PROJECT DESCRIPTION

CYBERSECURITY FOR THE WATER AND WASTEWATER SECTOR

A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems

Jim McCarthy

National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Bob Stea
Don Faatz

The MITRE Corporation
McLean, Virginia

Final

June 2023

water_nccoe@nist.gov

This revision incorporates comments from the public.

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 known cybersecurity characteristics for WWS sector utilities. The scenarios are informed by the project team's conversations with organizations 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 of all sizes—small, medium, and large, 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 organizations 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

Access management, 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.

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.

Critical infrastructure issues in the WWS sector present several unique challenges. Utilities in the sector typically cover a wide geographic area which include piped distribution networks and infrastructure together with centralized treatment operations. The supporting operational technologies (OT) underpinning this infrastructure typically rely 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 converging with Information Technology (IT) capabilities such as cloud-based SCADA and smart monitoring.

This project will develop a reference design that demonstrates practical solutions for water and wastewater utilities of all sizes. The reference design will use commercially available products and services to address four WWS cybersecurity challenges: asset management, data integrity, remote access, and network segmentation. The commercial products and services will be integrated into a demonstration of the reference design. The project also initiates a broad discussion with the WWS sector to identify commercial solution providers.

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 of all sizes—small, medium, and large. To contain scope, the project is not comprehensive. The following areas will be explored:

- Asset Management
- Data Integrity
- Remote Access
- Network Segmentation

Assumptions

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

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

Challenges

- WWS utilities vary widely in size and level of cybersecurity expertise which may require a range of cyber-related capabilities to provide risk-appropriate cybersecurity.
- Lab-constructed example solutions may not fully address the complexity of real-world operational scenarios.
- The NCCOE does not provide prescriptive solutions, but rather demonstrates illustrative case that may be voluntarily adopted by the sector.

Background

There is apparent general consensus from the WWS sector 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 collaborators, 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 of all sizes.

This project acknowledges efforts undertaken by other 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 WWS sector including the "15 Cybersecurity Fundamentals for Water and Wastewater Utilities." [5]

2 SCENARIOS

The NCCoE presents four scenarios in which significant Cybersecurity concerns to WWS organizations are identified. The NCCoE will explore specific situational challenges within each scenario and these will be addressed in collaboration with public and private organizations, including product manufacturers. The goal is to demonstrate a solution set for each scenario-based challenge with available commercial and open source products in an environment that replicates a real-world operational facility in the WWS. Given the abundance of small utilities in this sector, particular consideration will be given to addressing challenges from their perspective.

Scenario 1: Asset Management

Common situations among OT and cyber-related assets may produce additional cybersecurity risks among WWS facilities including:

- The existing OT equipment and software inventory does not include offsite or remote devices, creating a gap in managing their security configurations.
- Devices and equipment provided by external vendors are not included in the asset management plan.
- The production facility has programmable logic controllers (PLCs) and sensors that cannot be updated past a specific security revision.
- Automatic update installation is disabled or installation is set to manual.
- Devices that are no longer in active use remain connected to 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, a utility may be unaware that an asset is unpatched or misconfigured. Malicious actors can use unpatched vulnerabilities and insecure configurations in component software to establish an entry point to a system.

The expected cybersecurity outcomes for asset management are:

- Demonstrate techniques to discover, identify, categorize, and manage all network-enabled devices.
- Detect potential risks on the network from vulnerable network equipment, such as unpatched devices or improperly configured software.
- 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.
- validate device software patches and upgrades are provided in a secure manner by the product suppliers, and that they are tested and verified prior to release in the operating environment.

Scenario 2: Data Integrity

Areas of concern with the compromise of secure and reliable communications among networked and connected devices are exemplified by the following scenarios, 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 that have not been verified by the utility.

The expected cybersecurity outcomes for data integrity are:

- Demonstrate methods to protect the Integrity of data-at-rest and data-in-transit. Detect lack of protection and integrity compromises.
- Demonstrate methods of secure communications to prevent potential system compromise or diminished network availability.
- Provide solutions to allow sandbox testing of network devices, equipment, and updates prior to deployment in a production environment, to ensure data integrity in communications. Facilitate rollback to a previous state in the event that changes adversely interfere with critical OT communications.
- Demonstrate methods to ensure software updates are received unmodified from authoritiative sources.

Scenario 3: Remote Access

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

- Well known default usernames and passwords remain in place and allow access to systems without proper authentication.
- Remote access allows broad access to operational technologies and other systems.
- Remote access to the network does not require multifactor authentication.
- Third-party hardware and service providers have broad access to operational technologies, which may also lead to other network areas.

The expected cybersecurity outcomes for remote access are:

- Demonstrate methods to ensure security safeguards are configured on all devices and systems on the network, such as multifactor authentication and that shared and default accounts are eliminated.
- Demonstrate mechanisms that control access based on levels of responsibility.
- Detect potential compromise of the network by intrusion or anomalous behavior.
- Collect, aggregate, and analyze all system log information in a centralized log management capability.

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 isolate or 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, thereby allowing communications 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 cybersecurity outcomes for network segmentation are:

- Demonstrate the use of available commercial and open source products, such as firewalls, data diodes, or software defined networks, to provide logical segmentation of the operational network.
- Demonstrate inclusion of security controls within segmentation to provide additional protections, such as policy management, threat detection, monitoring, alerting and reporting.
- Detect vulnerabilities such as broad network perimeters or topologies that permit unauthorized access.
- Demonstrate the effectiveness of network segmentation solutions which provide security while also enhancing operations.
- Provide solutions to logically secure sensitive access to high-risk operational components.

3 HIGH-LEVEL ARCHITECTURE

This section presents a simplified reference architecture of water and wastewater systems. The reference architecture illustrates the capabilities and connections needed within WWS. It serves as a model against which security solutions can be developed. On a broad scale, a municipal WWS utility covers a wide area, with an architecture typified in Figure 1.

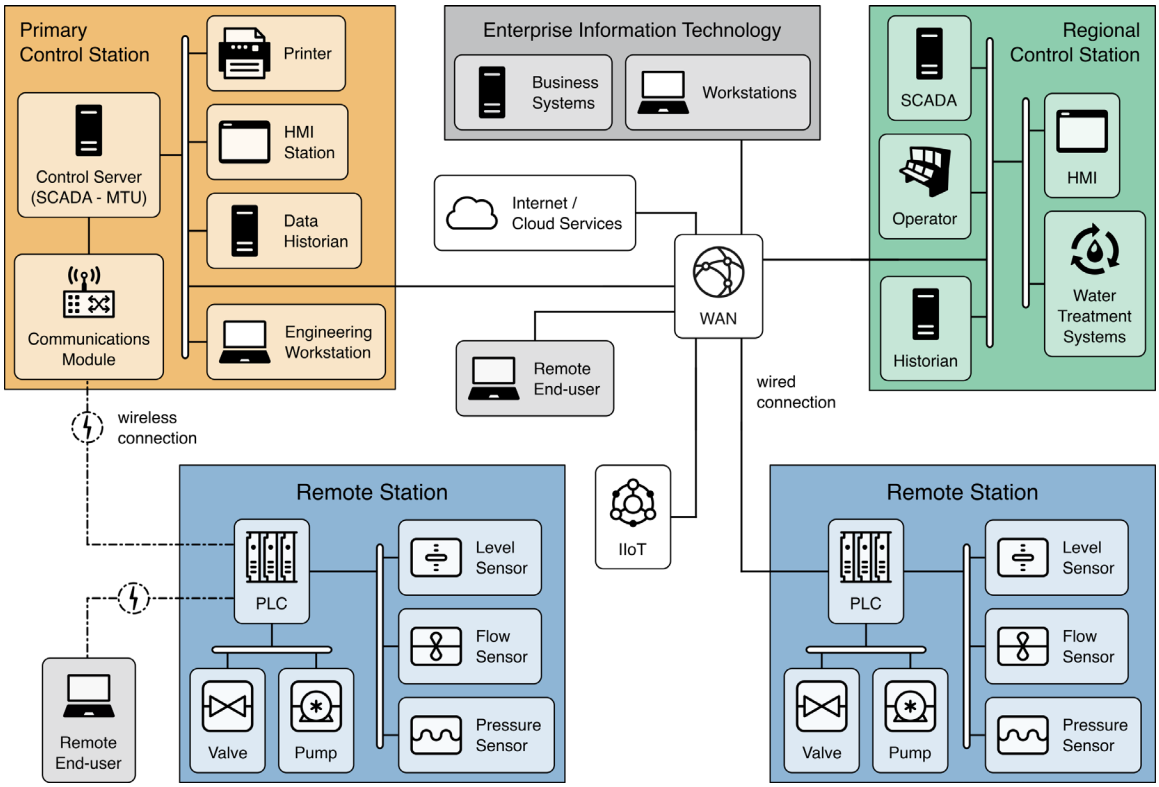

Figure 1 WWS Reference Architecture

A WWS generally consists of the following components:

- A **primary control station** that provides access to server and historian data for management and business purposes.
- **Regional control stations** at localized treatment centers that include wired network servers, supervisory control and data acquisition (SCADA) systems, human-machine interfaces (HMIs), and treatment systems that use PLCs and sensors to provide real-time control of the treatment process.
- **Remote stations**, connected to a wide-area network, that monitor remote infrastructure such as pump stations and the water distribution network.
- PLCs and industrial controls, distributed among the network and pump stations, with sensors to measure pressure, temperature, and physical-chemical characteristics.

The utility depicted in Figure 1 operates a centralized treatment facility, with several regional sub-facilities. The primary control station can connect with the regional control stations and the remote stations via a wide-area network.

Required Capabilities

This project will employ products, provided by collaborating vendors, that provide the following cybersecurity capabilities to address the four scenarios described in Section 2:

Asset Management: Asset management capabilities discover and identify physical and virtual assets in the OT environment. These assets may be geographically distributed and may be cloud-based. In addition to network-connected assets, these capabilities should provide a means to discover and identify assets connected by low-bandwidth communications channels and disconnected assets. The asset management capability maintains an inventory of known assets which contains information such asset type, product version, and communication protocols used. Asset management capabilities may provide automation to establish and enforce a baseline security posture.

Data Integrity: Data integrity capabilities protect data and communications within the OT environment against improper modification or destruction. Additionally, these capabilities monitor the OT environment to detect potential integrity violations and generate alerts to initiate any needed responses.

Remote Access: Remote access capabilities provide entities (people and systems) controlled access to OT assets from outside the OT environment. These capabilities authenticate any entity seeking access, allow only explicitly authorized access, control which actions are allowed for each authorized entity, and maintain a record of all actions attempted and completed by each entity.

Network Segmentation: Network segmentation capabilities provide logically isolated network subsets that can be managed more efficiently and effectively. Segmentation allows for 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 resources listed below were critical for helping the project team define this project's scope. This is not an exhaustive list, and the references below are not listed in any specific order of importance or priority:

- 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.
- NIST SP 800-53r5, *Security and Privacy Controls for Information and Organizations*, provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets from a diverse set of threats and risks. The controls are flexible and customizable and can be implemented as part of an organization-wide process to manage risk.
- 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.
- AWWA*, Water Sector Cybersecurity Risk Management Guidance prepared by West Yost Associates*, available https://www.awwa.org/Portals/0/AWWA/ETS/Resources/AWWACybersecurityGuidance2019.pdf. This guide, in conjunction with the AWWA Cybersecurity Risk Management Tool, provides step-by-step guidance for protecting water sector process control systems (PCS).

- ISA/IEC 62443 is a collection of standards that address requirements and methods of managing cybersecurity for control systems and operational technology. The standards are organized in four layers: general, policy and procedures, system, and component.

5 Security Control Map

The NIST Framework for Improving Critical Infrastructure Cybersecurity Core, also known as the NIST Cybersecurity Framework (CSF) Core, provides a set of desired cybersecurity activities and outcomes in a common language that guides organizations in managing and reducing their cybersecurity risks in a way that complements an organization's existing cybersecurity and risk management processes. The table below identifies the subset of CSF Core activities and outcomes that this project will demonstrate for WWS. The table also relates the CSF Core activities and outcomes to relevant cybersecurity controls defined in NIST Special Publication 800-53r5 and to existing WWS cybersecurity guidance provided by the American Water Works Association (AWWA) and by the Water Information Sharing and Analysis Center (ISAC).

NIST will use commercially available and open source products to achieve these CSF Core outcomes for WWS in example solutions. The cybersecurity characteristics of products used will be mapped to these CSF Core activities and outcomes.

This information is not comprehensive, but it documents the applicability of standards, guidelines, and recommended practices to the security characteristics of the solution. It does not imply that any products and services used in example solutions will meet an industry's requirements for regulatory approval or accreditation**.**

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	**ID.AM-1:** Physical devices and systems within the organization are inventoried.	CM-8	PM-1	Perform Asset Inventories

Function	Category	Subcategory	NIST 800-53, Revision 5 Control(s)	AWWA Cybersecurity Assessment Tool Controls	Water ISAC 15 Cybersecurity Fundamentals
	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-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 devices and is managed consistent with the assessed risk of unauthorized access to authorized	**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
		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

Function	Category	Subcategory	NIST 800-53, Revision 5 Control(s)	AWWA Cybersecurity Assessment Tool Controls	Water ISAC 15 Cybersecurity Fundamentals
	activities and transactions.	**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, management commitment, and coordination among	**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	
		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

Function	Category	Subcategory	NIST 800-53, Revision 5 Control(s)	AWWA Cybersecurity Assessment Tool Controls	Water ISAC 15 Cybersecurity Fundamentals
	organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-4:** Backups of information are conducted, maintained, and tested periodically.	CP-4, CP-6, CP-9	SA-5	Plan for Incidents, Emergencies, and Disasters
	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 events is understood.	**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
		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

Function	Category	Subcategory	NIST 800-53, Revision 5 Control(s)	AWWA Cybersecurity Assessment Tool Controls	Water ISAC 15 Cybersecurity Fundamentals
		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
MTU	Master Terminal Unit
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
OT	Operational Technology
PCS	Process Control System
PLC	Programmable Logic Controllers
RTU	Remote Terminal Unit
SCADA	Supervisor Control and Data Acquisition
WWS	Water and Wastewater Systems