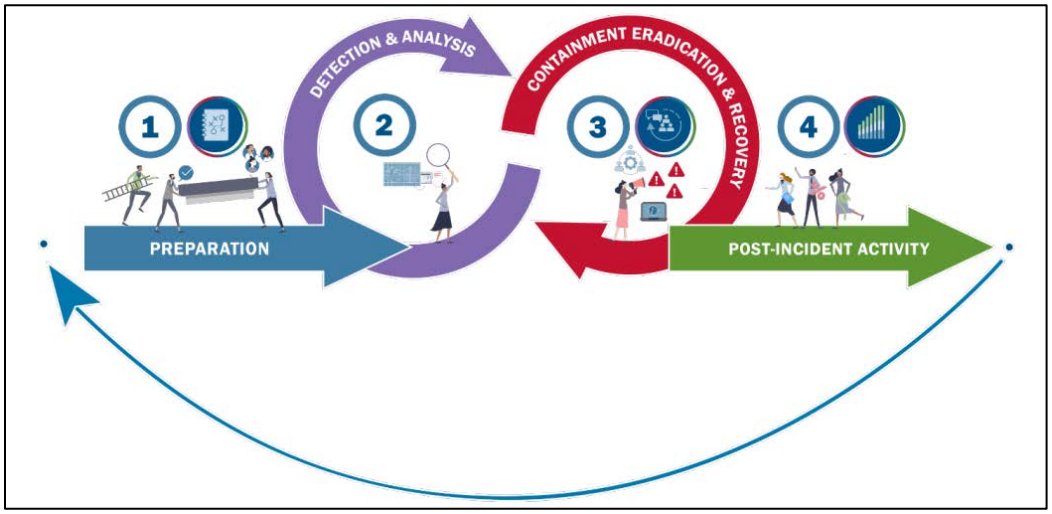


Figure 4 – The Incident and Vulnerability Response Lifecycle[2]

[2] Federal Roles and Resources for Cyber Incident Response Water and Wastewater Systems Sector. https://www.cisa.gov/sites/default/files/2024-10/WWS-Sector_Incident-Response-Guide.pdf. Accessed: April 25, 2025.

Cybersecurity Practice #5: Default Password Management

Desired End State

The system changes all default passwords on IT and OT devices.

Default passwords on IT and OT devices are a significant vulnerability exploited by malicious attackers.

Key Questions

- Have default passwords been changed on all network devices?
- Does the system have a policy requiring staff/ contractors/vendors to change default passwords when possible?

What does this mean?

The system takes proactive steps to eliminate the use of default passwords on all IT and OT devices. This includes a policy indicating that all staff/contractors/vendors must do this when deploying new equipment.

How to determine if this practice is in place:

Questions that help determine if the system is currently implementing this practice include, but are not limited to:

- Does the system have a policy in place indicating that staff and/or contractors/vendors must do this?
- Does the system conduct audits or scans of network devices to demonstrate that no default passwords are in place?
- Are system staff trained to change default passwords?
- Is documentation of non-default passwords available to qualified staff?

How to implement this practice:

Implement this practice through the following actions:

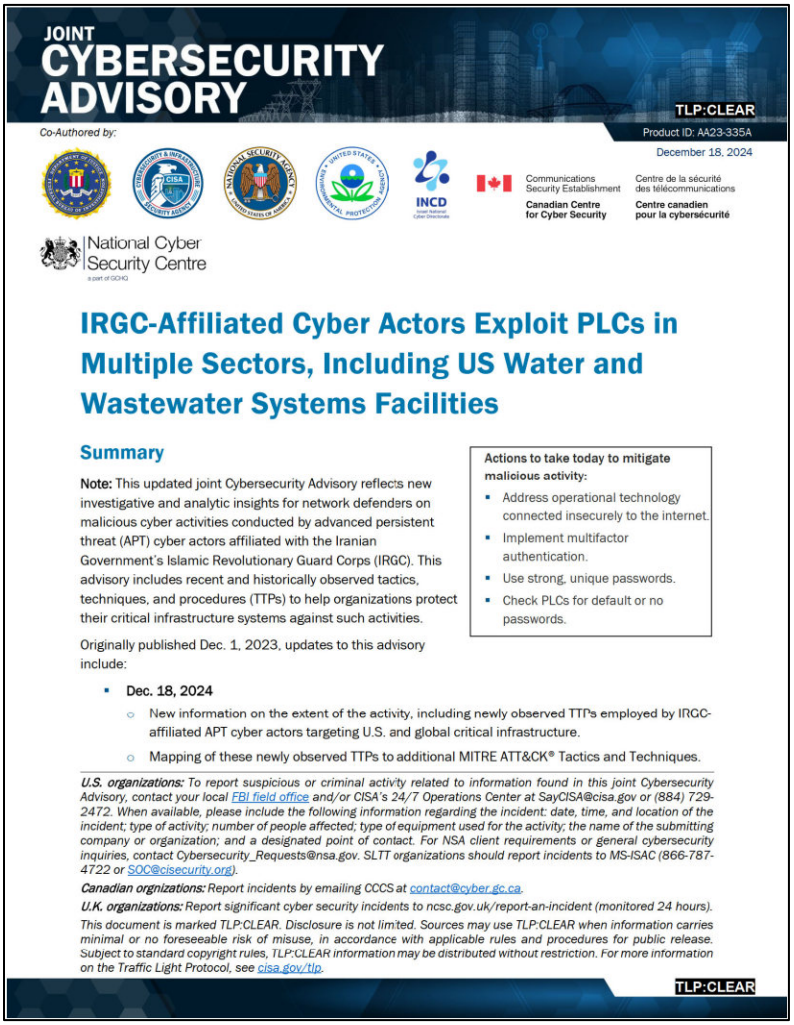
- Conduct an inventory of all IT and OT devices in the network.
- Implement a password management solution to generate, store, and manage strong, unique passwords for all devices.
- Establish a policy and procedure for changing default passwords immediately upon device installation or activation.

- Regularly scan the system's network for devices with default or weak passwords.

Additional Information:

Additional information may be found at:

- NIST SP 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final. Last Accessed: April 24, 2025.



JOINT
CYBERSECURITY
ADVISORY

TLP:CLEAR

Product ID: AA23-335A

December 18, 2024

Co-Authored by:

Communications Security Establishment
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre

IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities

Summary

Note: This updated joint Cybersecurity Advisory reflects new investigative and analytic insights for network defenders on malicious cyber activities conducted by advanced persistent threat (APT) cyber actors affiliated with the Iranian Government's Islamic Revolutionary Guard Corps (IRGC). This advisory includes recent and historically observed tactics, techniques, and procedures (TTPs) to help organizations protect their critical infrastructure systems against such activities.

Actions to take today to mitigate malicious activity:

- Address operational technology connected insecurely to the internet.
- Implement multifactor authentication.
- Use strong, unique passwords.
- Check PLCs for default or no passwords.

Originally published Dec. 1, 2023, updates to this advisory include:

- **Dec. 18, 2024**
  - New information on the extent of the activity, including newly observed TTPs employed by IRGC-affiliated APT cyber actors targeting U.S. and global critical infrastructure.
  - Mapping of these newly observed TTPs to additional MITRE ATT&CK® Tactics and Techniques.

U.S. organizations: *To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact your local FBI field office and/or CISA's 24/7 Operations Center at SayCISA@cisa.gov or (884) 729-2472. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. For NSA client requirements or general cybersecurity inquiries, contact Cybersecurity_Requests@nsa.gov. SLTT organizations should report incidents to MS-ISAC (866-787-4722 or SOC@cisecurity.org).*

Canadian orgnizations: *Report incidents by emailing CCCS at contact@cyber.gc.ca.*

U.K. organizations: *Report significant cyber security incidents to ncsc.gov.uk/report-an-incident (monitored 24 hours).*

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

TLP:CLEAR

Figure 5 **– CISA Alert AA23-335A[3]**

[3] IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities | CISA. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a. Last Accessed: April 25, 2025.

Cybersecurity Practice #6: Implement Network Monitoring

Desired End State

Network traffic is captured and monitored for malicious activity.

> Without network monitoring, a system may not know there is a problem until it is too late.

Key Questions

- Is internal network traffic via firewalls routinely monitored?
- Has another monitoring solution been implemented?

What does this mean?

The system has implemented sufficient internal network traffic monitoring to actively observe and analyze network traffic. This allows for the detection and response of cyber-incidents.

How to determine if this practice is in place:

Questions that help determine if the system is currently implementing this practice include, but are not limited to:

- Are firewalls or another monitoring solution deployed and actively logging network traffic?
- Are an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) is deployed?
- Are network traffic logs reviewed regularly?
- Do staff or third parties have defined network monitoring responsibilities?
- Are network monitoring policies and procedures are in place?

How to implement this practice:

Implement this practice through the following actions:

- Conduct a network assessment to identify the current capabilities for implementing network monitoring. Often this requires specific hardware (e.g. a managed switch) and/or specific firewall configurations.
- Implement network segmentation to facilitate more effective monitoring and containment of potential threats.

- Work with an IT or OT-specific vendor to determine the system's needs and support implementation.
- Establish policies and procedures for the use of the monitoring solution.
- Train staff or third parties on the use of the monitoring solution.

Additional Information:

Additional information may be found at:

- SANS. The Five ICS Cybersecurity Critical Controls. https://sansorg.egnyte.com/dl/R0r9qGEhEe Last Accessed: April 24, 2025.

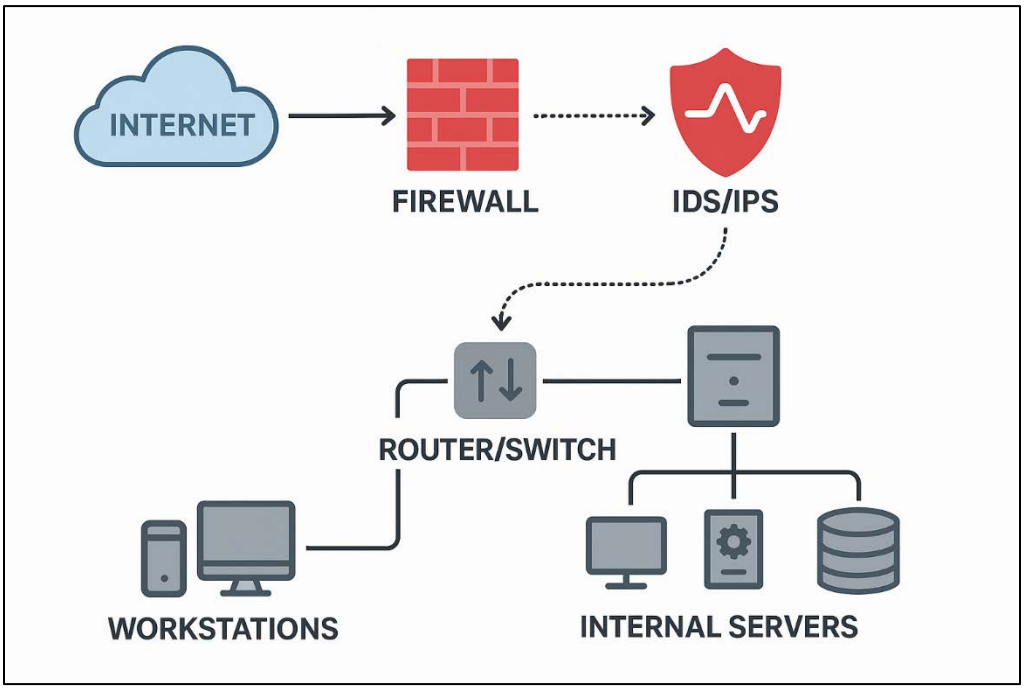


Figure 6 – Generic IDS/IPS Architecture

Cybersecurity Practice #7: Software and Program Backups

Desired End State

The system maintains backups of all critical data, software, and programs. This includes training and exercising to confirm recovery capabilities.

> 70% of organizations experienced a significant or very significant disruption to business as a result of a data breach.
> (IBM 2024)

Key Questions

- Does the system have backups of all critical data, software and programs?
- Does the system test recovery of critical data, software and programs?

What does this mean?

The system regularly backs up critical data, software and programs to ensure business continuity and rapid recovery in the case of data loss, system failures, or cyber incidents. These backups are safe from compromise (e.g. encryption by ransomware). This practice helps the system maintain service to customers, maintain compliance, prevent data loss, and maintain customer confidence.

How to determine if this practice is in place:

Questions to help determine if the system is currently implementing this practice include, but are not limited to:

- Does the system maintain an inventory of critical software and program backups including when the last backup was complete and if that backup is sufficient to meet the recovery needs of the system?
- Does the system have backups are stored in multiple locations?
- Does the system test the backups for recoverability and the associated procedures?
- Does the system review backup logs?
- Are staff trained on backup and recovery procedures?

How to implement this practice:

Implement this practice through the following actions:

- If backups of critical software and programs are missing, create new ones.

- Store them appropriately to protect them from compromise. A common strategy is the 3-2-1 backup strategy. This includes:
  - Maintain three copies of data: one primary and two backups.
  - Store the backups in two different locations.
  - Keep one backup copy offsite.
- Secure the backups to prevent compromise or damage.
- Establish backup and recovery policies and procedures. This should include a backup schedule, testing of backups, and identification of responsible staff and third parties.
- Train staff and third parties on backup and recovery procedures.

Additional Information:

Additional information may be found at:

- CISA. Cyber Essentials. https://www.cisa.gov/sites/default/files/publications/Cyber%20Essentials%20Toolkit%205%2020201015_508.pdf. Last Accessed: April 24, 2025.
- IBM. Backup and Restore. https://www.ibm.com/think/topics/backup-and-restore. Last Accessed: April 24, 2025.
- US-CERT. Data Backup Options. https://www.cisa.gov/sites/default/files/publications/data_backup_options.pdf. Last Accessed: April 24, 2025.

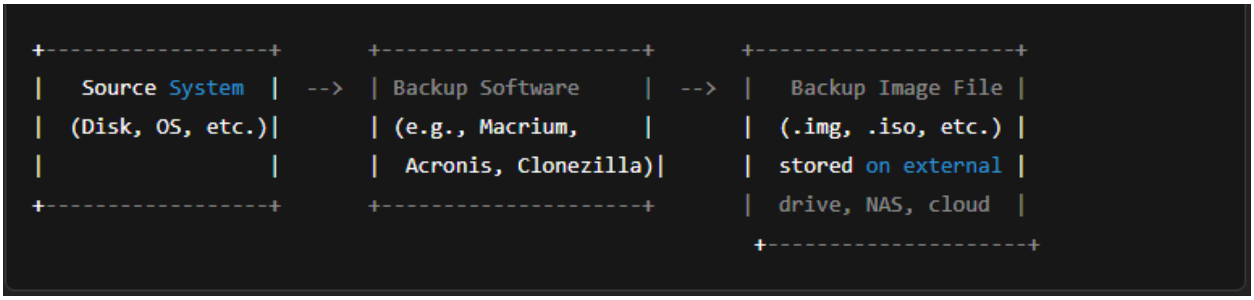


Figure 7 – Generic Backup High-Level Process

Cybersecurity Practice #8: Leadership Commitment

Desired End State

System executive leadership demonstrates a commitment to cybersecurity.

73% of systems ranked cybersecurity as Very to Critically Important in AWWA's 2025 State of the Water Industry Report. (AWWA 2025)

Key Question

- Is the system leadership team (board, council, etc.) briefed on cybersecurity risks at least once annually?

What does this mean?

Leadership's commitment is crucial for fostering a culture of cybersecurity throughout the organization. The system's executive team and governing council/board regularly and actively engage in cybersecurity discussions. This demonstrates an understanding of the importance of cybersecurity to the system and their commitment to ensuring the system is actively managing cyber-risks. This ensures that cybersecurity is treated as a risk to the whole system instead "just an IT issue".

How to determine if this practice is in place:

Questions that help determine if the system is currently implementing this practice include, but are not limited to:

- Do staff regularly provide cybersecurity briefings to the council/board?
- Is cybersecurity a recurring agenda item in board or executive meetings?
- Is cybersecurity included in strategic planning discussions?
- Does leadership actively participate in cybersecurity assessments?

How to implement this practice:

Implement this practice through the following actions:

- Schedule cybersecurity briefings for the executive team and council/board.
- Provide cybersecurity training for the executive team and council/board.
- Include cybersecurity in strategic planning discussions.
- Include leadership in cybersecurity assessments.
- Engage council/board members with cybersecurity and/or technology expertise.

Additional Information:

Additional information may be found at:

- AWWA. 2019. Cybersecurity Risk & Responsibility in the Water Sector. https://www.awwa.org/wp-content/uploads/AWWA-Cybersecurity-Risk-and-Responsibility.pdf. Last Accessed: April 24, 2025.
- CISA Corporate Cyber Governance: Owning Cyber Risk at the Board Level. https://www.cisa.gov/news-events/news/corporate-cyber-governance-owning-cyber-risk-board-level. Last Accessed: April 24, 2025.
- CISA Cyber Essentials. https://www.cisa.gov/sites/default/files/publications/Cyber%2520Essentials%2520Starter%2520Kit_03.12.2021_508_0.pdf. Last Accessed: April 24, 2025.
- NACD and ISA. Director's Handbook on Cyber-Risk Oversight. https://www.nacdonline.org/all-governance/governance-resources/governance-research/director-handbooks/nacd-directors-handbook-on-cyber-risk-oversight/
    - Last Accessed: April 24, 2025.

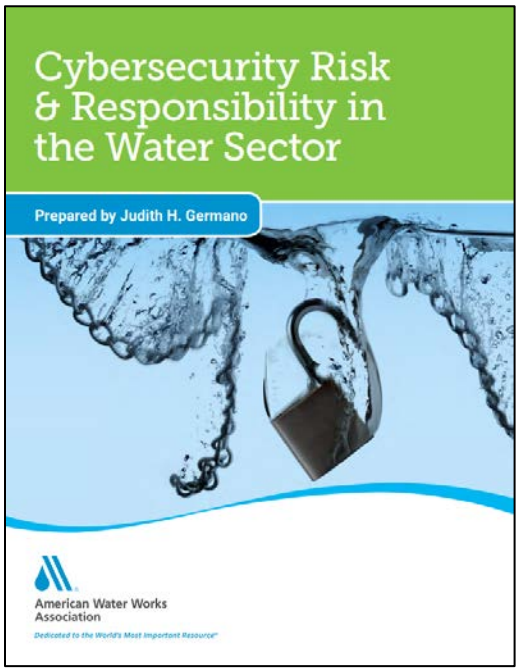


Figure 8 – AWWA's Cybersecurity Risk & Responsibility in the Water Sector[4]

[4] AWWA's Cybersecurity Risk & Responsibility in the Water Sector. https://www.awwa.org/wp-content/uploads/AWWA-Cybersecurity-Risk-and-Responsibility.pdf. Last accessed: April 25, 2025.

Cybersecurity Practice #9: Resource Allocation

Desired End State

The system consistently dedicates budget for cybersecurity improvements.

> "…It is well established that public and private entities that fail to anticipate and prepare for a diverse set of cyber threats face a very real threat of civil and regulatory liability when incidents do happen." (Germano 2019)

Key Question

- Does the system budget for cybersecurity improvements?

What does this mean?

The system recognizes the importance of securing digital systems and invests budget to improve and maintain its cybersecurity posture. This includes budgeting for technology, staff, contractors, training, and services related to cybersecurity.

How to determine if this practice is in place:

Questions that help determine if the system is currently implementing this practice include, but are not limited to:

Does the system have a multi-year plan to implement cybersecurity improvements?

Is there is a dedicated line item in the annual budget for cybersecurity improvements? These may include hardware, software, services and training for staff.

Are budget allocations are adjusted based on periodic risk assessments?

Are third-party integrators/consultants under contract and regularly supporting improvements?

How to implement this practice:

Implement this practice through the following actions:

- Develop a multi-year plan to implement cybersecurity improvements.
- Create a dedicated line item in the annual budget for cybersecurity improvements including hardware, software, services, and training for staff.
- Risk assessments inform improvements and budgeting decisions.
- Threat intelligence informs improvements and budgeting decisions.

- Apply for federal and state grants for cybersecurity improvements.

Additional Information:

Additional information may be found at:

- AWWA. 2019. Cybersecurity Risk & Responsibility in the Water Sector. https://www.awwa.org/wp-content/uploads/AWWA-Cybersecurity-Risk-and-Responsibility.pdf. Last Accessed: February 17, 2025.

Figure 9 – Budgeting and Resource Allocation

Cybersecurity Practice #10: Organizational Leadership

Desired End State

The system has a dedicated cybersecurity risk management leader who oversees and coordinates cybersecurity improvements across the system.

Key Questions

- Does the system have a defined cybersecurity risk management leader?
- Is the role of cyber risk management leader recognized in the Cyber-Incident Response Plan?

What does this mean?

The system has appointed a specific individual responsible for overseeing and coordinating cybersecurity strategies and ensuring that cybersecurity is integrated into the system's planning processes.

How to determine if this practice is in place:

Questions to determine if the system is currently implementing this practice include, but are not limited to:

- Is a designated leader part of the system's leadership structure?
- Does a staff member have this role or these responsibilities in their job description?

Many systems share IT/OT hardware, software, and personnel with separate portions of an organization (e.g. in a City). In these cases, a system staff member still needs to be responsible for the cybersecurity of the system. However, it is likely that a group will provide leadership, planning, management, and incident response across the entire enterprise. In these cases, it is critical to build the relationships and expectations to ensure appropriate security management for both IT and OT systems.

How to implement this practice:

Implement this practice through the following actions:

- Assign these responsibilities to an individual within the system.
- Establish a role within the system's leadership structure for a cybersecurity leader.

- Ensure the leader stays current on cybersecurity best practices and the current threat landscape through regular education (e.g. attending threat briefings and/or conferences).
- Establish policies governing the role and responsibilities of the system's cybersecurity leader.
- Establish a leader for development and implementation of a CIRP pre practice #1-4, above. Oftentimes this person is best positioned to provide organizational cybersecurity risk management leadership.

Additional Information:

Additional information may be found at:

- AWWA. 2019. Cybersecurity Risk & Responsibility in the Water Sector. https://www.awwa.org/wp-content/uploads/AWWA-Cybersecurity-Risk-and-Responsibility.pdf. Last Accessed: April 24, 2025.
- CISA Cyber Essentials. https://www.cisa.gov/resources-tools/resources/cyber-essentials. Last Accessed: April 24, 2025.
- CISA Cybersecurity Training and Exercises: https://www.cisa.gov/cybersecurity-training-exercises. Last Accessed: April 24, 2025.
- USEPA Cybersecurity Training: https://www.epa.gov/waterresilience/cybersecurity-training. Last Accessed: April 24, 2025.

Cybersecurity Practice #11: Training and Education

Desired End State

All system employees receive periodic cybersecurity training to protect the system against cyber threats.

Key Question

- Are system employees provided with cybersecurity training?

Employee training continues to be an essential element in cyber defense strategies, specifically for detecting and stopping phishing attacks.
(IBM 2024)

Almost 90% of cyber-attacks are caused by human error.
(Kelly 2017)

What does this mean?

The system has implemented a robust cybersecurity awareness program that educates all staff members, regardless of their role, about employees' responsibilities to maintain the system's security posture. Training also includes potential cyber threats and the associated best practices to reduce the system's exposure to these threats.

How to determine if this practice is in place:

Questions that help determine if the system is currently implementing this practice include, but are not limited to:

- Does the system currently require regular cybersecurity awareness training for employees? This may include role-based training. For example, administrators, OT staff, and operators receive training covering each of their unique day-to-day responsibilities.
- Does the system dedicate resource for staff to attend external education events (e.g. conferences or training) to understand current best practices and the threat landscape?
- Does the system conduct periodic phishing tests?

How to implement this practice:

Implement this practice through the following actions:

- Establish a cybersecurity training and education program that covers topics such as phishing techniques, password security, and incident reporting. Services such as KnowBe4®, Huntress, or those provided by CISA provide this service across multiple sectors.

- Tailor training to different roles within the system, with administrators, OT staff, and operators receiving more in-depth training on cybersecurity concepts and practices.
- Implement policies that outline cybersecurity roles, responsibilities, and expectations for all employees.

Additional Information:

Additional information may be found at:

- AWWA Cybersecurity in the Water Sector eLearning: https://www.awwa.org/cybersecurity. Last Accessed: February 18, 2025.
- CISA Cyber Essentials. https://www.cisa.gov/sites/default/files/publications/Cyber%2520Essentials%2520Starter%2520Kit_03.12.2021_508_0.pdf. Last Accessed: April 24, 2025.
- CISA Cybersecurity Training and Exercises: https://www.cisa.gov/cybersecurity-training-exercises. Last Accessed: April 24, 2025.
- USEPA Cybersecurity Training: https://www.epa.gov/waterresilience/cybersecurity-training. Last Accessed: April 24, 2025.

Numerous service providers offer cybersecurity awareness trainings. Several examples of training service providers include:

- Huntress – https://www.huntress.com/platform/security-awareness-training/episodes
- KnowBe4 – https://www.knowbe4.com/
- Proofpoint – https://www.proofpoint.com/us

Figure 11 – Common Training Platform Logos[5]

References

ANSI/ISA-62443-2-1 (99.02.01)-2009. Purdue Architecture Reference Model pg. 102

[5] Example of some service provider options, representation here is not an endorsement.

AWWA. 2025. State of the Water Industry 2025. https://www.awwa.org/state-of-the-water-industry/ Last Accessed: May 28, 2025.

IBM. 2024. Cost of a Data Breach Report 2024. https://www.ibm.com/reports/data-breach?src_trk=em679264ce3475c6.3700181715128807 25. Last accessed: April 24, 2025.

Kelly, Ross. 2019. Almost 90% of Cyber Attacks are Caused by Human Error or Behavior. https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/ Last Accessed: April 24, 2025.

Version. 2025. 2025 Data Breach Investigations Report. https://www.verizon.com/business/resources/T58b/reports/2025-dbir-data-breach-investigations-report.pdf. Last Accessed: April 28, 2025.

Wisdiam. 2024. 11 Recent Cyber Attacks on the Water and Wastewater Sector. https://wisdiam.com/publications/recent-cyber-attacks-water-wastewater/ Last accessed: April 24, 2025.

Appendix C: Cybersecurity Risk Management Plan Template

AWWA Cybersecurity Risk Management Plan Template
Version 1.0

Tool and Guidance Revision History		
Version	Date	Description
1.0	4/23/2025	Initial Release

Cover Photo Source: Naval Sea Systems Command
(https://www.navsea.navy.mil/Media/Images/igphoto/2001963531/)

TABLE OF CONTENTS

Background and Guidance on the Use of this Template

This Cybersecurity Risk Management Plan (CRMP) template is a companion document to the AWWA Water Sector Cybersecurity Risk Management Guidance and Self-Assessment Tool. These resources may be found at: https://www.awwa.org/cybersecurity.

This CRMP template was created to support systems with their IT and OT cybersecurity planning needs. The following sections are a recommendation for the structure and content that should be included in a system's CRMP. Systems using this template should tailor to their organizational needs. This may include adding sections or adapting the provided terminology to meet the needs of the system. This may require additional consultation with legal counsel to ensure that the system's CRMP properly addresses organizational risk.

Moving to Cybersecurity Risk Management Plan Development and Implementation

Once a system has implemented the practices included in the Phase 1 Getting Started Guide, the system should move on to Phase 2 – Cybersecurity Risk Management Planning. Phase 2 of the AWWA Cybersecurity Maturity Model (Figure 1) begins with conducting a cybersecurity assessment using either the full assessment approach or small systems approach. Completing Phase 1 and 2 is recommended to properly inform development of a Cybersecurity Risk Management Plan for implementation in Phase 3.

Figure 1 – Water Sector Cybersecurity Maturity Model

Key questions are provided as prompts in each section of the template for consideration while tailoring the CRMP document to the specific needs of the system. For each key question at least one example is stated to provide context. The first time a system uses the template, some of the information required to populate the CRMP may not be available. The CRMP sections are directly informed by the completed AWWA Assessment Excel output which provides a summary of the implementation status of controls within the following cybersecurity practice categories:

1. Access Control
2. Application Security
3. Business Continuity and Disaster Recovery
4. Cyber-Informed Engineering
5. Data Security
6. Cybersecurity Education
7. Encryption
8. Governance and Risk Management

9. Operations Security
10. Personnel Security
11. Physical Security
12. Server and Workstation Hardening
13. Service Level Agreements
14. Telecommunications, Network Security, and Architecture

In transitioning from Phase 2 to Phase 3 systems should consider which improvements need to be implemented in each of the practice categories noted above. Those improvements should be identified within the CRMP or related planning documents. These action items should be communicated to senior leadership to ensure they are provided with a clearly defined set of needs to effectively manage cyber-risk and budget accordingly. All systems implementing and maintaining a sustainable cybersecurity risk management program tailored to their organizational needs is the ultimate end-state goal.

The system should regularly revisit and update the CRMP as cybersecurity controls are implemented, capabilities change, and staffing changes. In addition, related documents such as the systems Emergency Response Plan or Cyber-Incident Response Plan should be aligned with and supplement the CRMP to the extent possible.

[System logo]

[System Name]

Cybersecurity Risk Management Plan [Template]

Version 1.0

Cybersecurity Risk Management Plan Sections

The CRMP should at minimum include the sections outlined below. These sections include key questions and example of answers to help a system initiate development and completion of a CRMP. Systems are encouraged to include additional sections, as needed, to address specific organizational conditions.

1. Introduction

The system should establish the purpose, scope, drivers and objectives behind their CRMP. This helps identify required changes to the document over time and establishes context for each subsequent section of the system's CRMP. The system decision-maker/s should be engaged in the development of this and subsequent sections of the CRMP to help ensure budgeting and long-term planning is successfully completed.

Key questions include:

- What is the purpose of the plan?
  - For example:
    - Establish a process for implementing and improving the cybersecurity posture of the system.
    - To support procurement of cyber-insurance.
- What is the scope of the plan? This includes the "what" and the "how" of cybersecurity risk management for the system.
  - For example:
    - Which critical functions/assets (identify critical systems, network, data, and applications)?
    - Types of threats (malware, phishing, insider, etc.)?
    - Existing vulnerabilities (gaps in controls that can be exploited)?
    - Is this for the information technology (IT) environment?
    - Is this for the operational technology (OT) environment?
- What regulatory drivers are applicable to our operations?
  - For example, AWIA §2013 or State requirements.
- What are the system 's cybersecurity objectives?
  - For example:
    - To ensure continuity of the system's critical functions during a cyber-attack.

- Smoothly and successfully respond to and recover from a cyber-attack.

Note: Timing for achieving an objective may be an important detail for some systems to manage expectations relative to budgetary and organizational considerations.

2. Cybersecurity Team

Establishing roles and responsibilities for system staff on a cybersecurity-focused team is an important step in establishing and maintaining the CRMP. Establishing a team with leaders responsible for cybersecurity helps ensure the sustainability of the system's cyber-risk management, planning, and budgeting processes.

Key questions include:

- Who is on the team?
  - For example:
    - Who is the decision maker for the system and are they present on the team?
    - Who is responsible for the different aspects of cybersecurity within the system?
    - Which contractors support the team and what are their responsibilities?
- What are the team members' roles and responsibilities?
  - For example:
    - Who is responsible for ensuring the annual cybersecurity budget is managed?
    - Who is responsible for maintaining firewall configurations?
    - Who is responsible for incident response?
- Are staff aware of who the main cybersecurity points of contact are for the system?
  - For example:
    - Is contact information shared during new staff orientation?
    - Are the main points of contact periodically shared with staff as a reminder?

3. Risk Assessment, Monitoring, and Reporting

Periodic risk assessments including monitoring of identified risks and reporting to system leadership is a key part of implementation of a CRMP. Establishing a schedule for assessment and expectations on reporting informs the system's cyber-risk management, planning, and budgeting processes.

Key questions include:

- How are cyber-risks assessed?
  - For example, using the AWWA Assessment Tool.
- How will cyber-risks be monitored?
- How will these risks be communicated to system leadership?
  - For example, how frequently and in what format will reports be provided?

4. Employee Training and Awareness

System staff are the most important line of defense against cyber-incidents. The system should consider developing or supplementing existing training to ensure that staff and contractors are sufficiently aware of the potential for and able to respond to cyber incidents.

Key questions include:

- What cybersecurity training should our staff and contractors have?
  - For example, phishing simulations to maintain awareness or cyber-attack simulations for operations staff.
  - Training should also be tailored to the organizational role and impact of the individual users. Organizational role examples include: IT User, OT User, IT Administrator (elevated privileges), OT Administrator (elevated privileges), OT Management, and Senior Management.

5. Third-Party Risk Management

Managing the risks with third parties such as contractors, integrators, vendors, and consultants can reduce cyber-risk to the system.

Key questions include:

- How do we assess vendors for cybersecurity risk?
  - For example, establishing requirements for how a third-party SCADA integrator implements and protects our SCADA system configurations and backups.
- What contractual requirements do we have to ensure our sensitive information is protected and maintained?
  - For example:
    - Requiring certain levels of cyber-insurance for service providers.
    - Terms and conditions for records retention and to ensure access to documentation.
    - Immediate notification of termination or suspension of contractors' employees that have access to system's systems and facilities.
    - Immediate notification of any security vulnerabilities within vendor-provided software or operating systems.
    - Service level agreements and contractual data privacy provisions to reduce the potential for the release of sensitive information.

6. Incident Response Plan

This section may reference a standalone Incident Response Plan. If the system decided to develop a standalone Cyber Incident Response Plan, staff should consider how to respond to and recover from a cyber incident.

Key questions include:

- How do we characterize incidents?
  - For example, scenarios a system may consider include:
    - A ransomware attack on the SCADA system.
    - An attacker making operational changes (e.g. changing chemical dosing)
    - An attacker accessing and changing PLC programs.

- Who is on the response team and what are their roles?
  - For example, internal resources who would have leadership roles in the response.
  - For example, third-parties who support our incident response operations.
- How do we capture response and recovery lessons learned?
  - For example, through an after-action reporting process and how are those archived for future reference.

7. Business Continuity and Disaster Recovery

This section may reference standalone plans such as a Business Continuity Plan (BCP) and/or Disaster Recovery Plan (DRP). If the system decided to develop BCP/DRP documents, staff should consider how they can maintain continuity of service to customers through a variety of disruptions.

Key questions include:

- What are our most critical functions and data?
  - For example, critical process, the SCADA system and customer information.
- What are our backup and recovery procedures?
  - For example, we store cold backups at a remote facility.
  - For example, our recovery procedures are available in the control room.
- How do we test and exercise our recovery capabilities?
  - For example, we conduct table-top exercises on the procedures required to ensure continuous service to our customers.
  - For example, we conduct backup restoration tests annually in a development environment.
  - For example, in the event of significant damage or destruction to facility X, personnel would reconstitute (system or operational processes) at (location) by (timeline) using (equipment).

8. Plan Maintenance and Review

The system should establish a schedule for periodic reviews and updates. This plan should inform regular planning and budgeting activities. Reviews and updates should be done annually, if not more frequent.

Key questions include:

- How do we make regular plan updates?
  - For example, through a periodic (e.g. annual) review.
- How do we ensure and document continuous improvement?
  - For example, through a periodic (e.g. annual) risk assessment project.
- How do we protect the information included in this plan from FOIA/sunshine laws or accidental release?
  - For example, citing the appropriate state statues summarized in AWWA's Protecting the Water Sector's Critical Infrastructure Information.[1]

[1] AWWA. 2020. Protecting the Water Sector's Critical Infrastructure Information. https://www.awwa.org/wp-content/uploads/Protecting-Water-Sectors-Critical-Infrastructure-Information.pdf.

Appendix D: Cybersecurity Controls

Working with water system owner/operators, subject matters experts, and federal agency partners and others, the AWWA Guidance and Assessment Tool are organized around 14 cybersecurity control practices areas. These were developed a means to simplify the process by which any water system, independent of cybersecurity expertise, could reasonably approach the issue and facilitate necessary decision making to address potential gaps.

AT: Awareness and Training		*Cybersecurity Practice Areas/Recommended Projects*
AT-1	A general security awareness and response program established to ensure staff is aware of the indications of a potential incident, security policies, and incident response/notification procedures.	Education
AT-2	Job-specific security training including incident response training for employees, contractors and third-party users.	Education; Cyber-Informed Engineering
AT-3	A forensic program established to ensure that evidence is collected/handled in accordance with pertinent laws in case of an incident requiring civil or criminal action.	Governance and Risk Management
AU: Audit and Accountability		*Cybersecurity Practice Areas/ Recommended Projects*
AU-1	Audit program established to ensure information systems are compliant with policies and standards and to minimize disruption of operations.	Application Security; Governance and Risk Management
AU-2	Framework of information security policies, procedures, and controls including management's initial and periodic approval established to provide governance, exercise periodic review, dissemination, and coordination of information security activities.	Governance and Risk Management
AU-3	Governance framework to disseminate/decentralize decision making while maintaining executive authority and strategic control and ensure that managers follow the security policies and enforce the execution of security procedures within their area of responsibility.	Governance and Risk Management
AU-4	Information security responsibilities defined and assigned.	Governance and Risk Management

AU-5	Risk based business continuity framework established under the auspices of the executive team to maintain continuity of operations and consistency of policies and plans throughout the organization. Another purpose of the framework is to ensure consistency across plans in terms of priorities, contact data, testing, and maintenance.	Business Continuity and Disaster Recovery
AU-6	Policies and procedures established to validate, test, update and audit the business continuity plan throughout the organization.	Governance and Risk Management; Business Continuity and Disaster Recovery
AU-7	Policies and procedures for system instantiation/deployment established to ensure business continuity.	Business Continuity and Disaster Recovery
AU-8	Template for the organization's confidentiality/non-disclosure agreements defined, reviewed, and approved periodically by management.	Governance and Risk Management
CM: Configuration Management		*Cybersecurity Practice Areas/ Recommended Projects*
CM-1	Policies for defining business requirements including data validation and message authenticity established to ensure that new/upgraded systems contain appropriate security requirements and controls.	Governance and Risk Management
CM-2	Procedure modification tracking program in place to manage and log changes to policies and procedures.	Governance and Risk Management
CM-3	Separation of duties implemented for user processes including risk of abuse.	Application Security; Governance and Risk Management
CM-4	Separation of duties implemented for development, production, and testing work.	Application Security; Personnel Security; Governance and Risk Management
CM-5	SLAs for all third parties established, including levels of service and change controls.	Service Level Agreement
CM-6	Risk based policies and procedures for change controls, reviews, and audits of SLAs.	Governance and Risk Management

CM-7	Monitoring of resources and capabilities with notifications and alarms established to alert management when resources/capabilities fall below a threshold.	Telecommunications, Network Security, and Architecture; SLA
A: Identification and Authentication & Access Control		*Cybersecurity Practice Areas/ Recommended Projects*
IA-1	Access control policies and procedures established including unique user ID for every user, appropriate passwords, privilege accounts, authentication, and management oversight.	Access Control; Application Security; Governance and Risk Management
IA-2	Access control for the management, monitoring, review, and audit of accounts established including access control, account roles, privilege accounts, password policies and executive oversight.	Access Control; Application Security; Governance and Risk Management
IA-3	Role based access control system established including policies and procedures.	Access Control; Application Security; Governance and Risk Management
IA-4	Access control for confidential system documentation established to prevent unauthorized access of trade secrets, program source code, documentation, and passwords (including approved policies and procedures).	Access Control; Application Security; Governance and Risk Management
IA-5	Access control for diagnostic tools and resources and configuration ports.	Access Control
IA-6	Access control for networks shared with other parties in accordance with contracts, SLAs and internal policies.	Access Control; Service Level Agreements; Governance and Risk Management
IA-7	Wireless and guest-access framework established for the management, monitoring, review, and audit of wireless and guest access in place.	Access Control; Governance and Risk Management
IA-8	Policies for security of standalone, lost, and misplaced equipment in place.	Governance and Risk Management
IA-9	Multifactor authentication system established for critical areas.	Access Control

IA-10	Policies and procedures for least privilege established to ensure that users only gain access to the authorized services.	Governance and Risk Management
IA-11	Workstation and other equipment authentication framework established to secure sensitive access from certain high-risk locations.	Access Control
IA-12	Session controls established to inactivate idle sessions, provide web content filtering, prevent access to malware sites, etc.	Access Control
IR: Incident Response, Contingency Planning, & Planning		*Cybersecurity Practice Areas/ Recommended Projects*
IR-1	Incident response program established with a formal Emergency Response Plan to restore systems and operations based on their criticality and within time constraints and effect recovery in case of a catalogue of disruptive events. Exercises conducted to test and revise plans and build organizational response capabilities.	Governance and Risk Management; Data Security
IR-2	A security program established with a formal Emergency Response Plan to respond to security incidents monitor, discover, and handle security alerts and technical vulnerabilities, collect and analyze security data, limit the organization's risk profile and ensure that management is aware of changing/emerging risks.	Governance and Risk Management; Data Security
IR-3	A legal/contractual/regulatory framework established with a formal Emergency Response Plan to track legal/contractual/regulatory requirements and the efforts to meet them with respect to each important system within the organization. Another purpose of the framework is to ensure compliance of policies and procedures with privacy laws, handling cryptographic products, intellectual property rights, and data retention requirements.	Governance and Risk Management; Data Security
MA: Maintenance		*Cybersecurity Practice Areas/ Recommended Projects*
MA-1	Equipment maintenance/replacement program established to maintain business continuity, availability, and integrity.	Service Level Agreement Governance and Risk Management; Cyber-Informed Engineering

MA-2	Maintenance of relationships with authorities, professional associations, interest groups etc., formalized. This is done, in part, to maintain an up-to-date situational awareness of relevant threats.	Governance and Risk Management
MA-3	Off-site equipment maintenance program including risk assessment of outside environmental conditions established.	Governance and Risk Management
MP: Media Protection		*Cybersecurity Practice Areas/ Recommended Projects*
MP-1	Storage media management and disposal program established to ensure that any sensitive data/software is used appropriately and is removed prior to media disposal (including approved policies and procedures).	Governance and Risk Management
MP-2	Information exit mechanisms in place to prevent data, software leaving premises without authorization or logging.	Governance and Risk Management
MP-3	Policies and procedure repository in place to be available to all authorized staff.	Governance and Risk Management
PE: Physical and Environmental Protection		*Cybersecurity Practice Areas/ Recommended Projects*
PE-1	Security perimeters, card-controlled gates, manned booths, and procedures for entry control.	Access Control; Physical Security
PE-2	Secure areas protected by entry controls and procedures to ensure that only authorized personnel have access.	Access Control; Physical Security
PE-3	Physical security and procedures for offices, rooms, and facilities.	Access Control; Governance and Risk Management; Physical Security
PE-4	Physical protection against fire, flood, earthquake, explosion, civil unrest, etc.	Access Control; Physical Security
PE-5	Physical security and procedures for working in secure areas.	Access Control; Physical Security
PE-6	Physical security and procedures for mail rooms, loading areas, etc., established. These areas must be isolated from OT and enterprise system areas.	Access Control; Physical Security

PE-7	Physical security and procedures against equipment environmental threats and hazards or unauthorized access.	Physical Security
PE-8	Physical/logical protection against power failure of equipment UPS.	Physical Security; Service Level Agreements
PE-9	Physical/logical protection against access to power and telecommunications cabling established.	Physical Security
PM: Program Management & Security Assessment and Authorization		*Cybersecurity Practice Areas/ Recommended Projects*
PM-1	Asset management program including a repository containing all significant assets of the organization with a responsible party for each, periodic inventories, and audits.	Governance and Risk Management; Cyber-Informed Engineering
PM-2	Policies and procedures for acceptable use of assets and information approved and implemented.	Governance and Risk Management;
PM-3	Centralized logging system including policies and procedures to collect, analyze and report to management.	Telecommunications, Network Security, and Architecture; Governance and Risk Management;
PM-4	SLAs for software and information exchange with internal/external parties in place including interfaces between systems and approved policies and procedures.	SLAs; Governance and Risk Management
PM-5	Data classification policies and procedures for handling and labeling based on confidentiality and criticality approved and implemented.	Governance and Risk Management
PS: Personnel Security		*Cybersecurity Practice Areas/ Recommended Projects*
PS-1	Policies and procedures for hiring/terminating processes on employees, contractors, or support companies to include background checks and contract agreements approved and implemented.	Governance and Risk Management; Personnel Security
PS-2	Defined and approved security roles and responsibilities of all employees, contractors and third-party users.	Governance and Risk Management; Personnel Security
PS-3	A clear desk policy in place including clear papers, media, desktop, and computer screens.	Governance and Risk Management; Personnel Security

PS-4	Disciplinary process for security violations established.	Governance and Risk Management; Personnel Security
RA: Risk Assessment		*Cybersecurity Practice Areas/ Recommended Projects*
RA-1	Risk assessment and approval process before granting access to the organization's information systems.	Governance and Risk Management
RA-2	Third party agreement process to ensure security on access, processing, communicating, or managing the organization's information or facilities.	Governance and Risk Management; SLAs
SA: System and Services Acquisition		*Cybersecurity Practice Areas/ Recommended Projects*
SA-1	Authorization process established for new systems or changes to existing information processing systems.	Governance and Risk Management
SA-2	Change controls of systems development, outsourced development, system modification, and testing established, including acceptance criteria for new systems, monitoring of internal/outsourced development, and control of system upgrades.	Governance and Risk Management; SLAs
SA-3	Change controls of operating systems, network configuration/topology, network security established, including changes to IDS/IPS, traffic control/monitoring, new systems, and system upgrades.	Governance and Risk Management; Server and Workstation Hardening
SA-4	Risk based mobility policies and procedures established to protect against inherent risk of mobile computing and communication systems.	Operations Security; Governance and Risk Management
SA-5	Periodic review of backup policies and procedures and testing of recovery processes.	Governance and Risk Management
SI: System and Information Integrity		*Cybersecurity Practice Areas/ Recommended Projects*
SI-1	Electronic commerce infrastructure in place providing integrity, confidentiality and non-repudiation and including adherence to pertinent laws, regulations, policies, procedures, and approval by management.	Governance and Risk Management
SI-2	System acceptance standards including data validation (input/output), message authenticity, and system integrity established to detect information corruption during processing.	Governance and Risk Management

SI-3	Interactive system for managing password implemented to ensure password strength.	Access Control; Application Security
SI-4	Organization-wide clock synchronization system in place.	Telecommunications, Network Security, and Architecture
SI-5	Privileged programs controls established to restrict usage of system programs that could reset passwords or override controls as well as enterprise system audit tools that can modify or delete audit data.	Application Security; Telecommunications, Network Security, and Architecture
DS: Data Security		*Cybersecurity Practice Areas/ Recommended Projects*
DS-1	A program established to ensure compliance with the minimum PCI requirements for your associated level.	Governance and Risk Management; Data Security
DS-2	A Privacy Policy as well as a Cyber Security Breach Policy are implemented.	Business Continuity and Disaster Recovery; Governance and Risk Management; Data Security
DS-3	A program is established to ensure compliance with the minimum HIPAA requirements. Develop a Privacy Policy as well as a Cyber Security Breach Policy.	Business Continuity and Disaster Recovery; Governance and Risk Management; Data Security
CIE: Cyber-Informed Engineering		*Cybersecurity Practice Areas/ Recommended Projects*
CIE-1	A program is in place to engage engineering staff in understanding and mitigating high-consequence and constantly evolving cyber threats throughout the engineering life-cycle including: design, implementation, maintenance, and decommissioning.	Cyber-Informed Engineering
SU: Supply Chain		*Cybersecurity Practice Areas/ Recommended Projects*
SU-1	A supply chain risk management program.	Governance and Risk Management
SU-2	A supply chain risk management program that includes cybersecurity.	Governance and Risk Management

	SC: System and Communications Protection	*Cybersecurity Practice Areas/ Recommended Projects*
SC-1	Policies and procedures governing cryptography and cryptographic protocols including key/certificate-management established to maximize protection of systems and information.	Governance and Risk Management
SC-2	Centralized authentication system or single sign-on established to authorize access from a central system.	Access Control; Application Security
SC-3	Policies and procedures established for network segmentation including implementation of DMZs based on type and sensitivity of equipment, user roles, and types of systems established.	Governance and Risk Management
SC-4	Intrusion detection, prevention, and recovery systems including approved policies and procedures established to protect against cyber-attacks. System includes repository of fault logging, analysis, and appropriate actions taken.	Governance and Risk Management; Telecommunications, Network Security, and Architecture
SC-5	Anomaly based IDS/IPS established including policies and procedures.	Telecommunications, Network Security, and Architecture
SC-6	Network management and monitoring established including deep packet inspection of traffic, QoS, port-level security, and approved policies and procedures.	Governance and Risk Management; Telecommunications, Network Security, and Architecture
SC-7	Information exchange protection program in place to protect data in-transit through any communication system including the Internet, email, and text messaging and approved policies and procedures.	Governance and Risk Management; Telecommunications, Network Security, and Architecture
SC-8	Routing controls established to provide logical separation of sensitive systems and enforce the organization's access control policy.	Operations Security; Telecommunications, Network Security, and Architecture
SC-9	Process isolation established to provide a manual override “air gap” between highly sensitive systems and regular environments.	Operations Security; Telecommunications, Network Security, and Architecture

SC-10	Program for hardening servers, workstations, routers, and other systems using levels of hardening based on criticality established. Program should include policies and procedures for whitelisting (deny-all, allow by exception).	Server and Workstation Hardening; Governance and Risk Management
SC-11	Framework for hardening of mobile code and devices established (including acceptance criteria and approved policies and procedures).	Server and Workstation Hardening; Governance and Risk Management
SC-12	Remote access framework including policies and procedures established to provide secure access to telecommuting staff, established for the management, monitoring, review, and audit of remote access to the organization.	Access Control; Governance and Risk Management
SC-13	Testing standards including test data selection, protection, and system verification established to ensure system completeness.	Governance and Risk Management
SC-14	Network segregation. Firewalls, deep packet inspection and/or application proxy gateways.	Operations Security; Telecommunications, Network Security, and Architecture
SC-15	Logically separated control network. Minimal or single access points between corporate and control network. Stateful firewall between corporate and control networks filtering on TCP and UDP ports. DMZ networks for data sharing.	Operations Security; Telecommunications, Network Security, and Architecture
SC-16	Defense-in-depth. Multiple layers of security with overlapping functionality.	Operations Security; Telecommunications, Network Security, and Architecture
SC-17	Virtual Local Area Network (VLAN) for logical network segregation.	Telecommunications, Network Security, and Architecture
SC-18	Minimize wireless network coverage.	Telecommunications, Network Security, and Architecture
SC-19	802.1X user authentication on wireless networks.	Telecommunications, Network Security, and Architecture
SC-20	Wireless equipment located on isolated network with minimal or single connection to control network.	Telecommunications, Network Security, and Architecture

SC-21	Unique wireless network identifier SSID for control network.	Telecommunications, Network Security, and Architecture
SC-22	Separate Microsoft Windows domain for wireless (if using Windows).	Telecommunications, Network Security, and Architecture
SC-23	Wireless communications links encrypted.	Encryption; Telecommunications, Network Security, and Architecture
SC-24	Communications links encrypted.	Encryption; Telecommunications, Network Security, and Architecture
SC-25	VPN using IPsec, SSL or SSH to encrypt communications from untrusted networks to the control system network.	Encryption; Telecommunications, Network Security, and Architecture

Appendix E: Cross Reference to NIST 2.0 Cybersecurity Framework

The Cybersecurity Controls in Appendix D are cross-referenced in this table with the NIST Cybersecurity Framework version 2.0 issued February 26, 2024.

Function	Category	Sub-Category	Description	Revised AWWA Guidance Control
GOVERN	Organizational Context (GV.OC)	GV.OC-01	The organizational mission is understood and informs cybersecurity risk management	IR-2
		GV.OC-02	Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	PS-2, AU-4, AU-6, SU-2
		GV.OC-03	Legal, regulatory, and contractual requirements regarding cybersecurity - including privacy and civil liberties obligations - are understood and managed	IR-3
		GV.OC-04	Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated	Not addressed
		GV.OC-05	Outcomes, capabilities, and services that the organization depends on are understood and communicated	Not addressed

Function	Category	Sub-Category	Description	Revised AWWA Guidance Control
	Risk Management Strategy (GV.RM)	GV.RM-01	Risk management objectives are established and agreed to by organizational stakeholders	IR-2
		GV.RM-02	Risk appetite and risk tolerance statements are established, communicated, and maintained	SA-4, SC-4
		GV.RM-03	Cybersecurity risk management activities and outcomes are included in enterprise risk management processes	AU-3, AU-5, CM-6
		GV.RM-04	Strategic direction that describes appropriate risk response options is established and communicated	SA-4
		GV.RM-05	Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	SU-1
		GV.RM-06	A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated	IR-2

Function	Category	Sub-Category	Description	Revised AWWA Guidance Control
		GV.RM-07	Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions	AWWA J100
	Roles, Responsibilities, and Authorities (GV.RR)	GV.RR	Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated	PS-2, AU-4, AU-6
		GV.RR-01	Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving	AU-3
		GV.RR-02	Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced	PS-2, AU-4, AU-6, PE-4

Function	Category	Sub-Category	Description	Revised AWWA Guidance Control
		GV.RR-03	Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies	IR-2
		GV.RR-04	Cybersecurity is included in human resources practices	AT-2
	Policy (GV.PO)	GV.PO	Organizational cybersecurity policy is established, communicated, and enforced	IR-2, AU-2
		GV.PO-01	Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced	IR-2, AU-2
		GV.PO-02	Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission	IR-2, AU-2
	Oversight (GV.OV)	GV.OV-01	Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction	AU-2

Function	Category	Sub-Category	Description	Revised AWWA Guidance Control
		GV.OV-02	The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks	IR-3
		GV.OV-03	Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed	AU-2
	Cybersecurity Supply Chain Risk Management (GV.SC)	GV.SC-01	A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders	SU-1
		GV.SC-02	Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally	PE-4, PS-2
		GV.SC-03	Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes	SU-2
		GV.SC-04	Suppliers are known and prioritized by criticality	SU-2

Function	Category	Sub-Category	Description	Revised AWWA Guidance Control
		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	SU-2
		GV.SC-06	Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships	SU-1
		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	SU-1, SU-2
		GV.SC-08	Relevant suppliers and other third parties are included in incident planning, response, and recovery activities	SU-1, SU-2
		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	SU-1

Function	Category	Sub-Category	Description	Revised AWWA Guidance Control
		GV.SC-10	Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement	SU-1
IDENTIFY	Asset Management (ID.AM)	ID.AM-01	Inventories of hardware managed by the organization are maintained	PM-1, PM-2
		ID.AM-02	Inventories of software, services, and systems managed by the organization are maintained	PM-1, PM-2
		ID.AM-03	Representations of the organization's authorized network communication and internal and external network data flows are maintained	PM-1, PM-2
		ID.AM-04	Inventories of services provided by suppliers are maintained	MA-3
		ID.AM-05	Assets are prioritized based on classification, criticality, resources, and impact on the mission	PM-5
		ID.AM-07	Inventories of data and corresponding metadata for designated data types are maintained	PM-1

Function	Category	Sub-Category	Description	Revised AWWA Guidance Control
		ID.AM-08	Systems, hardware, software, services, and data are managed throughout their life cycles	PM-1, CM-1, CM-6, MP-1, MA-1
	Risk Assessment (ID.RA)	ID.RA-01	Vulnerabilities in assets are identified, validated, and recorded	AU-5, RA-1, IR-2, PM-1
		ID.RA-02	Cyber threat intelligence is received from information sharing forums and sources	AU-5, PM-3, IR-2, MA-2
		ID.RA-03	Internal and external threats to the organization are identified and recorded	AU-5, RA-1, IR-2
		ID.RA-04	Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded	AU-5, RA-1, IR-2
		ID.RA-05	Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization	AU-5
		ID.RA-06	Risk responses are chosen, prioritized, planned, tracked, and communicated	IR-1, IR-2
		ID.RA-07	Changes and exceptions are managed, assessed for risk impact, recorded, and tracked	SA-3

Function	Category	Sub-Category	Description	Revised AWWA Guidance Control
		ID.RA-08	Processes for receiving, analyzing, and responding to vulnerability disclosures are established	PM-1, IR-2
		ID.RA-09	The authenticity and integrity of hardware and software are assessed prior to acquisition and use	SU-1, SU-2
		ID.RA-10	Critical suppliers are assessed prior to acquisition	SU-2, SU-1
	Improvement (ID.IM)	ID.IM	Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions	AU-6, SC-4
		ID.IM-01	Improvements are identified from evaluations	AU-2
		ID.IM-02	Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties	PS-4, AU-2, AU-4, IR-1, AWWA G430, G440
		ID.IM-03	Improvements are identified from execution of operational processes, procedures, and activities	AU-6, AU-7, SC-4, AWWA G430, G440

Function	Category	Sub-Category	Description	Revised AWWA Guidance Control
		ID.IM-04	Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved	PS-4, AWWA J100/G440/G430,M19
PROTECT	Identity Management, Authentication, and Access Control (PR.AA)	PR.AA-01	Identities and credentials for authorized users, services, and hardware are managed by the organization	IA-1, RA-1, SC-19
		PR.AA-02	Identities are proofed and bound to credentials based on the context of interactions	IA-2
		PR.AA-03	Users, services, and hardware are authenticated	IA-7, IA-9, SC-12, SC-21, RA-2, SC-2, SC-22, SI-3
		PR.AA-04	Identity assertions are protected, conveyed, and verified	SC-2
		PR.AA-05	Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	IA-1, RA-1, SC-19, IA-10, SC-12, SC-18, SC-21, RA-2, IA-3, SC-22

Function	Category	Sub-Category	Description	Revised AWWA Guidance Control
		PR.AA-06	Physical access to assets is managed, monitored, and enforced commensurate with risk	PE-1, PE-2, PE-3
	Awareness & Training (PR.AT)	PR.AT-01	Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind	AT-1, AT-2, AWWA G430, G440
		PR.AT-02	Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind	AT-1, AT-2, PS-4
	Data Security (PR.DS)	PR.DS-01	The confidentiality, integrity, and availability of data-at-rest are protected	PM-5, MP-2, MP-1, IR-3, IA-4, SI-2
		PR.DS-02	The confidentiality, integrity, and availability of data-in-transit are protected	PM-4,SC-7, SC-14, SC-23, SC-24, SI-2, IA-4
		PR.DS-10	The confidentiality, integrity, and availability of data-in-use are protected	IA-4, SI-2, PM-5
		PR.DS-11	Backups of data are created, protected, maintained, and tested	SA-5

Function	Category	Sub-Category	Description	Revised AWWA Guidance Control
	Platform Security (PR.PS)	PR.PS-01	Configuration management practices are established and applied	SA-3, SC-10, SC-19, MP-1
		PR.PS-02	Software is maintained, replaced, and removed commensurate with risk	AU-5
		PR.PS-03	Hardware is maintained, replaced, and removed commensurate with risk	PM-1, MA-1
		PR.PS-04	Log records are generated and made available for continuous monitoring	PM-3
		PR.PS-05	Installation and execution of unauthorized software are prevented	SI-5
		PR.PS-06	Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle	Not addressed
	Technology Infrastructure Resilience (PR.IR)	PR.IR-01	Networks and environments are protected from unauthorized logical access and usage	IA-7, CM-4, SC-12, SC-18, SC-21, RA-2, SI-2, SC-2, SC-8, SC-9, SC-14, SC-15, SC-16, SC-17, SC-20, SC-25
		PR.IR-02	The organization's technology assets are protected from environmental threats	PE-4
		PR.IR-03	Mechanisms are implemented to achieve resilience requirements in normal and adverse situations	Not addressed

Function	Category	Sub-Category	Description	Revised AWWA Guidance Control
		PR.IR-04	Adequate resource capacity to ensure availability is maintained	MA-1, CM-7
DETECT	Continuous Monitoring (DE.CM)	DE.CM-01	Networks and network services are monitored to find potentially adverse events	CM-7, SC-5, SA-4, PS-1
		DE.CM-02	The physical environment is monitored to find potentially adverse events	PE-1
		DE.CM-03	Personnel activity and technology usage are monitored to find potentially adverse events	CM-7, PS-1
		DE.CM-06	External service provider activities and services are monitored to find potentially adverse events	IA-2, PS-1, SU-2
		DE.CM-09	Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	CM-7, SC-5, SA-4
	Adverse Event Analysis (DE.AE)	DE.AE	Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents	SC-4, SC-6

Function	Category	Sub-Category	Description	Revised AWWA Guidance Control
		DE.AE-02	Potentially adverse events are analyzed to better understand associated activities	SC-4, SC-5
		DE.AE-03	Information is correlated from multiple sources	PM-3
		DE.AE-04	The estimated impact and scope of adverse events are understood	PM-3, SC-4
		DE.AE-06	Information on adverse events is provided to authorized staff and tools	IA-2
		DE.AE-07	Cyber threat intelligence and other contextual information are integrated into the analysis	MA-2
		DE.AE-08	Incidents are declared when adverse events meet the defined incident criteria	IR-2
RESPOND	Incident Management (RS.MA)	RS.MA-01	The incident response plan is executed in coordination with relevant third parties once an incident is declared	AT-1, AWWA G430, G440, IR-1, MA-2
		RS.MA-02	Incident reports are triaged and validated	SC-4, SC-5, AWWA J100
		RS.MA-03	Incidents are categorized and prioritized	AWWA J100, AT-3
		RS.MA-04	Incidents are escalated or elevated as needed	AWWA G430, G440, J100, IR-1, MA-2
		RS.MA-05	The criteria for initiating incident recovery are applied	IR-2

Function	Category	Sub-Category	Description	Revised AWWA Guidance Control
	Incident Analysis (RS.AN)	RS.AN-03	Analysis is performed to establish what has taken place during an incident and the root cause of the incident	AT-3
		RS.AN-06	Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved	AT-3
		RS.AN-07	Incident data and metadata are collected, and their integrity and provenance are preserved	AT-3
		RS.AN-08	An incident's magnitude is estimated and validated	AWWA J100
	Incident Response Reporting and Communication (RS.CO)	RS.CO-02	Internal and external stakeholders are notified of incidents	G430, IR-1, MA-2
		RS.CO-03	Information is shared with designated internal and external stakeholders	MA-2
		RS.MI-01	Incidents are contained	IR-1
	Incident Mitigation (RS.MI)	RS.MI-02	Incidents are eradicated	IR-1

Function	Category	Sub-Category	Description	Revised AWWA Guidance Control
RECOVER	Recovery Planning (RC.RP)	RC.RP-01	The recovery portion of the incident response plan is executed once initiated from the incident response process	AU-7
		RC.RP-02	Recovery actions are selected, scoped, prioritized, and performed	AU-7
		RC.RP-03	The integrity of backups and other restoration assets is verified before using them for restoration	SA-5
		RC.RP-04	Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms	AWWA J100, G430, G440
		RC.RP-05	The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed	IR-1, SA-5, AU-5, AU-6
		RC.RP-06	The end of incident recovery is declared based on criteria, and incident-related documentation is completed	IR-1, IR-2

Function	Category	Sub-Category	Description	Revised AWWA Guidance Control
	Incident Recovery Communications (RC.CO)	RC.CO-03	Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders	AWWA G430, G440
		RC.CO-04	Public updates on incident recovery are shared using approved methods and messaging	AWWA G430, G440

Appendix F: Cyber-Incident Response Plan Template

AWWA Cyber-Incident Response Plan Template
Version 1.0

Tool and Guidance Revision History		
Version	Date	Description
1.0	5/12/2025	Initial Release

Cover Photo Source: Naval Sea Systems Command
(https://www.navsea.navy.mil/Media/Images/igphoto/2001963531/)

TABLE OF CONTENTS

Background and Guidance on the Use of this Template

This Cyber-Incident Response Plan (CIRP) template is a companion document to the AWWA Water Sector Cybersecurity Risk Management Guidance and Assessment Tool. These resources may be found at: https://www.awwa.org/cybersecurity.

This CIRP template was developed by AWWA to provide a starting point for any water or wastewater system that does not already have one in place. This template is based on cross-sector best practices adapted for the water sector to aid systems with preparing for the inevitable reality of responding to a cyber-incident.

This CIRP template supports systems with their IT and OT cybersecurity planning needs. The following sections are a recommendation for the structure and content that should be included in a system's CIRP. Systems using this template should adapt it as they see fit. This may include adding sections or adapting the provided terminology to meet the needs of the system. In addition, a system should conduct table-top exercises with their CIRP to continually refine and adapt to the changing needs of the system. Resources for table-top exercises may be found at https://ttx.epa.gov/learn.html.

[The remainder of this document is a template with tables and text that should be updated and adapted by the system with specific information and activities staff and contractors should take during response operations.]

[System logo]

[System Name]

Cyber-Incident Response Plan [Template]

Version 1.0

Incident Response Team

A proactive cybersecurity approach includes identifying a dedicated Incident Response Team (IRT). An example table is provided, below. While smaller systems may have a single person responsible for more than one of the roles listed in the example table, it is strongly recommended that regardless of size, each of these roles be represented on the IRT.

[The system should adapt the following table.]

Position	Name	Phone Number	Alternate (Supervisor/ cell)	Role/Responsibility	Availability
General Manager	John Doe	555-789-0123	000-111-2222	Executive oversight and final decision-making	24/7
IT/OT Manager	Jane Smith	555-123-4567	--	Technical analysis and support	24/7
Operations Manager	Michael Green	555-234-5678	--	Maintain operations	24/7
Public Information Officer	Jane Doe	555-345-6789	--	Develop and make public statements on behalf of the system	24/7
Legal Counsel	Frank Black	555-456-7890	--	Advise system leadership and ensure actions are lawful	24/7
Insurer	Ann Onymous	555-567-8901	--	Provide guidance on response and recovery	24/7

While many CIRP implementations are focused on meeting customer demands, including the Public Information Officer and Legal Counsel on the response team is critical to ensuring communications and actions taken do not inadvertently result in post-response issues for the system.

On-call staff should also be aware of potential Indicators of compromise to facilitate detection of a cyber-incident. This also facilitates dissemination information up and down the chain of command to help ensure timely and effective communication.

Detecting an Incident

Understanding Indicators of Compromise (IoCs) through alert triage is critical to identifying an attack as early as possible. Examples of technology that helps identify IoCs includes intrusion detection system/intrusion protection system alerts, antivirus alerts, network scanners, log analyzers, security information and event management (SIEM).

The system should determine how, based on unique characteristics and current capabilities, it would detect an incident. This may include any of the technologies listed above coupled with the awareness of staff to identify and report potential incidents.

Severity Matrix

Incident response actions vary by the severity of the incident. The following severity matrix provides an example of how a system might characterize severity levels, recommended actions at each level, and escalation thresholds for how a system might move from one level to the next. The system should add or modify this information as appropriate to support threat detection and incident response.

[The system should adapt the following table.]

Severity Level	Recommended Actions	Escalation Threshold
Low: • Normal IT/OT operations • Staff monitor system per normal	Maintain normal operations.	The threat level escalates.
Medium: The country, industry, or local threat level has increased. Nothing specific to the system has been noted.	Maintain normal operations. Heighten awareness of system staff.	The threat escalates to directly target the system.
High: A threat directed at the system has been noted.	Activate the system's emergency response plan and Department Operations Center. Notify response partners.	It is discovered that the system is directly impacted.
Critical: The system discovers: • Infection of a device. • A breach is discovered.	Implement the Cyber-Incident Response Checklist, below.	Not applicable.

A system must also deescalate an incident. While the staff must determine what the relevant thresholds are for de-escalation, the following section presents a Cyber-Incident Action Checklist (Cyber-IAC) template that may be adapted for use in a CIRP.

Cyber-Incident Action Checklist

Developing a Cyber-IAC is a valuable tool in the Incident Response (IR) process. It aids in understanding the full scope of an attack and in capturing lessons learned during the post-incident phase. The following Cyber-IAC is written to support Operational Technology (OT)/SCADA incident response. It can be adapted to an IT environment, if that is helpful to the system. In the following Cyber-IAC template:

- Tasks are laid out sequentially and colored to indicate which phase of incident response the task should be completed within, including:
  - **Discovery –** During this phase, the system discovers the incident.
  - **Initial Response –** During this phase, the system begins executing response actions.
  - **Sustained Actions –** During this phase, the system implements sustained actions to ensure operational continuity, investigate the incident, and addresses the cause of the incident.
  - **Remediation & Recovery –** During this phase, the system confirms that systems/capabilities are fully recovered.
  - **Termination & Follow-up –** During this phase, the system concludes all response actions and conducts follow-up activities (e.g. conducts a "hot-wash" and completes after-action report).
- The role of the person who should take the action specified, including:
  - **Incident Discoverer –** The person who first reports the incident to colleagues.
  - **Incident Commander –** The person who declares an incident and directs the system's response to the cyber-incident.
  - **OT/SCADA Tech –** The person responsible for maintaining the OT/SCADA system.
  - **Operations –** The person responsible for ensuring both normal and emergency operations of the system.
  - **Public Information Officer –** The person responsible for development and delivery of external communications.
  - **Legal Counsel –** The person responsible for advising management to ensure lawful response practices by the system.

While multiple roles are called out, it may be that a single person serves in more than one role. This is a common occurrence under the principles of Incident Command System (ICS).

[The system should adapt the following table.]

Discovery	Initial Response	Sustained Actions	Remediation & Recovery	Termination & Follow-up

OT Cyber-Incident Action Checklist

Date/Time	No.	Task	Notes
	1	**Incident Discoverer:** The problem is discovered. This may occur through one of the following ways: • Observation by an OT user • System irregularity • Routine System Monitoring • OT alarms	
	2	**Incident Discoverer:** Notify: OT Staff, Supervisor, Incident Commander	
	3	**Incident Commander:** Assess the situation and declare an incident, if needed. Notify staff as appropriate including legal counsel, the Public Information Officer, and external response partners. Attempt to determine the source and extent of the problem or if it is suspected that the system has been compromised by an intruder.	
		If possible, physically disconnect all external links to SCADA systems. Do not turn off or reboot systems, this preserves evidence and allows for investigation.	
		If possible, place affected or potentially affected equipment in local/manual control, as needed.	

Date/Time	No.	Task	Notes
	4	**Public Information Officer:** Notify stakeholders and response partners that an incident has occurred, and the system is responding accordingly. Consider notifying the public, if determined necessary by the Incident Response Team.	
	5	**Incident Commander:** If SCADA has been manipulated, Notify Senior Staff.	
	6	**Incident Commander:** Mobilize necessary personnel. Direct available personnel to perform any needed repairs and operate local control of facilities/equipment as necessary. Additional personnel may be necessary to manually operate the water/wastewater facility.	
	7	**Operations:** Assume local control of affected facility/equipment, as needed. Deploy to the affected facilities. Direct available personnel to operate local control of facilities/equipment as necessary.	
	8	**Public Information Officer:** a. Communicate with law enforcement, as appropriate.	
		b. Conduct other notifications (e.g. state agencies), as appropriate.	
		Provide periodic updates to stakeholders and response partners that an incident has occurred, and the system is responding accordingly.	

Date/Time	No.	Task	Notes
	9	**Incident Commander:** When applicable, contact the system's insurer. This may result in engagement with a cybersecurity forensic consultant for comprehensive forensic analysis. Discuss the Tactics, Techniques, and Procedures, and indicator(s) of compromise with forensic team. Discuss steps required for remediation. If the insurer does not require engagement with a cybersecurity forensic consultant, the system should determine if they should engage.	
	10	**SCADA Tech:** Compare PLC programs for all potentially affected PLCs against baseline PLC program. Identify and record any anomalies. Isolate PLCs requiring remediation.	
		Completely purge the memory from all affected or potentially affected PLCs. Download latest archived, operative PLC program (if unaffected by the attack).	
		Recover and resume network connectivity based on baseline network switch configuration files.	
		Recover OT servers and workstations to last known operational state.	
		Force password change on all systems connected to, or impacting, OT systems.	
		Restart reconfigured OT server application. Verify that the application is current. If not, install any service packs or updates installed since the last backup.	

Date/Time	No.	Task	Notes
	11	**Operations:** When issue is resolved (and it has been determined by the operations lead that operating in local automatic mode poses no risk), reset controls to automatic mode.	
		Verify proper facility/equipment operations	
	12	**Incident Commander:** Return assets to safe operation and perform site cleanup as necessary.	
		Public Information Officer: Notify stakeholders that response actions are complete, and operations has returned to normal.	
	13	**Incident Commander:** Initiate post incident analysis and take corrective action.	
		Coordinate hot-wash with internal/external parties as appropriate.	
		Prepare an After-Action Report. Update ERP as necessary. Update policies and/or procedures as necessary.	

Post Incident Actions

Following any incident, the system staff should complete several steps to help ensure similar incidents do not occur again.

Evidence Retention

Where appropriate follow all data retention policies for evidence gathering and handling. In addition, identify how the attack occurred as this information might be needed for legal proceedings. Data such as location, serial number, model number, hostname, MAC and IP address can all be used for identifying information.

Lessons Learned / After Action Report (AAR)

Post incident analysis is crucial to preventing repeat incidents. Developing a timeline of events can help paint the full picture as to the nature and scope of the attack. The following questions are examples from the NIST Special Publication 800-61 and industry best practices that will assist in the investigation.

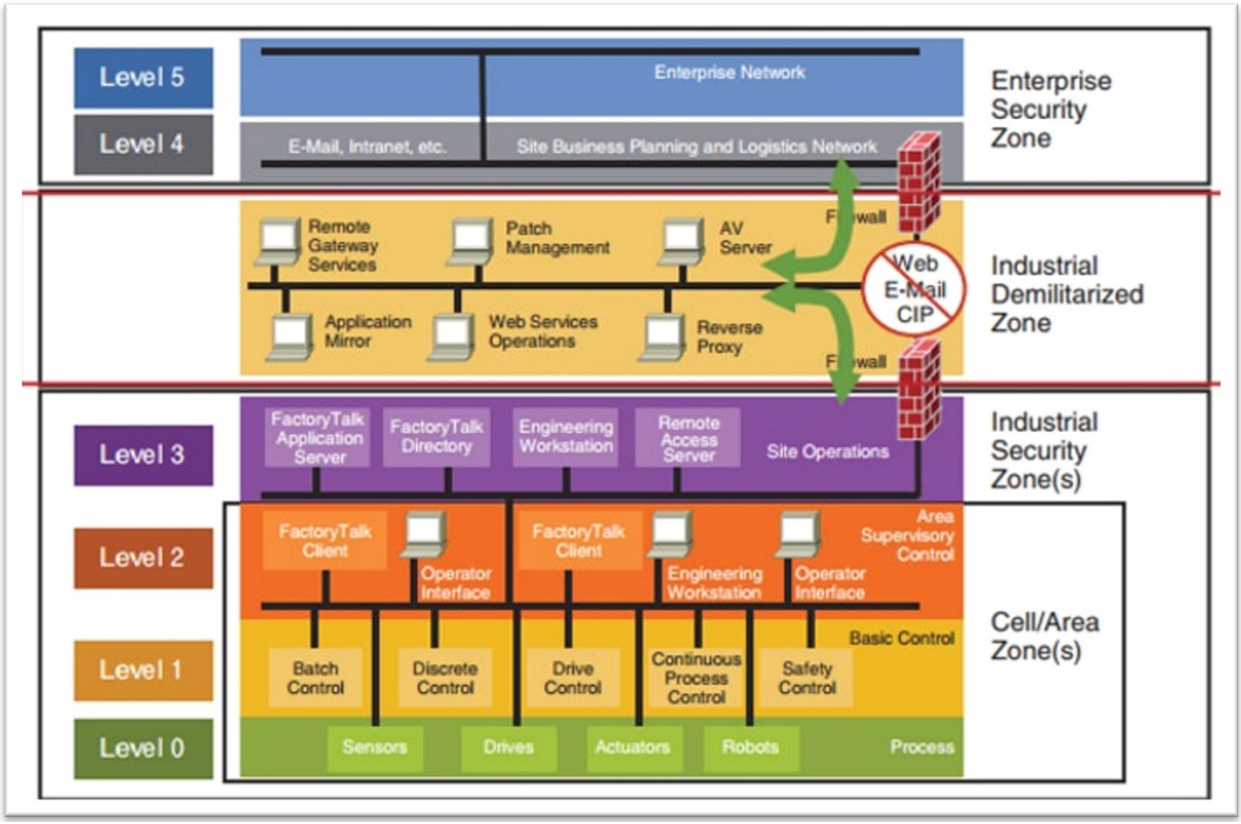
- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Implementing Improvements/Corrective Actions

Corrective actions are specific steps taken to address issues found in lessons learned. Identifying policies and procedures that need to be updated as well as potential tools or products that could have assisted in the identification or containment phases. Other actions such as enhanced training and awareness programs help facilitate team members understanding of attack vectors and IoCs.

Appendix G: Network Architecture Reference Diagram and Definitions

OT and enterprise system architectures provide an extensive list of new terminology for users of this guidance document and AWWA Assessment Tool to learn and understand. The Purdue Model for ICS security, as illustrated in the following figure, is a widely adopted network segmentation-based reference architecture for industrial control systems.[2] Implementation of this network architecture supports systems with the implementation of robust and sustainable cybersecurity controls.



Purdue Model for ICS Security (NIST 2021)

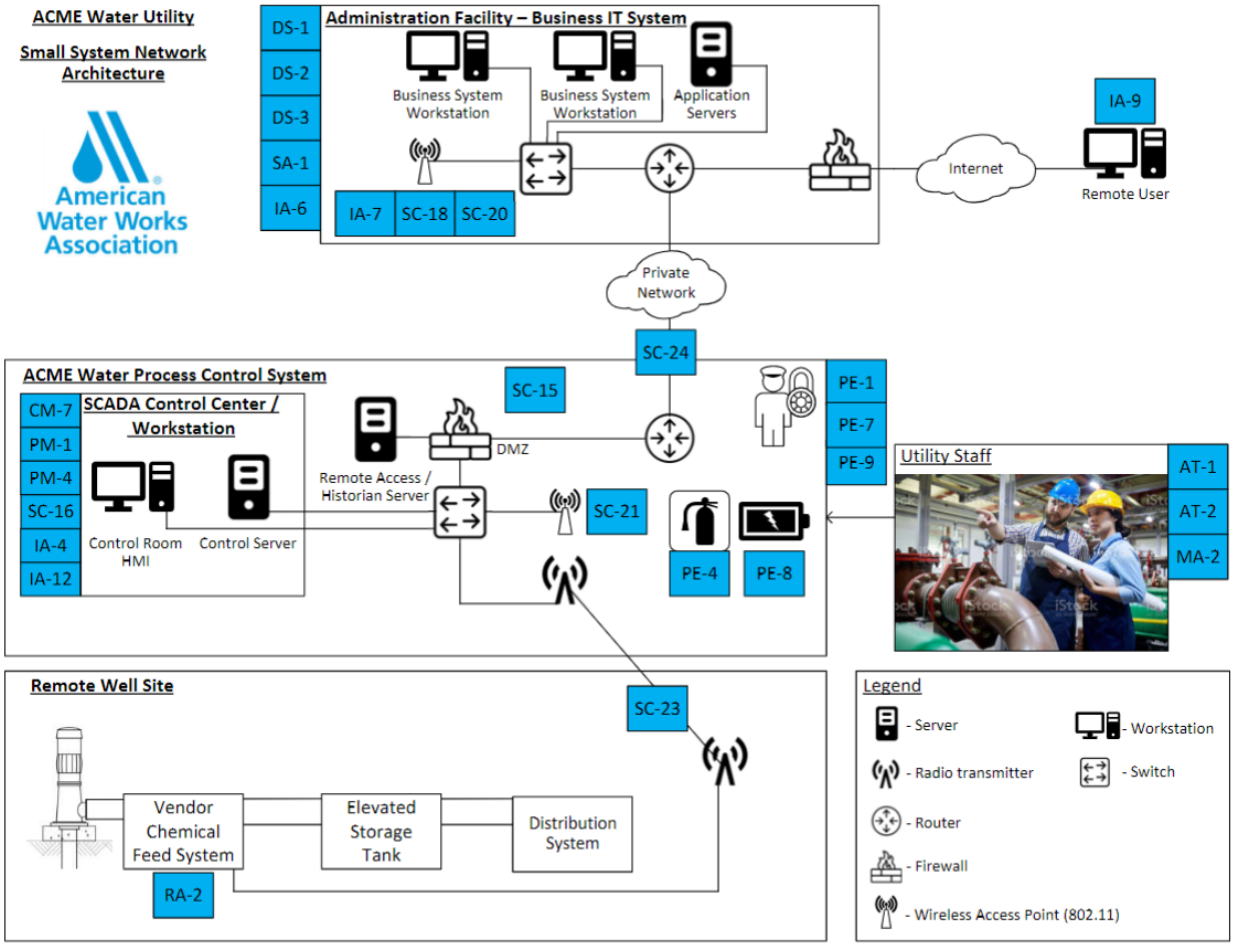
[2] NIST. 2021. Figure 1: Purdue Model of Computer Integrated Manufacturing. Figure 1: Purdue Model of Computer Integrated Manufacturing. Accessed: April 25, 2025

Appendix H: Water/Wastewater Small System Network Architectures

Each of these graphics show where each of the 28 Selected Small Systems Cybersecurity Controls would apply in a water and wastewater system.

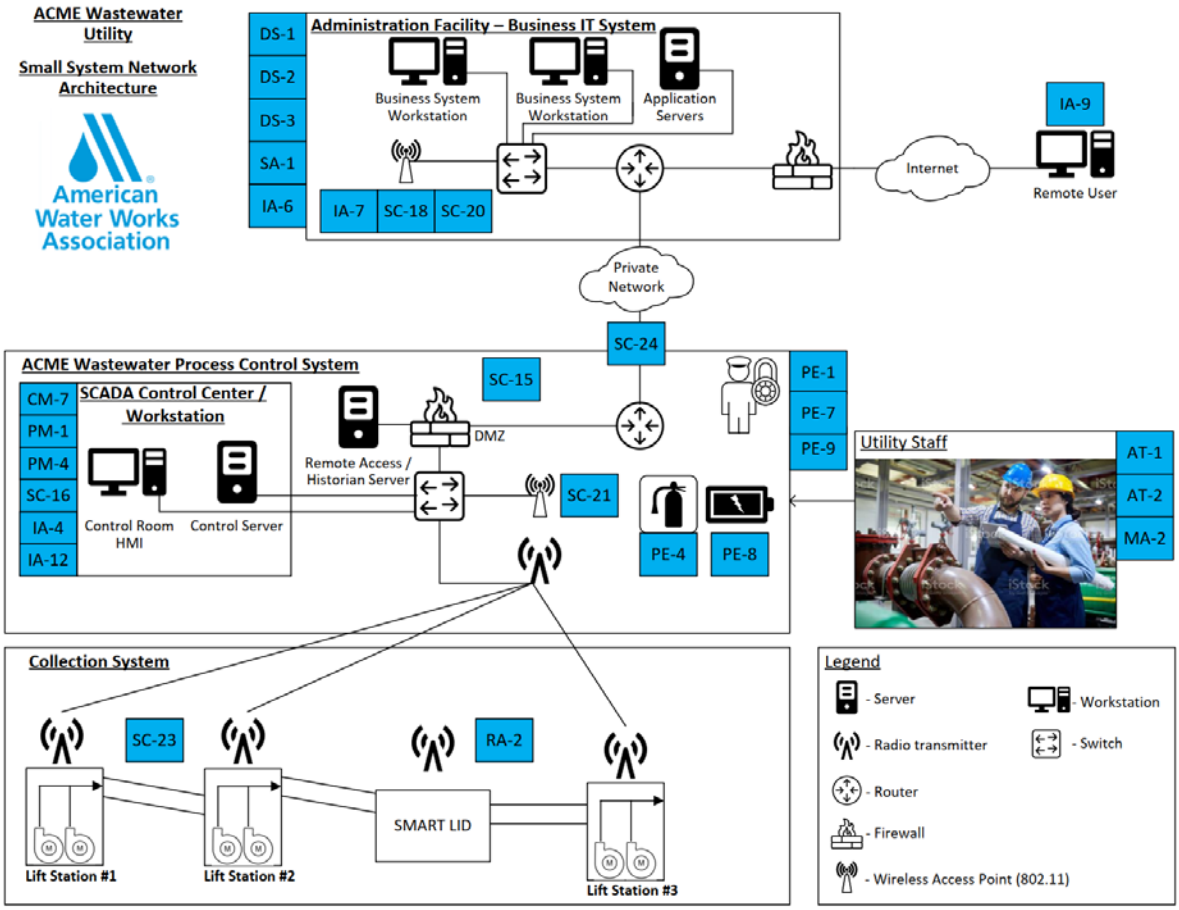
Water – Small System Example Network Architecture

The following graphic is representative of a small water systems network architecture. It shows where the system would implement the various 28 Selected Small Systems Cybersecurity Controls within its operations and OT environment.



Wastewater – Small System Example Network Architecture

The following graphic is representative of a small wastewater systems network architecture. It shows where the system would implement the various 28 Selected Small Systems Cybersecurity Controls within its operations and OT environment. This architecture is similar to the Water – Small System Example Network Architecture. Generally, the IT/OT technologies and associated cybersecurity controls are the same regardless of whether the system is water or wastewater.



Appendix I: SCADA in the Cloud: Risk and Resilience Management

AWWA SCADA in the Cloud: Risk and Resilience Management

Version 2.0

Tool and Guidance Revision History		
Version	Date	Description
1.0	9/1/2021	Initial Release as Appendix C in AWWA Water Sector Cybersecurity: Risk Management Guidance for Small Systems.
2.0	5/12/2025	Minor formatting, grammatical, and terminology revisions. Updated Consequence-driven, Cyber-Informed Engineering reference to a Cyber-Informed Engineering reference.

Cover Photo Source: Naval Sea Systems Command (https://www.navsea.navy.mil/Media/Images/igphoto/2001963531/)

Disclaimer

The authors, contributors, editors, and publisher do not assume responsibility for the validity of the content or any consequences of its use. In no event will AWWA be liable for direct, indirect, special, incidental or consequential damages arising out of the use of information presented herein. In particular, AWWA will not be responsible for any costs, including, but not limited to, those incurred as a result of lost revenue.

TABLE OF CONTENTS

Introduction

Cloud-based technologies have grown in popularity in recent years, leading to an increasing number of systems adopting cloud services for SCADA monitoring and control. This trend is most prevalent amongst small systems. While attractive for various reasons, systems considering the migration to cloud-based SCADA should be aware of the risks. These risks to the security and resilience of the system must be accounted for within the life-cycle costs of the SCADA system, and the potential impacts. Therefore, any system considering cloud-based SCADA should proceed with caution. This guide will help systems, especially small systems, understand some of the tradeoffs associated with adopting SCADA in the cloud.

Technology Background

Cloud computing technology includes a multitude of on-demand technology services where the user can utilize the internet to manage SCADA functions rather than having in-house (also referred to as “on-premises”) resources. These cloud technologies can be adapted to support a variety of enterprise and operational assets, including SCADA systems. There are multiple options to support water system monitoring and operations, including:

- **Monitoring only –** Cloud reporting/analytics tools to log and analyze data.
- **Monitoring & control –** Both monitoring and control capabilities to support data logging and analysis, and control of physical assets is enabled through the cloud.

The Evolving Purdue Model for Industrial Control Systems (ICS)

The Purdue Model for ICS security (Figure 1) is a widely adopted network segmentation-based reference architecture for industrial control systems. It works well for on-premises process control systems that are under the complete control of asset owners; however, with the introduction of cloud services and cloud-connected devices a hybrid model is necessary, and the flow of data is no longer strictly hierarchical.

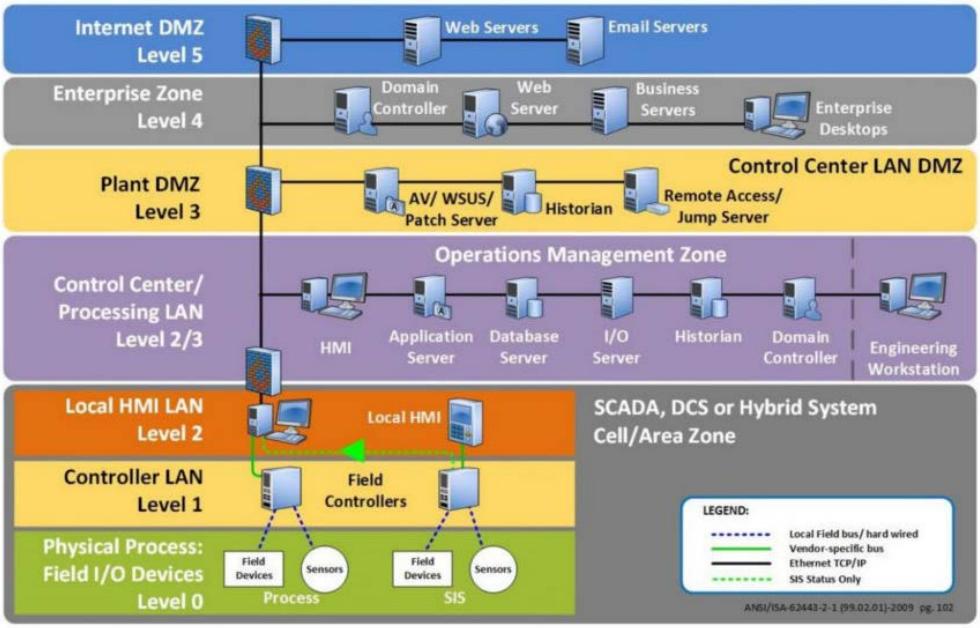


Figure 1 – Purdue Model for ICS Security (NIST 2021)

The Purdue model still serves a purpose. There is much work being done to revise the model into a new hybrid architecture. Figure 2 is a possible revision to support cloud services and cloud-connected devices.

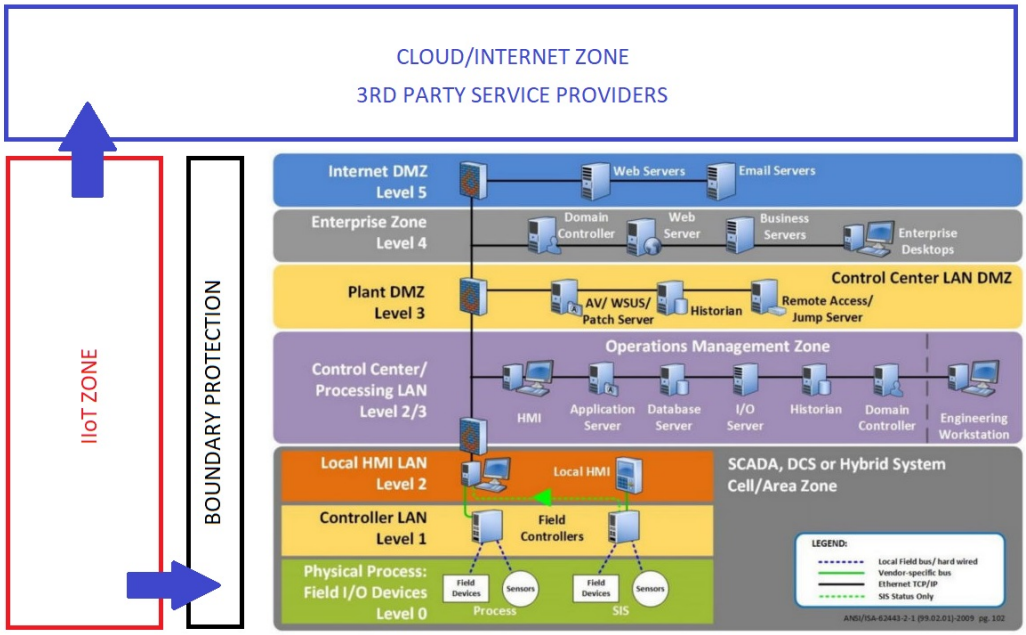


Figure 2 – Purdue Model for ICS in the Cloud Security (Adapted from NIST 2021)

Benefits of Adoption

There are many factors that contribute to the wide-spread adoption of cloud-based technologies. The following sections provide a high-level summary of these benefits.

Maintenance and Efficiency

Due to the virtual nature of cloud-based technologies, the hosting of a SCADA system often results in a reduced capital expenditure. Cloud-hosted technologies, including SCADA systems, require no control centers or backup centers, allowing for the use of technologies through the internet without requiring power systems, cooling and space for the physical storage of that technology or its data. In addition, cloud service providers for a public cloud environment tend to manage everything, including the application, data, runtime, middleware, operating system, virtualization, servers, storage, networking, and the physical security of the SCADA system,[1] freeing up the time of in-house employees for other tasks. Many municipalities struggle to support water and wastewater SCADA systems due to the focus on maintaining the high availability of first responder services (e.g. fire, police, 911).

Improved Cyber-hygiene

As a result of legacy underinvestment and the national cybersecurity skills gap, many systems struggle to maintain good cyber-hygiene within their system. Cyber-hygiene is a large concern for systems and providers, alike. Cyber-hygiene includes the steps taken by users and providers to maintain system health and improve security. Cloud service providers are expected to maintain their systems, including those containing the SCADA software and data, in a healthy manner, providing updates and patches to those systems as they are released. Additionally, cloud service providers provide routine maintenance, all of which allows the user of the service more time for other tasks. Finally, cloud service providers should have better disaster recovery/business continuity planning to respond to cyber-attacks. The system must understand how they fit into these plans.

Scalability and Cost

Due to the nature of the cloud, the resources needed for operation are easily changed, allowing for relatively easy scaling, up or down, as needed. For processing and data storage, the scaling up and down occurs automatically, making additional hardware

[1] National Security Agency. Cloud Security Basics (PP-18-0571) August 2018. https://www.nsa.gov/portals/75/documents/what-we-do/cybersecurity/professional-resources/csi-cloud-security-basics.pdf Last accessed: April 25, 2025.

purchases and installment for these system components unnecessary. Operational costs may be reduced, as in-house staff members are no longer responsible for hardware maintenance or backups and redundant resource costs disappear.

Risks of Adopting SCADA in the Cloud

While cloud adoption can reduce capital and O&M expenditures, there are inherent risks with implementing SCADA in the Cloud. A system considering implementing SCADA in the cloud must deal with several types of new risk. These are sorted by time scale into day-to-day risk and long-term planning risk as discussed below.

Fiduciary Responsibility

Cloud-based SCADA allows systems to contract out some fiduciary responsibility. It must be noted that the fiduciary responsibility that system leadership has for the cybersecurity and more broadly – risk and resilience management, cannot be contracted out. Systems are still required to do their due diligence and make best efforts to manage cyber-risk as discussed in AWWA's *Cybersecurity Risk & Responsibility in the Water Sector* (AWWA 2019).

Day-to-Day Risks

Relying on an external entity for control system operation creates new risks for the system. This is due to an inability to implement all of the security controls necessary, as many cloud providers do not allow for the implementation of outside controls and instead ask the consumer to rely on their pre-existing controls.

Dependence

A large issue with adopting SCADA in the cloud is the new dependency hazard on the cloud system. Operation of the water or wastewater system is now dependent on the cloud platform. Additionally, the reliance on the cloud-service provider will likely lead to the erosion of the knowledge and capabilities needed to successfully implement and run the water system. With the adoption of SCADA in the cloud, maintaining capabilities for manual operation of the system, in the absence of any automation, is an important risk management strategy.

Increasing the Cyber-Attack Surface

An inherent risk to migrating any environment to the cloud is that is automatically increases the cyber-attack surface. This is due to the digital nature of the cloud, as everything is stored online and likely out-of-house, so the possibility of illegal access to the operate and control systems in the cloud increases, even when controls have already been implemented.

Increased Target Value

Cyber-adversaries often act in a logical way. When numerous organizations rely on one service provider for services such as a SCADA in the cloud, that service provider becomes a more attractive target. As systems adopt SCADA in the cloud from a limited number of providers, the risks of a cyber-attack on one of those providers may unintentionally increase for an individual system.

Long-Term Planning Risks

Life-Cycle Cost Management & "Lock In"

Implementation of cloud-based SCADA requires a full "rip and replace" of the existing traditional SCADA system. Coupled with the fact that the cloud-based SCADA system hardware and software are proprietary, the system is "locked-in" to that solution and substantial capital investment is the only way out. If system leadership in the future decides to change from the cloud-based SCADA service provider to return to the traditional, on-premises SCADA, system owned and operated system. The reliance on the cloud-service provider will likely lead to the erosion of the knowledge and capabilities needed to successfully implement and run in-house SCADA by system staff.

Therefore, it is critical to understand the full life-cycle costs of adopting a cloud-based SCADA solution. This not only includes the implementation of the cloud-based SCADA solution, maintenance of that solution, but the potential turn-over of the *entire* system at some point in the future to a different SCADA solution. It is recommended that this planning risk be evaluated, much like other significant hazards/planning risks that a system must account for. Some level of financial modeling should be conducted to understand these current and future risks.

Recommendations for Systems Considering SCADA in the Cloud

The following sections provide recommendations to support systems with their effort to conduct due diligence and make best efforts to manage risk and resilience.

Security Objectives for Protecting Cloud Infrastructure

SCADA in the cloud providers must implement exceptional cybersecurity practices. While most cybersecurity assessment tools are focused on on-premises systems, they can inform the practices of the cloud service providers and serve as a starting point for a system to ask questions about cybersecurity practices.

Does the cloud service provider deploy controls/systems to provide the following?

1. **Asset Management –** automatically building an inventory and tracking the real-time status of the devices and collecting metrics such as:
    a. Device type, hardware version, software version
    b. Location
    c. Local/remote credentials
    d. Network traffic patterns (protocols, packet/byte counts, number of sessions)
    e. IP addressing information
    f. Threat level based on known vulnerabilities
2. **Application Visibility and Control –** continuous monitoring of protocols and functions that are being used between devices and alerting on abnormal communications/activities.
3. **Intrusion Detection and Prevention –** always assume cloud servers/devices may become compromised, leading to an attack. Does cloud provider deploy an intrusion prevention system (IPS) to detect and block attacks against cloud-connected devices.
4. **Network Segmentation –** how are cloud-connected devices segmented from other clients? How are control servers and remote access segmented? Is the service dedicated (not shared between clients) or a multi-tenant architecture?
5. **Logging and Monitoring –** centralized logging and monitoring of the entire cloud environment. This includes establishing baselines and providing access to logs and events that are generated from deviations to the baseline.

Many current cybersecurity assessment tools including the AWWA Cybersecurity Risk Management Guidance and Assessment Tool (AWWA 2025) are primarily applicable to on-premises SCADA systems. At the same time the most common SCADA architecture model (the Purdue model) has not been fully adapted to integrate cloud-based technologies.

Cloud SCADA service providers may not be willing to share many of these details on their operations. The system should conduct sufficient due diligence to ensure the security practices of the provider are consistent with risk management expectations of the system.

Service Level Agreements and Questions to Ask

One of the best ways to manage the risks mentioned above is to establish a strong service level agreement (SLA) with the cloud service provider. An SLA lays out all the

information a user might need in order to make an informed decision on which cloud service provider to use – especially regarding responsibility of use on both the user side and the provider side. The SLA should answer all of the following questions:

- **Availability –** What is the availability promised by the cloud service provider? Is there a plan in place for unexpected downtime? How are users updated on planned downtime due to maintenance and repairs?
  - For example, a 99% uptime SLA results in over 3.5 days of potential downtime per year while a 99.9% uptime SLA results in less than one hour of potential downtime per year.
- **Data ownership –** Who owns the data stored in the cloud? What is the data availability to the user after termination of use? How good is the cyber-hygiene of the provider?
- **Disaster recovery and backups –** What is the plan in case of a disaster? Does the cloud service provider have a backup and recovery system? Does it require activation of field units? How are backups of the data taken? How often are they taken? What is plan B in case of a disaster?
- **Cloud hardware and software –** What are the specifications behind the cloud environment construction? What hardware is being used by the cloud service provider? What software is being used? What are their versions?
- **Customer (system) responsibilities –** What is the customer liable for? What are the expectations of the customer? What type of backup operational capabilities does the system need to maintain?

Select Contracting Terms to Understand

The following select contracting terms should be understood by the system and negotiated to the extent possible.

1. **Data confidentiality and integrity –** Determine who holds the responsibility for data confidentiality and integrity. In most cases, the cloud service provider expects the user to be responsible for the confidentiality and integrity of data.
2. **Data storage –** Determine where the data is stored (i.e. country?) and if there are existing policies for the storage of various forms of data in secure places.
3. **Compensation –** Determine what happens if there is a failure on the side of the cloud service provider. In many cases, cloud service providers take a limited liability approach and provide no compensation in the case of negligence or failure, so it is important to understand what is provided if an incident occurs.

4. **Changes to the terms –** Determine how changes of the terms of agreement take place, as well as how the service provider will notify the user of changes.
5. **Dispute resolution –** Determine where dispute resolution is to take place in case of an issue. There are varying laws in different countries, and it is important to know the rights of the system.

Cyber-Physical Resilience

In addition to the adapted Purdue model presented above in Figure 2, process control systems should be engineered to protect physical assets and minimize the impact of a cyber-incident. A good framework to direct the engineering and operations efforts to improve cyber-physical resilience is Idaho National Laboratory's (INL's) Cyber-informed Engineering (CIE; INL 2023). This framework helps to identify common engineering and operations approaches to minimize the impact of a cyber-incident. While the principles of CIE are universal in their application, it should be applied to individual implementations to ensure that any engineering and operations-based controls do not interfere with the proprietary hardware and software from the cloud-based SCADA service provider.

Cyber Risk

While relying on a cloud service provider for SCADA monitoring and control may be an attractive idea, there are some inherent risks with it that must be explored. Any monitoring and processing of data, especially sensitive or business-critical data, from outside of the business introduces risk due to the inability for that data to be processed using in-house security controls. Any control of physical assets through the cloud should be evaluated in detail and backups and physical protections must be considered.

SCADA in the cloud may be most applicable to facilities and operations where the risk of service disruption to customers, especially critical customers like healthcare facilities, is minimal. This likely means smaller facilities in less populated areas. Regardless of the application of a cloud-based SCADA solution, a system must do their due diligence and make well-informed efforts to manage risk.

References

AWWA. 2019. Cybersecurity Risk & Responsibility in the Water Sector. https://www.awwa.org/wp-content/uploads/AWWA-Cybersecurity-Risk-and-Responsibility.pdf. Last Accessed: September 3, 2021.

AWWA. 2025. Water Sector Cybersecurity Risk Management Guidance. www.awwa.org/cybersecurity

INL. 2023. Cyber-informed Engineering. https://www.osti.gov/biblio/1995796. Last accessed: April 23, 2025.

ISA. 2009. ISA62443 – ANSI/ISA-62443-2-1 (99.02.01)-2009. Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program.

NSA. 2018. Cloud Security Basics. https://www.nsa. gov/Portals/70/documents/what-we-do/cybersecurity/ professional-resources/csi-cloud-security-basics.pdf. Last Accessed: April 23, 2025.

Appendix J: User Interface Questions

The questions summarized in the following tables are included in the user interface. These include questions for:

- Phase 1 – Getting Started on Cybersecurity Fundamentals
- Phase 2 – Complete a Cybersecurity Assessment
  - Cybersecurity Assessment Options
  - AWWA Small System Assessment
  - AWWA Assessment – Technology Use Questions

Phase 1 – Getting Started on Cybersecurity Fundamentals

#	Question	Additional Details	Yes/No/ Uncertain
1	Does the system have public internet facing devices?	Publicly facing devices/surfaces provide the most obvious attack vectors for adversaries. This question has two components. First is to ensure that any devices that don't need to be publicly facing, are removed from that condition. Second, is to ensure that any devices that are required to be publicly facing, are free of vulnerabilities.	
1.1	Does the system currently conduct vulnerability scanning of public internet facing devices?	For example, CISA's Vulnerability Scanning[3] service provides no-cost to the system scanning of publicly facing devices. In addition, it provides reporting on vulnerabilities detected during the scan.	
2	Does the system use remote access to your systems?	Many systems use remote access to monitor and control their process and pumping performance.	
2.1	Does the system enforce multi-factor authentication for remote access?	If remote access is implemented, it must be include multi-factor authentication (MFA). MFA provides protection against the many cyber-attacks.	
3	Does the system have unique usernames and passwords for each user?	Each user has unique individual credentials. In addition, they have unique credentials for each system (e.g. IT and OT).	

[3] https://www.cisa.gov/cyber-hygiene-services. Last accessed: December 9, 2024.

#	Question	Additional Details	Yes/No/ Uncertain
3.1	Does the system enforce password management best practices?	Best practices such as password strength are implemented.	
4	Does the system have a Cyber Incident Response Plan?	Development of a CIRP is critical for a system to establish response and recovery capabilities. This plan includes specific procedures and communications protocols for how to establish safe and reliable operations if a cyberattack is suspected or may be occurring.	
5	Does the system change default passwords on all network devices and have a policy indicating staff/ contractors must do this?	Default passwords are set by manufacturers and are common across devices. Therefore, if an adversary knows the default password, they may access and reconfigure the device. Updating default passwords to custom passwords can prevent adversaries accessing and manipulating devices.	
6	Does the system monitor internal network traffic via firewalls or another monitoring solution?	Monitoring internal network traffic allows for several important capabilities: 1. Asset management of network devices. 2. Establishing a network traffic baseline. Comparison of network traffic to known adversary tactics techniques and protocols (TTPs).	
7	Does the system have backups of all critical software and programs?	The system has easily accessible backups of programs and device configurations to support response and recovery operations.	
7.1	Does the system test recovery of critical software and programs?	The system periodically verifies that backups function as expected and staff are knowledgeable on how to test and deploy backups.	
8	Does the system leadership team (board, council, etc.) address cybersecurity at least once, annually?	The system's governance teams prioritizes cybersecurity.	

#	Question	Additional Details	Yes/No/ Uncertain
9	Does the system budget for cybersecurity improvements?	The system has budget for the implementation and maintenance of cybersecurity, including sufficient staff and/or contractor support.	
10	Does the organization have a defined cybersecurity risk management leader?	A single staff member should have explicit responsibility for cybersecurity of the system. This includes documenting this responsibility in job descriptions and including it in periodic performance reviews.	
11	Does the organization provide cybersecurity training to all employees?	The system provides some level of cybersecurity training to all employees so they can better understand their role in keeping the organization cyber-secure.	

Phase 2 – Cybersecurity Assessment Options

#	Question	Additional Details
1	AWWA Small System Assessment (systems serving less than 10,000 people)	Systems serving fewer than 10,000 people should start with this assessment format.
2	AWWA Assessment	Systems serving more than 10,000 people or systems serving less than 10,000 people with mature cybersecurity practices should use this assessment format.
3	CSET® Assessment	AWWA collaborated with the Department of Homeland Security (DHS) and INL to integrate the AWWA Tool output with CSET®. This integration allows a user to seamlessly move into a more intricate cybersecurity assessment methodology.

Phase 2 – AWWA Small System Assessment

#	Question	Additional Details	Yes/No
1	Does the SCADA system monitor or control two or fewer sites and have only one workstation/server?	The size, geographic distribution, and whether or not control/monitoring is centralized, may require additional cybersecurity controls to ensure secure and reliable operations.	
2	Is the SCADA system used by only one person?	If more than one person uses the SCADA system, additional considerations are required to ensure secure access and logging of user actions.	
3	If the SCADA system was completely disabled, could operations continue to operate the water system indefinitely and have operations operated that way recently?	Losses of automation can result in operational disruptions. Maintaining operational continuity through these events is an important emergency response capability.	
4	Does the organization have any type of documented policies and procedures for staff?	Policies and procedures provide direction to system staff and provide legal protection to the system from misuse by both authorized and unauthorized users.	

#	Question	Additional Details	Yes/No
5	Does the SCADA system use only “cloud” technology (i.e. access via phone with no servers onsite)?		
6	Does the organization have less than five (5) staff members?		

Phase 2 – AWWA Assessment – Technology Use Questions

#	Question	Additional Details	Yes/No
1	Are any data transferred to or from your OT network, by any electronic means?	Examples of electronic data transfer include both automatic (e.g. automated export of data from the OT environment) and manual (e.g. transfer of data to/from the OT environment via thumb drive). Examples of data that may be transferred include: • Water quality data collected by the OT and transferred for regulatory reporting • Asset performance data for asset management • Operating system / software patches and updates	
2	Do users manually transfer any electronic data to or from the OT environment?	Users include anyone internal or external with access to OT. This may include operators, technicians, and third-party consultants. Users are able to initiate transfer of data to and from the OT. Examples of manual data transfer include: • USB • Portable media device • Temporary network connections (an ad hoc network connection for transferring data from one computer to another) • Shared drives • Cloud file share (e.g. DropBox)	
3	Are any electronic data transferred to or from the OT environment using an automated process, without user interaction?	Examples of automated transfer of data include: • Automated software or firmware updates • Licensing • Operating System updates • Antivirus signatures • Database transfer • Network monitoring by devices external to the OT	

#	Question	Additional Details	Yes/No
4	Are any users allowed to access the OT environment remotely?	Users include any personnel with internal or external access to the OT environment. These may include operators, technicians, and third-party consultants. Devices can be any network enabled device either corporate supplied or personal. Examples of remote access include: • Operations staff access the PCS environment from mobile device. This includes web view and read only. • Users have access to remote physical site using any non-OT environment.	
5	Is remote access to the OT environment allowed via mobile devices?	Devices can be any network enabled device either corporate supplied or personal. This includes web view and read only. Examples of mobile devices include: • Laptops • Tablets • Cellphones • Smart Phones	
6	Is remote access to the OT environment allowed at physically secured fixed location(s)?	Examples of remote access from physically secured fixed location include: • Control center managing remote sites • Control center remotely managing a treatment center • Office desktop computer • Computer at secured office used for managing remote booster station	
7	Are resources outside the organization used to support and/or maintain your OT environment?	Examples of resources outside of the organization supporting and/or maintaining your OT environment include: • Subsystems owned and operated by 3rd party • Systems Integrators • Equipment Manufacturers • Consultants • Vendors	

#	Question	Additional Details	Yes/No
8	Do resources (e.g. service providers) outside the organization provide OT support via remote access?	Examples of resources outside your organization providing support by remote access includes: • "Black box" solution vendor - "Black box" refers to piece of equipment on a network with contents and/or function that are unknown to the user/owner/operator. • Vendor panel solution - Vendor panel refers to a control panel provided by a vendor to monitor or operate a treatment or distribution process. For example: a vendor provided ultrafiltration unit would have an accompanying control panel to control the ultrafiltration process. • Network administration, from external sources.	
9	Do internal staff provide support for the OT via remote access?	Remote access is from outside (for example, from home) of the controlled or control room environments. Devices can be any smart phone, tablet, laptop either corporate supplied or personal. Examples of internal staff providing support by remote access include: • Remote operation and monitoring • Remote troubleshooting	
10	Are all changes or updates made to the OT environment first tested in a development, testbed, non-production, and/or training environment prior to being deployed and implemented in the field/production environment?	• These changes/updates include any programming of logic controllers, human machine interfaces, instrumentation, or any devices involved with the OT. • System changes or updates do not negatively impact OT operation. • OT changes are tested in a non-production environment before they are made in the field/production environment. • Testing is performed to ensure the proper operation and interaction with other system components before deployment. • Changes or updates may be made by either internal or external resources.	

#	Question	Additional Details	Yes/No
11	Does the OT environment include 3rd party network communication services?	Examples of 3rd party network communications services include: • Cellular (3G, 4G, 5G) • Dedicated leased line (copper, fiber) • Communication over internet • City/county communication network not dedicated to OT	
12	Does the OT environment use licensed or unlicensed wireless radios between facilities?	Unlicensed wireless spectrum frequencies – Unlicensed wireless devices operate in one of the frequency bands set aside by the Federal communications Commission (FCC) for industrial, scientific or medical (ISM) applications. Frequencies within the unlicensed wireless spectrum are free to use. Licensed wireless spectrum frequencies – Frequencies or frequency bands designated by the Federal Communications Commission (FCC) as reserved for organizations with licenses. Examples of licensed or unlicensed wireless spectrum services include: • Radio - 450MHz • Radio - 900MHz • WiFi - 2.4GHz • WiFi - 5GHz • WiFi - 6GHz • Microwave	
13	Does the OT environment share a LAN or WAN with non-OT equipment?	Examples of non-OT equipment include: • Security cameras • Access control equipment • Enterprise network services at a facility with a shared communication path • Voice over Internet Protocol (VOIP) • Fire Alarms • Vault or Panel Intrusion Alarms	

#	Question	Additional Details	Yes/No
14	Is Wi-Fi used within the OT environment to transfer data in support of operations or monitoring?	• Does your OT communication network have wireless access points? • Wi-Fi is defined in IEEE 802.11	
15	Is virtualization technology used for the OT environment?	Virtualization Technology – Technology capable of creating a virtual (rather than actual) version of something, including virtual computer hardware platforms, storage devices, and computer network resources. Examples of virtualization technology include: • VMware • Oracle VM • HyperV	
16	Is the virtualization technology dedicated to the OT environment only?	Virtualization Technology – Technology capable of creating a virtual (rather than actual) version of something, including virtual computer hardware platforms, storage devices, and computer network resources. • A separate physical host(s) is used for OT virtual machines. • All non-OT virtual machines reside on non-OT physical host(s).	
17	Does the organization accept, process, store or transmit credit card or debit card information, or accept payment with pre-paid cards branded with American Express, Discover, JCB, MasterCard or Visa International logos?	This information may be collected and stored for service payment purposes. Using a third-party company for processing PCI may cut down on risk exposure but does not exclude a company from PCI DSS compliance. Customer billing information including: • Credit/debit card numbers • Credit/debit card numbers with name, expiration date or service code • Sensitive authentication data (including magnetic stripe, PINs, CVV, etc.) NOTE: Includes organizations that have outsourced payment services.	

#	Question	Additional Details	Yes/No
18	Does the organization own, license, acquire or maintain any personally identifiable information (PII)?	PII is any information that may be used to identify an individual. This includes customers, employees, and contractors. Examples of PII include: • Customer billing information and addresses • Employee personal information, including SSN, birthdate, etc. Each state has its own data breach notification law(s) regarding PII. Depending on the state statute, a non-exhaustive list of possible examples may include (alone or in conjunction with other information) tax identification numbers, social security numbers, government issued identification numbers, account numbers, health information, email addresses in conjunction with a password, unique biometric information, etc.	

#	Question	Additional Details	Yes/No
19	Is the organization an employer that creates or receives health information that is HIPAA protected?	HIPAA defines protected health information (written, electronic, or oral) as information, including demographic data, that identifies an individual (or there is a reasonable basis to believe it can identify an individual) and that relates to: • the individual's past, present or future physical or mental health or condition, • the provision of health care to the individual, or • the past, present, or future payment for the provision of health care to the individual. Examples of HIPAA protected information include: • Employee medical records • Employee vaccine records • Health and safety records may include HIPAA protected records • Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).	
20	Is the organization responsible for the engineering design and implementation of critical infrastructure?	The water/wastewater sector is defined as critical infrastructure by the federal government (42 U.S.C. 5195(e)). Examples of holding responsibility for engineering services include: • System has an internal engineering department • System hires engineering consultants • You are part of a stakeholder organization that has internal resources or hires external resources to design and implement critical infrastructure	
21	Does the organization have a supply chain risk management program?	Do you currently require your supplier to provide any chain-of-custody documents? An example of supply chain risk management program includes ordering and confirming treatment chemicals are NSF certified.	

#	Question	Additional Details	Yes/No
22	Does the organization have a supply chain risk management program that specifically addresses cybersecurity?	Does the supply chain risk management program specify how delivery for procured products – hardware, software, and/or data will be validated and monitored to ensure their integrity? Examples of specifically addressing cybersecurity in supply chain risk management include: • Documenting information protection practices of supplier • Integrity management program for components provided by sub-suppliers • Supplier contracts include appropriate language to meet objectives of the organization's cybersecurity program	

Appendix K: Small System Baseline Cybersecurity Controls

The following controls were identified as the top priority for small systems serving populations of 10,000 or less. Note that these are generally applicable to all systems.

Category 1: Training Staff to be Cybersecurity Aware	
AT-1	A general security awareness and response program established to ensure staff is aware of the indications of a potential incident, security policies, and incident response/notification procedures.
AT-2	Job-specific security training including incident response training for employees, contractors and third-party users.
MA-2	Maintenance of relationships with authorities, professional associations, interest groups etc., formalized. This is done, in part, to maintain an up-to-date situational awareness of relevant threats.
Category 2: Know What Hardware and Software are Connected to and Operating on Your Networks	
CM-7	Monitoring of resources and capabilities with notifications and alarms established to alert management when resources/capabilities fall below a threshold.
PM-1	Asset management program including a repository containing all significant assets of the organization with a responsible party for each, periodic inventories, and audits.
PM-4	SLAs for software and information exchange with internal/external parties in place including interfaces between systems and approved policies and procedures.
SA-1	Authorization process established for new systems or changes to existing information processing systems.
Category 3: Maintain Data Security Compliance	
DS-1	A program established to ensure compliance with the minimum PCI requirements for your associated level.
DS-2	A Privacy Policy as well as a Cyber Security Breach Policy are implemented.
DS-3	A program is established to ensure compliance with the minimum HIPAA requirements. Develop a Privacy Policy as well as a Cyber Security Breach Policy.
Category 4: Protect Systems from Unauthorized Access or Use	
IA-4	Access control for confidential system documentation established to prevent unauthorized access of trade secrets, program source code, documentation, and passwords (including approved policies and procedures).
IA-6	Access control for networks shared with other parties in accordance with contracts, SLAs and internal policies.
IA-7	Wireless and guest-access framework established for the management, monitoring, review, and audit of wireless and guest access in place.
IA-9	Multifactor authentication system established for critical areas.

IA-12	Session controls established to inactivate idle sessions, provide web content filtering, prevent access to malware sites, etc.
RA-2	Third party agreement process to ensure security on access, processing, communicating, or managing the organization's information or facilities.
Category 5: Physical Security	
PE-1	Security perimeters, card-controlled gates, manned booths, and procedures for entry control.
PE-4	Physical protection against fire, flood, earthquake, explosion, civil unrest, etc.
PE-7	Physical security and procedures against equipment environmental threats and hazards or unauthorized access.
PE-8	Physical/logical protection against power failure of equipment UPS.
PE-9	Physical/logical protection against access to power and telecommunications cabling established.
Category 6: Good Network Design	
SC-15	Logically separated control network. Minimal or single access points between corporate and control network. Stateful firewall between corporate and control networks filtering on TCP and UDP ports. DMZ networks for data sharing.
SC-16	Defense-in-depth. Multiple layers of security with overlapping functionality.
SC-18	Minimize wireless network coverage.
SC-20	Wireless equipment located on isolated network with minimal or single connection to control network.
SC-21	Unique wireless network identifier SSID for control network.
SC-22	Separate Microsoft Windows domain for wireless (if using Windows).
SC-23	Wireless communications links encrypted.
SC-24	Communications links encrypted.

Appendix L: Small System Baseline Cybersecurity Control – Implementation Guidance

AWWA has identified examples of implementation and implementation resources for systems to use to support implementation for each of the 28 baseline controls. The examples provided are not exhaustive of a single control's potential implementations. For example, a control may refer specifically to an operator's workstation in the example, but the control could be applicable to all workstations in the water system's network.

Depending on a system's use of technology as characterized by answering the 22 up-front questions in the AWWA Tool, not all 28 controls may be applicable. The system should prioritize any controls in this list of 28 that appear in their list generated by the AWWA Tool.

The implementation support resources identified below are from the Center for Internet Security (CIS) Top 18 Controls and Resources, an authority on implementation and maintenance of cybersecurity controls.

Category 1: Training Staff to be Cybersecurity Aware

Training staff to reduce the risk associated with a cyber-attack. Training should be based on staff members' roles and responsibility within the system. In addition, training may be informed by the current situational awareness provided by intelligence and law enforcement agencies.

Baseline Control: AT-1

A general security awareness and response program established to ensure staff is aware of the indications of a potential incident, security policies, and incident response/notification procedures

- **What it means:** A system has a cybersecurity training program that educates staff on how to identify a potential cyber-attack, who to report to, and what immediate actions to take.
- **Examples**:
    - Staff are able to identify a cyber threat
    - Staff know who to notify in the event of a cyber threat/attack
    - Staff know what immediate actions they can take to isolate their workstations from the outside world
    - Routine staff training includes information on reporting cyber threats/attacks

- **Resources**:
  - CIS Control 14: Security Awareness and Skills Training https://www.cisecurity.org/controls/cis-controls-navigator
  - CIS Control 17: Incident Response Management https://www.cisecurity.org/controls/cis-controls-navigator

Baseline Control: AT-2

Job-specific security training including incident response training for employees, contractors and third-party users.

- **What it means:** A system has a cybersecurity training program that educates staff on how to identify a potential cyber-attack, who to report to, and what immediate actions to take.
- **Examples**:
  - There are written response procedures that define roles and responsibilities for incident response
  - A cybersecurity training and awareness program in place
  - Based on the training, staff know how to recognize to, and respond to, different types of attacks (e.g. phishing)
  - Staff know how to report a suspected cyber incident
- **Resources**:
  - CIS Control 14: Security Awareness and Skills Training https://www.cisecurity.org/controls/cis-controls-navigator
  - CIS Control 17: Incident Response Management https://www.cisecurity.org/controls/cis-controls-navigator

Baseline Control: MA-2

Maintenance of relationships with authorities, professional associations, interest groups etc., formalized. This is done, in part, to maintain an up-to-date situational awareness of relevant threats.

- **What it means:** The system works closely with authorities, professional associations, interest groups, etc., so that it is aware of any developments that might affect their security.

- **Examples**:
  - Develop and maintain formal relationship with local emergency response personnel, regulators, Internet service providers, and other organizations (e.g. local FBI contact, InfraGard, CISA, etc.)
  - Develop and maintain a response plan that includes coordination with external organizations
  - Develop and maintain relationships with external organizations to stay up to date on relevant threats.
  - Share its threat and incident information with external organizations in accordance with applicable requirements and restrictions. Maintain current contact information for external organizations
- **Resources**:
  - CIS Control 7: Continuous Vulnerability Management https://www.cisecurity.org/controls/cis-controls-navigator
  - CIS Control 16: Application Software Security https://www.cisecurity.org/controls/cis-controls-navigator
  - CIS Control 17: Incident Response Management https://www.cisecurity.org/controls/cis-controls-navigator

Category 2: Know What Hardware and Software are Connected to and Operating on Your Networks

Knowing what hardware and software are present on a network is important for maintenance and security. Managing hardware and software assets helps establish a baseline for network performance that could indicate a cyberattack. In addition, conducting regular updates of hardware and software are critical for managing vulnerabilities.

Baseline Control: CM-7

Monitoring of resources and capabilities with notifications and alarms established to alert management when resources/capabilities fall below a threshold.

- **What it means:** The system has implemented the software/hardware to continuously monitor network traffic and server performance.
- **Examples**:
  - Continuous monitoring the performance of the network/servers via an automated hardware/software solution

    - Establish network baselines against which to compare continuously generated data
    - Establish performance thresholds for the network/servers
    - Automatic alerts are issued when the network/server performance drifts below the established thresholds
- **Resources**:
    - CIS Control 8: Audit Log Management https://www.cisecurity.org/controls/cis-controls-navigator

Baseline Control: PM-1

Asset management program including a repository containing all significant assets of the system with a responsible party for each, periodic inventories, and audits.

- **What it means:** The system keeps a detailed record of all its electronic devices.
- **Examples**:
    - The system maintains an up-to-date list of all its electronic devices and components
    - The list includes model numbers, software/firmware versions, and any other information required to assess future vulnerabilities
    - The system references the list to assess vulnerabilities when they are disclosed by vendors
    - The system knows how to recover assets if data is corrupted
- **Resources**:
    - CIS Control 1: Inventory and Control of Enterprise Assets https://www.cisecurity.org/controls/cis-controls-navigator
    - CIS Control 2: Inventory and Control of Software Assets https://www.cisecurity.org/controls/cis-controls-navigator
    - CIS Control 11: Data Recover https://www.cisecurity.org/controls/cis-controls-navigator

Baseline Control: PM-4

SLAs for software and information exchange with internal/external parties in place including interfaces between systems and approved policies and procedures.

- **What it means:** The system has implemented service level agreements with all internal/external parties (contractors, service providers, vendors, etc.) who exchange software or information with the system.
- **Examples**:
  - The system has an SLA for each internal/external party (contractors, service providers, vendors, etc.) that exchanges software or information with the system
  - The system's SLAs include defining the approved interfaces between the two parties' systems
  - The system's SLAs include policies and procedures for interaction between the two parties. For example, what are they approved to do?, when?, who needs to approve the actions?, etc.
- **Resources**:
  - CIS Control 6: Access Control Management https://www.cisecurity.org/controls/cis-controls-navigator

Baseline Control: SA-1

Authorization process established for new systems or changes to existing information processing systems.

- **What it means:** A system manages the security of Information Systems through an organizational risk management process.
- **Examples:**
  - Risk management process (including policies and procedures) are in place.
  - Roles and responsibilities related to risk management are properly defined and assigned.
- **Resources**:
  - CIS Control 4: Secure Configuration of Enterprise Assets and Software https://www.cisecurity.org/controls/cis-controls-navigator
  - CIS Benchmarks for hardening https://www.cisecurity.org/cis-benchmarks/

Category 3: Maintain Data Security Compliance

Many systems store and transmit, or contract out the storage and transmittal of protected data. These include payment card industry (PCI) data, personally identifiable information (PII), and personal health information protected under the Health Insurance

Portability and Accountability Act (HIPAA). Individual states have laws establishing the requirements for protection of PII while broader standards are established for PCI and HIPAA data.

Baseline Control: DS-1

A program established to ensure compliance with the minimum PCI requirements for your associated level.

- **What it means:** The system complies with the applicable PCI requirements and has a plan to make sure that they protect cardholder data.
- **Examples:**
  - Has the system assessed its security needs against the PCI requirements?
  - Does the system request current ROC (Record of Certification) from third party payment processors?
  - Does the system maintain strong network security and access control according to PCI requirements?
  - Does the system maintain a vulnerability management program in compliance with PCI requirements?
- **Resources**:
  - CIS Control 3: Data Protection https://www.cisecurity.org/controls/cis-controls-navigator

Baseline Control: DS-2

A Privacy Policy as well as a Cyber Security Breach Policy are implemented.

- **What it means:** The system has established a Privacy Policy to protect data (e.g. personally identifiable information) that the system collects or generates. It also has a Cyber Security Breach Policy that defines the system's required response in the event of a cyber breach.
- **Examples:**
  - Does the system have a Privacy Policy that complies with any applicable standards?
  - Does the system have a Cyber Security Breach Policy that complies with any applicable standards?

- **Resources**:
  - CIS Control 3: Data Protection https://www.cisecurity.org/controls/cis-controls-navigator
  - CIS Control 17: Incident Response Management https://www.cisecurity.org/controls/cis-controls-navigator

Baseline Control: DS-3

A program is established to ensure compliance with the minimum HIPAA requirements. Develop a Privacy Policy as well as a Cyber Security Breach Policy.

- **What it means:** The system has a plan for meeting the minimum HIPAA requirements. It has also developed a Privacy Policy to protect personally identifiable data and a Cyber Security Breach Policy that defines the system's required response in the event of a cyber breach.
- **Examples:**
  - Does the system have a plan to meet minimum HIPAA requirements?
  - Does the system have a Privacy Policy that complies with any applicable standards?
  - Does the system have a Cyber Security Breach Policy that complies with any applicable standards?
- **Resources**:
  - CIS Control 3: Data Protection https://www.cisecurity.org/controls/cis-controls-navigator
  - CIS Control 17: Incident Response Management https://www.cisecurity.org/controls/cis-controls-navigator

Category 4: Protect Systems from Unauthorized Access or Use

Protection from unauthorized access to and use of systems and data protect the system from consequences associated with misuse of the data and systems. As a background reference, the AWWA prepared the document Cybersecurity Risk & Responsibility in the Water Sector.[4] This provides a summary of the importance of sound cybersecurity practices and risk management.

[4] AWWA Cybersecurity Risk and Responsibility in the Water Sector;

Baseline Control: IA-4

Access control for confidential system documentation established to prevent unauthorized access of trade secrets, program source code, documentation, and passwords (including approved policies and procedures).

- **What it means:** The system protects its sensitive system documentation and data via well-documented access control policies and procedures.
- **Examples:**
  - The system has a well-documented access control policies and procedures for protecting its documentation (e.g. PLC programs, administrative account inventories)
  - The system requires special account privileges to access sensitive documentation
  - The system uses dedicated administrative accounts. These accounts are not used for such things as internet browsing or email
  - The system has a well-rounded access control framework, including password policies, authorization, role-based access control, etc.
  - The system disables any account that cannot be associated with a practice or owner
  - The system dormants accounts after a period of inactivity
- **Resources**:
  - CIS Control 5: Account Management https://www.cisecurity.org/controls/cis-controls-navigator
  - CIS Control 3: Data Protection https://www.cisecurity.org/controls/cis-controls-navigator

Baseline Control: IA-6

Access control for networks shared with other parties in accordance with contracts, SLAs and internal policies.

https://www.awwa.org/Portals/0/AWWA/Government/AWWACybersecurityRiskandResponsibility.pdf?ver=2018-12-05-123319-013

- **What it means:** Service Level Agreements (SLA) specify security requirements for a vendor to connect to the control network (secure corporate VPN client, HTTPS, etc.)
- **Examples:**
  - Access control lists are maintained so that only authorized individuals are able to access restricted information
- **Resources**:
  - CIS Control 6: Access Control Management https://www.cisecurity.org/controls/cis-controls-navigator

Baseline Control: IA-7

Wireless and guest-access framework established for the management, monitoring, review, and audit of wireless and guest access in place.

- **What it means:** The system has a formal plan for ensuring the security of the wireless network that includes a guest access plan.
- **Examples:**
  - The system has a wireless network separate from the SCADA network
  - The system has a separate guest wireless network
  - The activity of wireless users/guests is monitored and audited by the system
  - The system actively manages and reviews the configuration of the network and user/guest access policies
- **Resources**:
  - CIS Control 6: Access Control Management https://www.cisecurity.org/controls/cis-controls-navigator
  - CIS Control 8: Audit Log Management https://www.cisecurity.org/controls/cis-controls-navigator

Baseline Control: IA-9

Multifactor authentication system established for critical areas.

- **What it means:** The system requires multifactor authentication for employees to access systems from critical areas (i.e. remote access).

- **Examples:**
  - The system physically secures critical areas
  - The system requires users to present two types of authentication, such as an RFID keychain and password or a key and thumbprint
- **Resources**:
  - CIS Control 5: Account Management https://www.cisecurity.org/controls/cis-controls-navigator
  - CIS Control 6: Access Control Management https://www.cisecurity.org/controls/cis-controls-navigator

Baseline Control: IA-12

Session controls established to inactivate idle sessions, provide web content filtering, prevent access to malware sites, etc.

- **What it means:** The system's workstations all have session controls based on security policies.
- **Examples:**
  - Workstations automatically disconnect from network after being idle for a set period of time
  - The system automatically locks workstation sessions after a standard period of inactivity
  - The workstations filter and block content from malicious or other undesirable sources
- **Resources**:
  - CIS Control 9: Email and Web Browser Protections https://www.cisecurity.org/controls/cis-controls-navigator
  - CIS Control 6: Access Control Management https://www.cisecurity.org/controls/cis-controls-navigator

Baseline Control: RA-2

Third party agreement process to ensure that external vendors and contractors utilize appropriate security measures for access, processing, communicating, or managing the system's information or facilities.

- **What it means:** The system requires third party providers to agree with their security standards before allowing them access to the facility or giving them any sensitive information.
- **Examples:**
  - Does the system enforce security standards on third-party service providers?
  - Are service providers restricted from access to any sensitive information or facilities until they have agreed with the system's security policies?
- **Resources**:
  - CIS Control 6: Access Control Management https://www.cisecurity.org/controls/cis-controls-navigator

Category 5: Physical Security

Physically securing network components and data is important to limit the potential for unauthorized access and damage from such hazards as natural hazards, structure fires, and electrical outages.

Baseline Control: PE-1

Security perimeters, card-controlled gates, manned booths, and procedures for entry control.

- **What it means:** A system enforces physical access control measures to any areas where the control system resides.
- **Examples:**
  - Individual's access is verified prior to entry to the facility.
  - Keys, cards, and/or combinations are utilized.
  - Physical access devices are audited/inventoried on periodic basis.
  - SCADA workstations are located in secure areas (i.e., locked control room).
- **Resources**:
  - AWWA G430-14 https://store.awwa.org/AWWA-G430-14-Security-Practices-for-Operation-and-Management-PDF
  - NIST 800-53 Control PE-3 https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home

Baseline Control: PE-4

Physical protection against fire, flood, earthquake, explosion, civil unrest, etc.

- **What it means:** As part of a contingency plan, a system has appropriate measures in place to continue operations in as timely a manner as possible.
- **Example:**
  - Appropriate fire suppression system in place (e.g. FM200 for server rooms)
  - Facility flood protection measures
  - Fencing and hardened doors and windows
- **Resources**:
  - NIST 800-53 Control CP-2 https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home

Baseline Control: PE-7

Physical security and procedures against equipment environmental threats and hazards or unauthorized access.

- **What it means:** A system has an alternate processing site in place that can be utilized for production should the primary site be rendered unusable due to environmental hazards.
- **Examples:**
  - Appropriate fire suppression system in place (e.g. FM200 for server rooms)
  - Procedures to implement flood protection measures
  - Policies and procedures on when and how to secure physical security components (e.g. fencing and doors)
- **Resources**:
  - AWWA G430-14 https://www.awwa.org/Store/Product-Details/productId/45320372
  - NIST 800-53 Control CP-7 https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home

Baseline Control: PE-8

Physical/logical protection against power failure of equipment (UPS).

- **What it means:** A system has a contingency plan in place in case of loss of primary means of power.
- **Examples:**
  - Uninterruptible Power Supply (UPS), generators for critical communications equipment.
  - Alternate telecommunications service in place in case of failure of primary means of communications.
  - Minimize single points of failure.
- **Resources**:
  - NIST 800-53 Control CP-8 https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home

Baseline Control: PE-9

Physical/logical protection against access to power and telecommunications cabling established.

- **What it means:** A system routes critical power and communications cabling in redundant paths.
- **Examples:**
  - Redundant paths for power and telecommunications cabling
  - Wiring terminations located in a locked wiring closet, pedestal, manholes, etc.
- **Resources**:
  - NIST 800-53 Control PE-9 https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home

Category 6: Good Network Design

Implementing a proper network design using best practices helps mitigate the potential for an attack and the consequences of an attack.

Baseline Control: SC-15

Logically separated control network. Minimal or single access points between corporate and control network. Stateful firewall between corporate and control networks filtering on TCP and UDP ports. DMZ networks for data sharing.

- **What it means:** The system's OT environment has minimal access points to any other part of the system or external network.
- **Examples:**
  - Does the system minimize connections between the ICS and other networks?
  - Are all connections to the ICS protected by a stateful firewall filtering on TCP and UDP, as well as a DMZ?
  - Does network design follow the NIST 800-82 guidelines?
- **Resources**:
  - CIS Control 12: Network Infrastructure Management https://www.cisecurity.org/controls/cis-controls-navigator
  - NIST 800-82 https://csrc.nist.gov/pubs/sp/800/82/r3/final

Baseline Control: SC-16

Defense-in-depth. Multiple layers of security with overlapping functionality.

- **What it means:** A system employs overlapping physical and cybersecurity measures to protect assets.
- **Examples:**
  - Server room is protected by means of doors under lock and key, access control authentication, unique login requirements, two-factor authentication, antivirus, firewalls, etc.
  - The following are implemented;
    - Host-based firewalls
    - Anti-virus applications (e.g. Symantec, Trend Micro, Windows Defender)
    - Anti-malware applications,
    - Intrusion detection applications
    - Network traffic access controls

- **Resources**:
  - CIS Control 10: Malware Defenses https://www.cisecurity.org/controls/cis-controls-navigator
  - CIS Control 12: Network Infrastructure Management https://www.cisecurity.org/controls/cis-controls-navigator

Baseline Control: SC-18

Minimize wireless network coverage.

- **What it means:** A system performs a wireless survey to determine antenna location and strength to minimize broadcast range of the wireless network.
- **Examples:**
  - If it is determined that the wireless network is broadcasting too far outside the boundaries of the system, radio transmit strength shall be reduced.
- **Resources**:
  - CIS Control 12: Network Infrastructure Management https://www.cisecurity.org/controls/cis-controls-navigator

Baseline Control: SC-20

Wireless equipment located on isolated network with minimal or single connection to control network.

- **What it means:** Wireless network is on a separate network from the ICS network, with minimal (single if possible) connections to the hardwired ICS network. Any connections between wireless network and ICS network are documented.
- **Examples:**
  - The system maintains a separate wireless network for personal or untrusted devices
- **Resources**:
  - CIS Control 4: Secure Configuration of Enterprise Assets and Software https://www.cisecurity.org/controls/cis-controls-navigator
  - CIS Control 12: Network Infrastructure Management https://www.cisecurity.org/controls/cis-controls-navigator

Baseline Control: SC-21

Unique wireless network identifier (SSID) for control network.

- **What it means:** The wireless network identifier (SSID) is unique for the corporate network compared to the SCADA network.
- **Examples:**
  - Implement a guest network for guests to connect personal devices
  - Implement a wireless network for staff to connect personal devices
  - The system SCADA wireless network is separate from the corporate wireless network
- **Resources**:
  - CIS Control 12: Network Infrastructure Management https://www.cisecurity.org/controls/cis-controls-navigator

Baseline Control: SC-23

Wireless communications links encrypted.

- **What it means:** Wireless data-in-transit encrypted using current wireless communications best practices.
- **Examples:**
  - SCADA data transferred via radio or cellular service is encrypted when in transit.
  - Use of standard encryption like the Advanced Encryption Standard (AES)
- **Resources**:
  - CIS Control 12: Network Infrastructure Management https://www.cisecurity.org/controls/cis-controls-navigator
  - CIS Control 13: Network Monitoring and Defense https://www.cisecurity.org/controls/cis-controls-navigator

Baseline Control: SC-24

Communications links encrypted.

- **What it means:** Hardwired data-in-transit encrypted using current wired communications best practices.

- **Example:**
  - Data transferred via hard-line communications links (fiber, leased circuits) between the control room and remote sites encrypted when in transit.
- **Resources**:
  - CIS Control 13: Network Monitoring and Defense https://www.cisecurity.org/controls/cis-controls-navigator