PROJECT DESCRIPTION

SECURING WATER AND WASTEWATER UTILITIES

Cybersecurity for the Water and Wastewater Systems Sector

Jim McCarthy

National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Bob Stea
Don Faatz

The MITRE Corporation
McLean, Virginia

DRAFT

November 2022

water_nccoe@nist.gov

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, adaptable example cybersecurity solutions demonstrating how to apply standards and best practices by using commercially available technology. To learn more about the NCCoE, visit https://www.nccoe.nist.gov/. To learn more about NIST, visit https://www.nist.gov/.

This document identifies common scenarios across the Water and Wastewater Systems (WWS) sector that may demonstrate higher-risk cybersecurity characteristics for WWS sector utilities. The scenarios are informed by the project team's conversations with stakeholders across the WWS sector. The NCCoE project team will address each scenario in collaboration with members of the WWS sector and vendors of cybersecurity solutions. The resulting reference design will detail an approach that can be used by WWS sector organizations to plan for and mitigate cybersecurity risks.

Abstract

The U.S. Water and Wastewater Systems (WWS) sector has been undergoing a digital transformation. Many sector stakeholders are utilizing data-enabled capabilities to improve utility management, operations, and service delivery. The ongoing adoption of automation, sensors, data collection, network devices, and analytic software may also increase cybersecurity-related vulnerabilities and associated risks.

The NCCoE has undertaken a program to determine common scenarios for cybersecurity risks among WWS utilities. This project will profile several areas, including asset management, data integrity, remote access, and network segmentation. The NCCoE will also explore the utilization of existing commercially available products to mitigate and manage these risks. The findings can be used as a starting point by WWS utilities in mitigating cybersecurity risks for their specific production environment. This project will result in a freely available NIST Cybersecurity Practice Guide.

Keywords

Asset management; data integrity; network segmentation; remote access; SCADA; water and wastewater utility

Acknowledgements

The NCCoE would like to thank the following individuals for their discussions and insights during the development of this project description:

- Leonardo Burgos, Miami-Dade Water and Sewer Department
- Kenneth Crowther, Xylem
- Dan Hartnett, Association of Metropolitan Water Agencies (AMWA)
- Elkin Hernandez, DC Water
- Andrew Hildick-Smith, WaterISAC
- Leilani Martinez, Intern, National Institute of Standards and Technology
- Lisa McFadden, Water Environment Federation
- Lars Schmekel, Miami-Dade County Information Technology Department
- Jennifer Lyn Walker, WaterISAC

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

COMMENTS ON NCCOE DOCUMENTS

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at https://www.nccoe.nist.gov/.

Comments on this publication may be submitted to water_nccoe@nist.gov.

Public comment period: November 2, 2022 to December 19, 2022.

TABLE OF CONTENTS

1 Executive Summary

Purpose

This document outlines a National Cybersecurity Center of Excellence (NCCoE) project that will develop example cybersecurity solutions to protect the infrastructure in the operating environments of WWS sector utilities. The increasing adoption of network-enabled technologies by the sector merits the development of best practices, guidance, and solutions to ensure that the cybersecurity posture of facilities is safeguarded.

This project explores four areas of concern identified by WWS stakeholders, namely: asset management, data integrity, remote access, and network segmentation. These areas have been under review to determine the common features among sector stakeholders and to identify issues being faced by broad segments of the sector. For this project, the focus is on municipal-scale utilities.

Critical infrastructure issues in the WWS sector present several unique challenges. Utilities in the sector typically cover a wide geographic area regarding piped distribution networks and infrastructure together with centralized treatment operations. The supporting operational technologies (OT) underpinning this infrastructure are likely reliant on supervisory control and data acquisition (SCADA) systems which provide data transmission across the enterprise, sending sensor readings and signals in real time. These systems also control the automated processes in the production environment which is linked to the distribution network. Additionally, many OT devices are now converging upon information technology (IT) capability with the advent of Industrial Internet-of-Things (IIoT) devices and platforms, such as cloud-based SCADA and smart monitoring.

This project will identify challenges and develop a reference architecture that demonstrates solutions using commercially available products and services. The project described herein also serves to initiate a broad discussion with WWS sector stakeholders, both from the public and private sectors, to identify stakeholders and commercial solutions providers. The commercial solutions will be integrated into a pilot-lab environment to develop a reference architecture and case study.

This project will result in a publicly available NIST Cybersecurity Practice Guide which will include a detailed implementation guide of the practical steps needed to implement a cybersecurity reference design that addresses these challenges.

Scope

This project description profiles several areas to strengthen the cybersecurity posture within the operational environment of WWS facilities. The following areas will be explored:

- Asset Management – inventory, visibility, criticality
- Data Integrity
- Remote Access
- Network Segmentation

Assumptions

The project will demonstrate solutions to improve the cybersecurity posture of WWS stakeholders and is guided by the following assumptions:

- WWS infrastructure that adequately reflects operational capabilities is available for solution testing
- A range of commercially available solutions exist and are readily available to sector stakeholders to demonstrate solutions to the identified challenges

Challenges

There are a wide range of capabilities among WWS utilities regarding cyber-enabled operations. Identifying challenges that can be representative in addressing a broad range of issues may be difficult. Also, lab-constructed test solutions may not address the complexities of real-world operational scenarios. The NCCoE does not provide prescriptive solutions, but rather demonstrates illustrative cases that may be voluntarily adopted by a large segment of the sector.

Background

There is apparent general consensus from WWS stakeholders that additional cybersecurity implementation references are needed to assist in the protection of its critical infrastructure. The advancement of network-based approaches, together with an ongoing increase in cyber threats, merit the need for sector-wide improvements in cybersecurity protections. The NCCoE, together with its stakeholders, is undertaking this project to identify and demonstrate cybersecurity solutions for the sector. The project will build on existing sector guidance to provide information for the direct implementation of readily available commercial solutions towards the most pressing cybersecurity challenges faced by sector utilities.

This project references efforts undertaken by Federal agencies to ensure the protection of water and wastewater providers. The Environmental Protection Agency (EPA) [1] in its role as the Sector Risk Management Specific Agency (SRMA) provides coordination in responding to cyber incidents and support in the form of tools, exercises, and technical assistance. The Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) [2] leads the efforts to protect assets, mitigate vulnerabilities, and reduce impacts from potential cyber incidents.

WWS organizations have also contributed to sector awareness and capacity building. The American Water Works Association (AWWA) provides resources and guidance for aiding water systems in evaluating cybersecurity risks. The AWWA Cybersecurity Assessment Tool and Guidance, referenced herewith, assists utilities in identifying exposure to cyber risks, setting priorities, and executing appropriate and proactive cybersecurity strategies in support of Section 2013 of America's Water Infrastructure Act of 2018 (AWIA) [3]. Additionally, the Water Environment Federation (WEF) leads the effort among wastewater utilities and is providing guidance and information in the identification of sector needs and priorities [4]. The Water Information Sharing and Analysis Center (WaterISAC) is an all-threats security information source for the water and wastewater sector, providing invaluable information and resources to the WSS sector including the "15 Cybersecurity Fundamentals for Water and Wastewater Utilities." [5]

2 SCENARIOS

Based on discussions with WWS utilities and stakeholders, the NCCoE has identified four categories of interest that have demonstrated high risk characteristics for WWS utilities. The NCCoE plans to explore specific situational challenges within each scenario which will be addressed in collaboration with public and private stakeholders. The goal is to demonstrate a solution set for each scenario-based challenge with commercially available products in an environment that replicates a real-world operational facility in the WWS.

Scenario 1: Asset Management

Common situations may exist in WWS facilities that may produce additional cybersecurity risks:

- The existing equipment and software inventory does not include offsite or remote devices, creating a gap in managing their security configurations.
- Third-party devices are not included in the asset management plan.
- The production facility has PLCs and sensors that cannot be updated past a specific security revision.
- Automatic updates are either disabled or set to manual.
- Non-operating devices are on the network (such as HVAC or smart IoT devices) which may increase the attack surface.
- The entire operational configuration is not backed-up or archived in the event of a cyber-related incident.

In these cases, the utility may be unaware or lack the capability to comprehensively assess the disposition of their assets. Malicious actors can use unpatched vulnerabilities in component software to establish an entry point to implant software.

The expected security requirements / outcomes for asset management are:

- Demonstrate techniques to identify, categorize, and manage all network-enabled devices.
- Detect potential risks on the network from vulnerable network equipment, such as unpatched devices or software flaws.
- Provide solutions for operational system archiving and back-up that can be utilized to restore the system to full functionality in the event of a cyber incident.

Scenario 2: Data Integrity

Secure and reliable communications among network devices may be compromised through several scenarios, such as:

- Data-in-transit is not encrypted, allowing for cleartext transmissions and eavesdropping on packets.
- Direct monitoring of system activity allows spoofing and man-in-the-middle attacks on the network.
- Threat actors can simulate device communications with invalid data packets and diminish network availability.
- Third-party integrators provide updates and changes to existing operational software without aligning the requirements with those of the utility, potentially creating a gap in data security.

The expected security requirements / outcomes for data integrity are:

- Integrity of data-at-rest and data-in-transit is protected. Lack of protection and integrity compromises are detected.
- Demonstrate methods of secure communications to prevent potential system compromise or diminished network availability.
- Provide solutions to allow sandbox testing for network devices and equipment prior to deployment in a production environment, to ensure data integrity in communications.

Scenario 3: Remote Access

Threat actors can obtain access to the network through many avenues, such as credential harvesting, phishing campaigns, or access to cleartext identification and authentication data. The following scenarios can then unfold:

- SCADA software uses generic usernames and passwords, allowing multiple users to access the system without unique authentication.
- Server ports are not restricted to minimum necessary for network traffic, increasing the attack surface.
- Remote access to the network does not require multifactor authentication.
- Third-party hardware and service providers have broad access to the operational technologies, which may also lead to other network areas.

The expected security requirements / outcomes are:

- Demonstrate methods to ensure security policy and practice safeguards are configured on all devices and systems on the network, such as multifactor authentication and elimination of shared accounts.
- Provide a mechanism to enforce protocols such as rules or role-based controls, such that access is dependent on levels of responsibility.
- Detect potential compromise on the network by intrusion or anomalous behavior.
- Demonstrate methods to protect against and remediate malicious activity.

Scenario 4: Network Segmentation

Sector best practices call for network segmentation, which is the division of the network into smaller, logical partitions by either physical or virtual means, based on similarities in function or permissions. The lack of network segmentation may be found in the following types of scenarios:

- There is no manual method to disconnect industrial control system (ICS) components from the general network.
- Secure operations data is not transferred through an actively managed router via a network demilitarized zone (DMZ) to utility managers.
- The network is not segmented (by virtual local area networks or software defined networks) such that communications can flow from any part of the enterprise to another.
- Digital communications between centralized supervisory platforms and process control systems are not implemented through a DMZ.
- Access to critical equipment for plant operations are available from unsecured terminals, providing unauthorized accessibility.

The expected security requirements / outcomes are:

- Provide solutions for the use of commercially available products, such as firewalls or software defined networks, which would provide logical segmentation of the enterprise network.
- Detect vulnerabilities such as congestion, broad network perimeters, or topologies that permit unauthorized access.
- Demonstrate the effectiveness of DMZ-related solutions as an alternative to an entirely air-gapped facility.
- Provide solutions to logically secure sensitive access to high-risk operational components.

3 HIGH-LEVEL ARCHITECTURE

This section proposes a simplified reference architecture as a model to develop the project scenarios. On a broad scale, a municipal WWS utility covers a wide area, with an architecture typified in Figure 1.

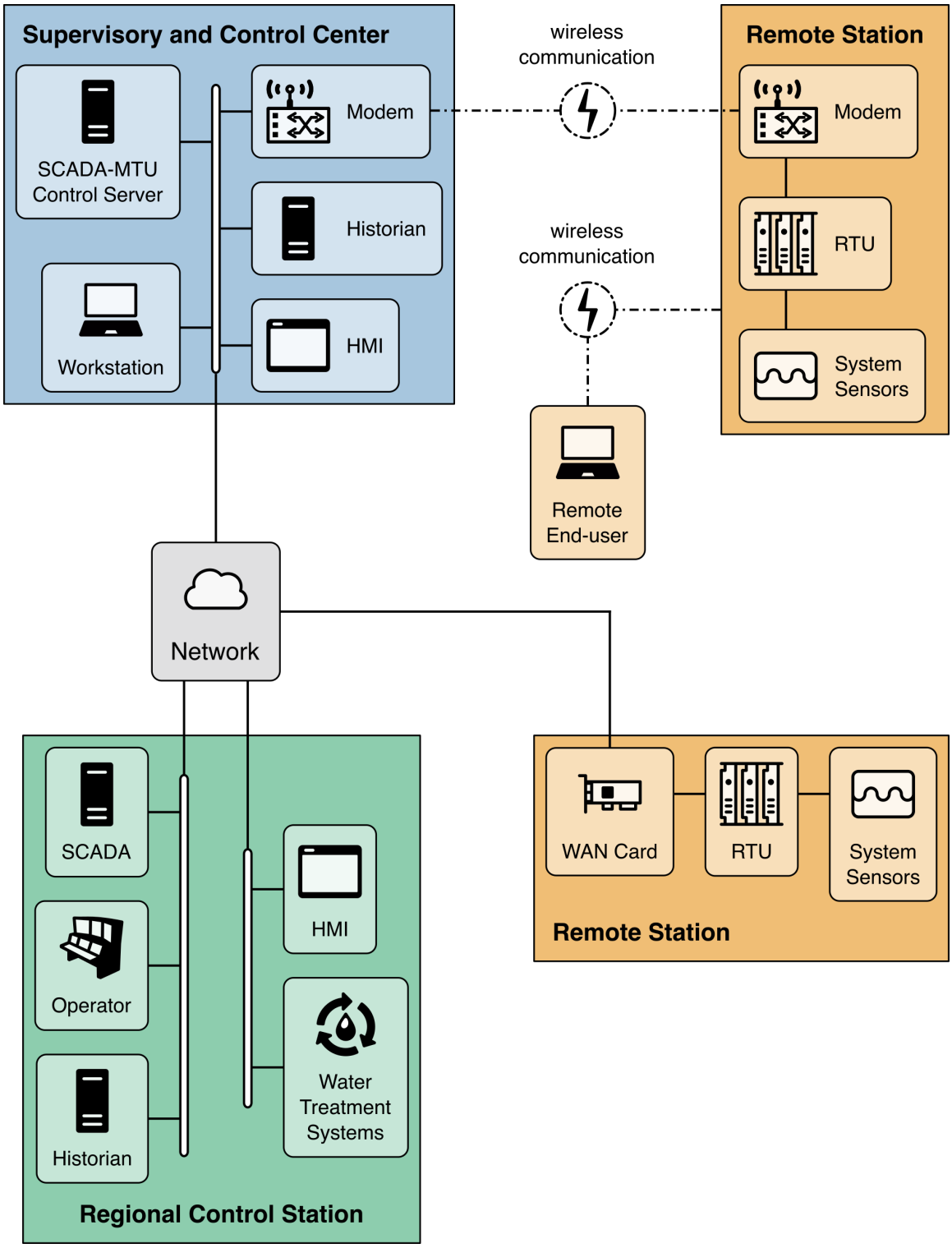

Figure 1 Example WWS Infrastructure

As shown in Figure 1, a WWS utility generally consists of the following components:

- **Centralized**: supervisory capability with remote access to servers and historians collecting data for management and business
- **Regional**: localized treatment centers including wired network servers, supervisor control and data acquisition (SCADA), human-machine interface (HMI), and programmable logic controllers (PLCs) with process controls data and sensor readings
- **Remote**: a wide-area network SCADA with wireless telemetry to monitor remote infrastructure such as pump stations and water distribution network
- Additionally, PLCs and controls distributed among the network and pump stations, with sensors to enable logging of metrics such as pressure, temperature, and physical-chemical characteristics

In this diagram, the WWS utility operates a centralized treatment facility, with several regional sub-facilities depending on the geographic requirements of the municipality. The supervisory and control center can connect with the information from operations and stations via the Internet through remote access capabilities. Network segmentation ideally creates a logical separation among the clusters of connected devices.

Requirements

The project will identify specialized cybersecurity capabilities from collaborating vendors to address the vulnerabilities identified in the previous section. To demonstrate the reference architecture, collaborating stakeholders need to supply products and technology that offer:

Asset Management: Asset discovery and visibility solutions identify all assets that exist on the network, whether physical, virtual, on- or off-premises, or on the cloud. These software solutions also provide information on existing gaps in configurations, product versions, or protocols that require updates or enforcement of security policies. Improving asset discovery and visibility is generally accomplished by the classification and categorization of all network devices, followed by an audit and compliance stage. Enforcement of a predetermined security posture can be accomplished by automation and orchestration of baseline requirements.

Data Integrity: Data integrity solutions will provide capabilities to assure communications within the OT environment are not modified or replaced in transit. These technologies will determine if integrity has been compromised, such as in data modification or spoofing. They provide capabilities to prevent loss of integrity, such as cryptographic mechanisms and validation techniques. These capabilities would also integrate with existing security information and event management systems in the capture and analysis of network traffic data.

Remote Access: Capabilities which serve to provide and enforce access policies will be included in this project. These solutions ensure that authorized communications can take place among network devices and prevent unauthorized access or information exchanges from unknown systems. The capabilities can be configured to monitor and log for unauthorized attempts to authenticate onto the network, providing visibility into the anomalous behavior. In addition, these systems may need to work in tandem with existing identity and access management solutions within the WWS entity, such as federated systems, hybrid cloud / IT networks, multifactor authentication, and IIoT device management.

Network Segmentation: Network segmentation capabilities will provide logically isolated network subsets that can be managed more efficiently and effectively. Segmentation is accomplished by establishing zones, or logical groups, of devices and infrastructure based on

commonalities such as process or operational area, ICS protocol, or accessibility requirements. Segmentation provides a more detailed level of authorization and access, visibility into network flows among critical assets and infrastructure, and control of device management, and minimizes the potential harm from threats by isolating them to a limited part of the network.

4 Relevant Standards and Guidance

- The NIST *Framework for Improving Critical Infrastructure Cybersecurity* (NIST Cybersecurity Framework [CSF]) is a tool to help organizations understand cybersecurity risks associated with their business and define objectives for managing those risks. The framework consists of three components: the Core, the Implementation Tiers, and CSF Profiles. The core organizes cybersecurity into five functions: Identify, Protect, Detect, Respond, and Recover. Each function is further subdivided into categories and subcategories that describe outcomes and objectives related to the function. The four tiers of the CSF describe the level of rigor and sophistication in an organization's cybersecurity program. They provide a basis for understanding and reasoning about the degree to which cybersecurity is or needs to be integrated into business processes. Lastly CSF profiles are used to relate business functions to cybersecurity functions helping an organization understand how cybersecurity can contribute to business outcomes.
- NIST SP 800-82r3 IPD, *Guide to Operational Technology (OT) Security*, provides guidance for securing operational technology systems while preserving performance, reliability, and safety of these systems. The publication addresses establishing an OT cybersecurity program, managing OT cybersecurity risk, developing an OT cybersecurity architecture, and applying the NIST CSF to OT systems.
- WaterISAC, "15 Cybersecurity Fundamentals for Water and Wastewater Utilities", https://www.waterisac.org/fundamentals. This guide, originally published in 2012 and updated in 2019, describes best practices for IT and OT cybersecurity organized under fifteen high-level categories.
- American Water Works Association (AWWA) Cybersecurity Risk Management Tool, Home Page (awwa.org). Using this tool, a user answers 22 questions about their control system environment and the tool generates a prioritized list of needed cybersecurity controls.
- ISO/IEC 62443 is a collection of standards that address requirements and methods of managing cybersecurity control systems and operational technology. The standards are organized in four layers: general, policy and procedures, system, and component.

5 Security Control Map

This table maps the characteristics of the commercial products that the NCCoE will apply to this cybersecurity challenge to the applicable standards and best practices described in the Framework for Improving Critical Infrastructure Cybersecurity, and to other NIST activities. This exercise is meant to demonstrate the real-world applicability of standards and best practices but does not imply that products with these characteristics will meet an industry's requirements for regulatory approval or accreditation.

338 **Table 1: Security Control Map**

Function	Category	Subcategory	NIST 800-53, Revision 5 Control(s)	AWWA Cybersecurity Assessment Tool Controls	Water ISAC 15 Cybersecurity Fundamentals
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried.	CM-8	PM-1	Perform Asset Inventories
		ID.AM-2: Software platforms and applications within the organization are inventoried.	CM-8	PM-1	Perform Asset Inventories
PROTECT (PR)	**Identity Management, Authentication, and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.	IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12	IA-1, SI-3, SC-2, IA-11	Enforce User Access Controls
		PR.AC-3: Remote access is managed	AC-17, AC-19, AC-20	SC-12	Enforce User Access Controls

Function	Category	Subcategory	NIST 800-53, Revision 5 Control(s)	AWWA Cybersecurity Assessment Tool Controls	Water ISAC 15 Cybersecurity Fundamentals
	devices and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-4:** Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24	IA-1, CM-3, CM-4, PS-2, PM-5, IA-10, IA-3, IA-4, IA-11	Enforce User Access Controls
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).	AC-4, AC-10, SC-7, SC-10, SC-20	SC-15	Minimize Control System Exposure
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data at rest is protected.	MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SC-28	SC-1, MP-1, PM-5	
		PR.DS-2: Data in transit is protected.	SC-8, SC-11	SC-1, SC-7	Minimize Control System Exposure
		PR.DS-6: Integrity-checking mechanisms are used to verify software, firmware, and information integrity.	SI-7, SI-10	SI-2, SI-1	
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities,	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained.	CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10	SA-2, SA-3, SC-10	

Function	Category	Subcategory	NIST 800-53, Revision 5 Control(s)	AWWA Cybersecurity Assessment Tool Controls	Water ISAC 15 Cybersecurity Fundamentals
	management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-3:** Configuration change control processes are in place.	CM-3, CM-4, SA-10	SA-2	Develop and Enforce Cybersecurity Policies and Procedures
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-4:** Communications and control networks are protected.	AC-4, AC-17, AC-18, CP-8, SC-7	SC-9, SC-14, SC-23, SC-24, SC-15, SC-8, SC-25, SC-3	Minimize Control System Exposure
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected, and the potential impact of	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed.	AC-4, CA-3, CM-2, SC-16, SI-4		Minimize Control System Exposure

Function	Category	Subcategory	NIST 800-53, Revision 5 Control(s)	AWWA Cybersecurity Assessment Tool Controls	Water ISAC 15 Cybersecurity Fundamentals
	events is understood.	**DE.AE-2:** Detected events are analyzed to understand attack targets and methods.	AU-6, CA-7, RA-5, IR-4, SI-4	SC-4, SC-5	Implement Threat Detection and Monitoring
		DE.AE-4: Impact of events is determined.	CP-2, IR-4, RA-3, SI -4	SC-4, SC-5	Implement Threat Detection and Monitoring
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	AU-12, CA-7, CM-3, SC-5, SC-7, SI-4	SC-4, SC-5, SC-6	Implement Threat Detection and Monitoring
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4		Implement Threat Detection and Monitoring
		DE.CM-8: Vulnerability scans are performed.	RA-5		Embrace Vulnerability Management
Respond (RS)	**Mitigation (RS.MI)**: Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-3**: Newly identified vulnerabilities are mitigated or documented as accepted risks.	CP-1, RA-3, RA-5		Embrace Vulnerability Management

APPENDIX A REFERENCES

[1] United States Environmental Protection Agency (EPA), *The Sources and Solutions: Wastewater*. Available: https://www.epa.gov/nutrientpollution/sources-and-solutions-wastewater.

[2] Cybersecurity and Infrastructure Security Agency (CISA), *National Critical Functions—Supply Water and Manage Wastewater*. Available: https://www.cisa.gov/ncf-water.

[3] Summary 3021, *America's Water Infrastructure Act of 2018*, Available: https://www.congress.gov/115/bills/s3021/BILLS-115s3021enr.pdf.

[4] M. Arceneaux and L. McFadden, *The State of Cybersecurity in the Water Sector*. Water Environment Technology, January, 2022. Available: https://www.waterenvironmenttechnology-digital.com/waterenvironmenttechnology/january_2022/MobilePagedArticle.action?articleId=1753528#articleId1753528.

[5] Water Information Sharing and Analysis Center (ISAC), *15 Cybersecurity Fundamentals for Water and Wastewater Utilities*. 2019. Available: https://www.waterisac.org/system/files/articles/15%20Cybersecurity%20Fundamentals%20%28WaterISAC%29.pdf.

APPENDIX B ACRONYMS AND ABBREVIATIONS

DMZ	Demilitarized Zone
IIoT	Industrial Internet of Things
ICS	Industrial Control Systems
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
OT	Operational Technology
PLC	Programmable Logic Controllers
SCADA	Supervisor Control and Data Acquisition
WWS	Water and Wastewater Systems